Jason Garbis
Jerry W. Chapman

Zero Trust Sicherheit

Ein Leitfaden für Unternehmen

Springer Vieweg

Zero Trust Sicherheit

Ein Leitfaden für Unternehmen

Jason Garbis
Jerry W. Chapman

Apress®

Zero Trust Sicherheit: Ein Leitfaden für Unternehmen

Jason Garbis
Boston, MA, USA

Jerry W. Chapman
Atlanta, GA, USA

ISBN 979-8-8688-0104-4 ISBN 979-8-8688-0105-1 (eBook)
https://doi.org/10.1007/979-8-8688-0105-1

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der DeutschenNationalbibliografie; detaillierte bibliografische Daten sind im Internet über https://portal.dnb.de abrufbar.

Dieses Buch ist eine Übersetzung des Originals in Englisch „Zero Trust Security“ von Jason Garbis, publiziert durch APress Media, LLC im Jahr 2021. Die Übersetzung erfolgte mit Hilfe von künstlicher Intelligenz (maschinelle Übersetzung). Eine anschließende Überarbeitung im Satzbetrieb erfolgte vor allem in inhaltlicher Hinsicht, so dass sich das Buch stilistisch anders lesen wird als eine herkömmliche Übersetzung. Springer Nature arbeitet kontinuierlich an der Weiterentwicklung von Werkzeugen für die Produktion von Büchern und an den damit verbundenen Technologien zur Unterstützung der Autoren.

Planung/Lektorat: Susan McDermott
Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft APress Media, LLC und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: 1 New York Plaza, New York, NY 10004, U.S.A.

Das Papier dieses Produkts ist recycelbar.

Für Amy, Shira und Shelly
—J.G.

Für meine schöne und liebevolle Frau, Suzette—Danke!
An unsere geliebten Töchter, Nena und Alex—Ihr seid geliebt!
—J.W.C.

Inhaltsverzeichnis

Über die Autoren

Jason Garbis ist Gründer und Leiter von Numberline Security, einem Beratungsunternehmen, das Schulungen und Beratungsdienste zu Zero Trust Security anbietet. Jason ist Mitautor des viel beachteten Buches „Zero Trust Security: An Enterprise Guide“, Co-Vorsitzender der Zero Trust Working Group bei der Cloud Security Alliance und ist ein häufiger Redner auf Branchenkonferenzen. Jason ist CISSP-zertifiziert, hat einen BS in Computerwissenschaften von Cornell und einen MBA von Northeastern. Beruflich hat er Erfahrung in den Bereichen Identitätsmanagement, Unternehmenssicherheitsarchitekturen, Netzwerksicherheit und Sicherheitsstrategie. Zuvor war er als Chief Product Officer bei Appgate tätig und hatte Positionen bei Sicherheitsunternehmen wie RSA und Aveksa inne.

Jerry W. Chapman ist ein Cybersecurity-Experte mit Schwerpunkt Identität. Mit mehr als 25 Jahren Branchenerfahrung hat Jerry Chapman zahlreiche Kunden erfolgreich bei der Konzeption und Implementierung ihrer Unternehmens-IAM-Strategien beraten, die sowohl den Sicherheits- als auch den Geschäftszielen entsprechen. Seine Aufgaben umfassten die Bereiche Unternehmensarchitektur, Solution Engineering sowie Softwarearchitektur und -entwicklung. Jerry ist Co-Vorsitzender der Zero Trust Working Group bei der Cloud Security Alliance und ist in der technischen Arbeitsgruppe der Identity Defined Security Alliance (IDSA) aktiv, wo er der ursprüngliche Technical Architect der Gruppe war. Jerry ist ein zertifizierter Forrester Zero Trust Strategist, hat einen BS in Computer Information Systems von

der DeVry University und macht derzeit einen Abschluss in angewandter Mathematik von der Southern New Hampshire University.

Über den technischen Gutachter

Christopher Steffen bringt über 20 Jahre Branchenerfahrung als bekannter Informationssicherheitsleiter, Forscher und Präsentator mit, mit Schwerpunkt auf IT-Management/Führung, Cloud-Sicherheit und regulatorischer Konformität.

Chris hatte eine Vielzahl von Rollen als Fachmann und/oder Führungskraft, vom Campingdirektor für die Pfadfinder bis zum Pressesekretär für den Sprecher des Hauses in Colorado. Seine technische Karriere begann im Finanzdienstleistungssektor in der Systemverwaltung für ein Kreditberichtsunternehmen, baute schließlich die Netzwerkbetriebsgruppe auf, sowie die Praxis für Informationssicherheit und technische Compliance für das Unternehmen, bevor er als Haupttechnischer Architekt ausschied. Er war der Direktor für Information bei einem Produktionsunternehmen und der Chief Evangelist für mehrere technische Unternehmen, mit Schwerpunkt auf Cloud-Sicherheit und Cloud-Anwendungstransformation, und hatte auch die Position des CIO eines Finanzdienstleistungsunternehmens inne, bei dem er die technologiebezogenen Funktionen des Unternehmens überwachte.

Chris ist derzeit der leitende Forscher für Informationssicherheit, Risiko- und Compliance-Management bei Enterprise Management Associates (EMA), einem führenden Branchenanalystenunternehmen, das tiefe Einblicke in das gesamte Spektrum der IT- und Datenmanagementtechnologien bietet.

Chris besitzt mehrere technische Zertifizierungen, einschließlich Certified Information Systems Security Professional (CISSP) und Certified Information Systems Auditor (CISA), und wurde fünfmal mit dem Microsoft Most Valuable Professional Award für Virtualisierung und Cloud- und Data Center Management (CDM) ausgezeichnet. Er hat einen Bachelor of Arts (Summa Cum Laude) vom Metropolitan State College of Denver.

Danksagungen

Zero Trust-Sicherheit umfasst ein sehr breites Gebiet, und der Prozess, den wir durchlaufen haben, um technische, nicht-technische und architektonische Konzepte zu erkunden, zu lernen und zu verknüpfen, war oft herausfordernd. Wir hatten das Glück, viele Menschen zu haben, die bereit waren, Zeit mit uns zu verbringen, uns zu unterrichten, unsere Fragen zu beantworten und Feedback und Anleitung zu geben. Einige Leute halfen uns, indem sie unseren geplanten Entwurf oder unsere Arbeit im Gange lasen und kommentierten, einige trugen dazu bei, indem sie mit uns in Videokonferenzen brainstormten (ein Markenzeichen von 2020, vermuten wir), während andere uns halfen (ob sie es wissen oder nicht), indem sie Teil der Informationssicherheitsindustrie waren und als Teil ihrer regelmäßigen beruflichen Interaktionen mit uns.

Vielen Dank an Dr. Chase Cunningham für Ihren breiten Brancheneinfluss und Brigadegeneral (a.D.) Greg Touhill für Ihre Unterstützung im Vorwort. Und Dank an Sie beide für Ihre Karrieren im Dienst unseres Landes in militärischen und informationssicherheitsbezogenen Rollen. Wir möchten auch Evan Gilman, Doug Barth, Mario Santana, Adam Rose, George Boitano, Bridget Bratt, Leo Taddeo, Rob Black, Deryck Motielall und Kurt Glazemakers danken. Außerdem ein Dankeschön an das Team der Cloud Security Alliance und seiner SDP Zero Trust Arbeitsgruppe, einschließlich Shamun Mahmud, Junaid Islam, Juanita Koilpillai, Bob Flores, Michael Roza, Nya Alison Murray, John Yeoh und Jim Reavis. Und ein weiteres Dankeschön an Julie Smith und das Identity Defined Security Alliance (IDSA) Team, insbesondere die technische Arbeitsgruppe, die die Identität in der Mitte der Sicherheit hält. Wir möchten auch unseren zu zahlreichen Kollegen für ihre vielen Gespräche und ihre Unterstützung danken, sowie unseren Apress-Editoren Rita Fernando und Susan McDermott für ihre Unterstützung, Ermutigung und Hilfe während dieses Prozesses. Und natürlich ein riesiges Dankeschön an unseren technischen Gutachter, klingendes Brett und Freund Chris Steffen.

Schließlich möchten wir uns bei Ihnen bedanken - als Praktiker oder Führer in der Informationssicherheitsbranche, der jeden Tag daran arbeitet, Ihre Organisation besser abzusichern. Wir hoffen, dass dieses Buch Ihre Arbeit erleichtert. Bitte besuchen Sie uns unter https://ZeroTrustSecurity.guide mit jeglichen Kommentaren oder Vorschlägen und um die Begleitvideoserie dieses Buches anzusehen.

Geleitwort

Zero Trust wurde nicht aus dem Bedürfnis heraus geboren, eine weitere Sicherheitskontrolle oder Lösung zu verkaufen. Es entstand aus dem Wunsch, ein reales Unternehmensproblem zu lösen…Zero Trust konzentriert sich auf Einfachheit und die Realität, wie die Dinge jetzt sind.

—Dr. Chase Cunningham, auch bekannt als „Dr. Zero Trust"

Ich habe über zwei Jahrzehnte auf dieses Buch gewartet und freue mich, seine Ankunft vorzustellen.

Lange vor der kühnen Erklärung des Jericho Forums im Jahr 2004 über eine neue Sicherheitsstrategie mit dem Schwerpunkt „De-Perimeterisierung" waren viele von uns in der nationalen Sicherheitsgemeinschaft zu der Erkenntnis gelangt, dass das Perimetersicherheitsmodell keine tragfähige Sicherheitsstrategie mehr für internetverbundene Systeme und Unternehmen war. Der unersättliche Durst, alles mit dem Internet zu verbinden, die steigenden Kosten und die Komplexität der Sicherheitsschichten und das rasante Tempo des technologischen Wandels brachen das Perimetersicherheitsmodell um uns herum auf. Unser Verteidigung-in-die-Tiefe-Sicherheitsperimeter war ein Deich, der zu viele Lecks aufwies, als dass wir in irgendeiner sinnvollen oder fiskalisch verantwortungsvollen Weise Schritt halten könnten. Die Arbeit des Jericho Forums wies in eine andere Richtung und gab vielen von uns eine neue Hoffnung.

Leider hatten sich, wie Grand Moff Tarkin auf dem Todesstern, viele Sicherheitsprofis und Kommentatoren mit dem Status quo angefreundet und die Vorstellung belächelt, dass ein neuer Ansatz zur Sicherung moderner Unternehmen benötigt wurde. Ein Sicherheitskommentator ging sogar so weit zu sagen, dass das Jericho Forum „das Ziel verfehlt" habe und spottete voraus, dass seine Arbeit wahrscheinlich „auf dem Schrotthaufen unrealisierter Ideen und verschwendeter Anstrengungen enden würde." Ich hoffe, dass er dieses Buch mit einem Hauch von Schuld und Bedauern liest.

Die Arbeit des Jericho Forums war nicht umsonst, aber sie brachte auch nicht sofort Früchte. Nach etwas mehr als 5 Jahren seit der Einführung des Konzepts der „De-Perimeterisierung“ prägte John Kindervag, damals Analyst bei Forrester Research, im Jahr 2010 den Begriff „Zero Trust“ zur Beschreibung des Sicherheitsmodells, dass Organisationen nichts außerhalb oder innerhalb ihrer Perimeter automatisch vertrauen sollten, und stattdessen alles und jedes überprüfen müssen, bevor sie sie mit ihren Systemen verbinden und Zugang zu ihren Daten gewähren.

Für uns im Militär war Zero Trust kein revolutionäres Sicherheitsmodell. Wir hatten es mit physischer Sicherheit während unserer gesamten Karriere praktiziert. Zum Beispiel wurde jede Person am Tor von Sicherheitspersonal begrüßt und musste ordnungsgemäße Identitätsnachweise vorlegen, bevor sie Zugang zur Basis erhielt. Wir praktizierten Segmentierung mit Schutzzonen um das, was wir Priorität A, B und C Ressourcen nannten. Die Fluglinienbereiche waren das Zuhause von Priorität A Vermögenswerten und hatten streng kontrollierten Zugang mit bewaffneten Wachen. Rollenbasierte Eintritte wurden streng kontrolliert und der Einsatz von tödlicher Gewalt gegen diejenigen autorisiert, die die „rote Linie durchbrachen“. Als Leutnant musste ich vier Sicherheitsstufen durchlaufen, bevor ich überhaupt in mein Büro gelangen konnte. Sicherheit war in unserer Kultur, unseren Prozessen und unseren Erwartungen verankert.

Leider fehlte die Technologie, um ein „Zero Trust“-Sicherheitsmodell zum Schutz unserer zunehmend wertvollen und mit dem Internet verbundenen digitalen Vermögenswerte zu implementieren, als meine Generation schrittweise die Informationsnetzwerke des Verteidigungsministeriums aufbaute, während wir ein „Zero Trust“-physisches Sicherheitsmodell befolgten, um unsere wertvollsten Einrichtungen und Waffensysteme zu schützen. Kommerziell erhältliche Werkzeuge waren äußerst komplex und teuer. Zum Beispiel mussten wir einen Vertrag mit einem bekannten Anbieter abschließen, um eine „Akademie“ zu schaffen, nur um unsere bereits hochqualifizierte Belegschaft richtig in die Nutzung ihrer komplexen Netzwerkprodukte einzuschulen. Die Kosten stiegen weiter an, während wir unseren Marsch zur Digitalisierung jeder Funktion fortsetzten, doch der Sicherheitsperimeterdamm um uns herum sprang weiterhin Lecks. Als ich vom Bundesdienst als Chief Information Security Officer der US-Regierung in den Ruhestand ging, war ich zu dem Schluss gekommen, dass die Zero Trust-Sicherheitsstrategie unsere einzige Hoffnung war, unser digitales Ökosystem zu sichern.

XX

Die COVID-19-Pandemie hat einen massiven Wechsel von traditionellen Büroumgebungen zu einem Modell der Heimarbeit angestoßen, das den lang erwarteten Übergang zur Zero Trust-Sicherheitsstrategie beschleunigt hat. Die Illusion des Sicherheitsperimeters wurde durch massive Mobilität, Cloud-Computing, Software-as-a-Service und beispiellose Implementierung von Bring-Your-Own-Device in Organisationen überall zerstört, als sie von traditionellen Unternehmensumgebungen zur heutigen modernen digitalen Realität wechselten. Die Realität heute ist, dass der traditionelle Netzwerksicherheitsperimeter tot ist; es gibt kein „außen“ oder „innen“ mehr.

Leider sind viele Menschen und Organisationen, einschließlich dieses Skeptikers, der die Vision des Jericho Forums verspottet hat, auf den Zero Trust-Zug aufgesprungen. Viele bekennen sich zu „Zero Trust“, wissen aber nicht, was es wirklich ist oder wie man es praktiziert. Organisationen, deren veraltete Netzwerktechnik und -methoden sich als übermäßig komplex und anfällig erwiesen haben, lassen ihre Marketingteams ihre anfälligen Fähigkeiten wunderbarerweise als „Zero Trust“ bezeichnen. Trotz der großartigen Zero Trust-Forschung, die von Forrester's Dr. Chase Cunningham und Gartner's Neil MacDonald durchgeführt wurde, gab es bis zu diesem Buch keinen praktischen definitiven Leitfaden zu Zero Trust.

Glücklicherweise sind die Autoren Jason Garbis und Jerry Chapman hocherfahrene Technologen und Praktiker, die als anerkannte Experten in Zero Trust, Unternehmensnetzwerkbetrieb, Cybersicherheit und Geschäftsbetrieb gelten. Ich ermutige Sie, ihre Biografien zu lesen, da ihre Qualifikationen beeindruckend und unverfälscht sind. Um es mit militärischem Jargon zu sagen, sie haben „Das schon erlebt, das schon gemacht“.

In den folgenden Kapiteln liefern Jason und Jerry ein hervorragendes Buch, das eine unschätzbare Erklärung von Zero Trust präsentiert, die meiner Meinung nach als das endgültige Referenzwerk für Studenten und Praktiker überall verwendet werden sollte.

Die Organisation des Inhalts ist hervorragend. Diejenigen, die nicht mit dem Konzept des Zero Trust vertraut sind, und sogar diejenigen, die es sind, werden von den ersten vier Kapiteln profitieren, die einen strategischen Überblick über die Zero Trust-Reise bieten. Kap. 1 bietet eine aufschlussreiche Diskussion, die die Frage beantwortet: „Warum wird Zero Trust benötigt?“ Diejenigen, die gerade ihre Zero Trust-Reise beginnen, werden Kap. 2 als unschätzbar wertvoll empfinden,

da die Autoren eine ausgezeichnete Chronik darüber liefern, wie wir zur heutigen Zero Trust-Umgebung gekommen sind und klar definieren, was Zero Trust ist und was nicht. Diejenigen, die versuchen zu sehen, wie sie Zero Trust in ihre Betriebsarchitekturen integrieren können, werden den praktischen Rat und die lebendigen Beschreibungen zu schätzen wissen, die in Kap. 3 präsentiert werden. Viele Menschen, einschließlich mir selbst, ziehen es vor, dass andere „Flugtests" von Fähigkeiten durchführen, bevor sie bedeutende Investitionen tätigen oder größere strategische Änderungen vornehmen. Wir werden in Kap. 4 mit einer umfassenden Diskussion belohnt, wie Organisationen wie Google Zero Trust in ihren Betrieb integriert haben.

Der zweite Teil des Buches bietet einen hervorragenden Überblick über die wesentlichen Komponenten von Zero Trust, beginnend mit Kap. 5's außergewöhnlicher Diskussion über Identität. Ich behaupte, dass Identität die Kernkomponente jeder erfolgreichen Zero Trust-Implementierung ist und war erfreut zu sehen, dass Jason und Jerry diesen Abschnitt des Buches mit diesem Kapitel beginnen. Die nächsten drei Kapitel bieten eine wichtige Diskussion über die Auswirkungen von Zero Trust auf die Netzwerkinfrastruktur, die Netzwerkzugangskontrolle und die Systeme zur Erkennung und Abwehr von Eindringlingen. Wenn Sie diese drei Kapitel provokativ finden, wird Kap. 9's Diskussion über virtuelle private Netzwerke in einer Zero Trust-Welt wahrscheinlich die Art und Weise ändern, wie Sie die heutige Umgebung und die anhaltende Bewegung zu einer Arbeit-von-überall-Zukunft sehen.

Die Diskussion in Kap. 10 über Next-Generation Firewalls (NGFWs) ist ebenso provokativ, da die Autoren die Geschichte und Entwicklung der betreffenden Fähigkeiten diskutieren und ihre Zukunft in einer Welt des Zero Trust prognostizieren. Die Diskussion in Kap. 11 über Security Information and Event Management (SIEM) und Security Orchestration, Automation, and Response (SOAR) in einem Zero Trust Modell ist ein Muss für diejenigen, die sich auf die Identifizierung, das Management und die Kontrolle von Risiken konzentrieren. Diejenigen, die die Diskussion in Kap. 5 über Identität außergewöhnlich finden, werden von der Diskussion in Kap. 12 über Privileged Access Management nicht enttäuscht sein. Organisationen, die bestrebt sind, ihr Risiko von Insider-Bedrohungen zu reduzieren, sollten dem ebenfalls besondere Aufmerksamkeit schenken!

Die nächsten vier Kapitel bieten praktische Analysen und Anleitungen zu aktuellen technischen Problemen, mit denen viele Organisationen heute konfrontiert sind. Die Diskussion in Kap. 13 über Datenschutz ist außergewöhnlich und etwas, dem meine Studenten am Heinz College der Carnegie Mellon University besondere Aufmerksamkeit schenken sollten (das ist ein nicht allzu subtiler Hinweis vom Professor!). Die Diskussion in Kap. 14 über Cloud-Ressourcen bietet unkomplizierte praktische Ratschläge, wie man Zero Trust richtig anwendet, wenn man in Cloud-basierten Umgebungen arbeitet. Da viele Organisationen Technologien wie Software as a Service, Secure Web Gateways und Cloud Access Security Broker einsetzen, bietet Kap. 15 eine hervorragende Diskussion darüber, wie diese Technologien in Ihre Zero Trust-Strategie integriert werden können und gibt praktische Ratschläge, wie man es „richtig macht". Schließlich war ich begeistert, die Einbeziehung von Jason und Jerry's Diskussion in Kap. 16 über Internet of Things-Geräte und „Dinge" zu sehen. Zu viele Cybersicherheitspersonal sind auf Informationstechnologiegeräte fixiert und ignorieren die Risiken, die mit organisationaler Betriebstechnologie, industriellen Steuerungssystemen und „Internet of Things"-Geräten verbunden sind. Unabhängig von Ihrer organisatorischen Rolle, bitte beachten Sie dieses Kapitel und erkennen Sie die Bedeutung der Anwendung von Zero Trust beim Schutz dieser wichtigen Systeme.

Den Abschluss des Buches bilden drei Kapitel, die für jede Organisation, die sich dazu verpflichtet hat, Zero Trust in ihren Organisationen richtig umzusetzen, von entscheidender Bedeutung sind. Kap. 17 bietet eine wesentliche Diskussion darüber, wie man ein aussagekräftiges Zero Trust-Politikmodell erstellt und implementiert. Kap. 18 bietet unschätzbare Diskussionen über die wahrscheinlichsten Anwendungsfälle, die Ihre Organisation behandeln wird, wenn Sie Ihre Zero Trust-Implementierung ausrollen. Kap. 19 ist ein willkommener Begleiter zum vorherigen Kapitel, da es diskutiert, wie Organisationen Zero Trust angehen sollten, um die größte Wahrscheinlichkeit für Erfolg zu haben. Diejenigen, die an das Mantra „klein anfangen, groß denken und schnell skalieren" glauben, werden von Jasons und Jerrys praktischen Ratschlägen nicht enttäuscht sein. Schließlich bietet Kap. 20 einen zufriedenstellenden Abschluss der Reise des Buches durch Zero Trust, mit der Erinnerung daran, dass Sicherheit dazu dient, Organisationen bei der Erreichung ihrer Ziele zu unterstützen.

Zero Trust ist nicht nur ein eingängiger Aphorismus, es liegt in unserer Reichweite und wartet darauf, überall implementiert zu werden. Dieses Buch wird Ihnen helfen, Ihre Zero Trust-Ziele mit Geschwindigkeit und Präzision zu erreichen. Staatsakteure und Cyberkriminelle haben bewiesen, dass das auf dem Perimeter basierende Sicherheitsmodell nicht mehr gültig ist. So auch bemerkenswerte Insider-Schurken wie Edward Snowden. Die Zeit, sich schnell und gezielt auf das Zero Trust-Sicherheitsmodell zu bewegen, ist jetzt. Dank der aufschlussreichen Arbeit von Jason Garbis und Jerry Chapman haben wir nun einen praktischen Leitfaden, wie wir unsere Zero Trust-Ziele erreichen können.

Generäle seit Sun Tzu und Alexander dem Großen implementierten das perimeterbasierte Sicherheitsmodell, um ihre Vermögenswerte zu verteidigen. Sie hatten nicht das Internet, mobile Geräte, Cloud-Computing und andere moderne Technologien. Das Jericho Forum hat es richtig gemacht; der Perimeter ist tot. Jetzt ist es an der Zeit, Zero Trust überall zu umarmen und zu implementieren. Unsere nationale Sicherheit und nationaler Wohlstand verdienen nichts weniger.

—Gregory J. Touhill, CISSP, CISM,
Brigadegeneral, USAF (im Ruhestand)

TEIL I

Zero Trust Security

Zero Trust ist eine Sicherheitsphilosophie und ein Satz von Prinzipien, die zusammen eine bedeutende Veränderung darstellen, wie Unternehmens-IT und Sicherheit angegangen werden sollten. Die Ergebnisse können enorm vorteilhaft für Sicherheitsteams und für Unternehmen sein, aber Zero Trust ist breit gefächert und kann überwältigend sein. Im Teil I dieses Buches werden wir Ihnen eine historische und grundlegende Einführung in Zero Trust geben, erklären, was es ist (und was es nicht ist), und Zero Trust-Architekturen in Theorie und Praxis darstellen. Dies wird Ihnen helfen, Zero Trust Stück für Stück zu verstehen und darüber nachzudenken, wie es angewendet werden kann, um die Sicherheit, Widerstandsfähigkeit und Effizienz Ihrer Organisation zu verbessern.

KAPITEL 1

Einführung

Unternehmenssicherheit ist schwierig. Dies liegt an der Komplexität von IT- und Anwendungsinfrastrukturen, der Breite und Geschwindigkeit des Benutzerzugriffs und natürlich der inhärent adversen Natur der Informationssicherheit. Es liegt auch an der allzu offenen Natur der meisten Unternehmensnetzwerke – indem sie das Prinzip der geringsten Privilegien sowohl auf Netzwerk- als auch auf Anwendungsebene nicht durchsetzen, machen sich Organisationen unglaublich anfällig für Angriffe. Dies gilt sowohl für interne Netzwerke als auch für öffentliche, dem Internet zugewandte Remote-Zugangsdienste wie Virtual Private Networks (VPNs). Die letzteren sind jedem Gegner im Internet ausgesetzt. Angesichts der heutigen Bedrohungslandschaft würden Sie niemals ein System auf diese Weise entwerfen. Und doch perpetuieren traditionelle Sicherheits- und Netzwerksysteme, die nach wie vor weit verbreitet sind, dieses Modell.

Zero Trust-Sicherheit, das Thema dieses Buches, ändert dies und bringt einen modernen Ansatz zur Sicherheit, der das Prinzip der geringsten Privilegien für Netzwerke und Anwendungen durchsetzt. Nicht autorisierte Benutzer und Systeme haben überhaupt keinen Zugriff auf Unternehmensressourcen, und autorisierte Benutzer haben nur den minimal notwendigen Zugriff. Das Ergebnis ist, dass Unternehmen sicherer, geschützter und widerstandsfähiger sind. Zero Trust bringt auch Verbesserungen in Effizienz und Effektivität durch die automatisierte Durchsetzung dynamischer und identitätszentrierter Zugriffsrichtlinien.

Bitte beachten Sie, dass das „Zero“ in Zero Trust ein wenig irreführend ist – es geht nicht buchstäblich um „null“ Vertrauen, sondern um null *inhärentes* oder *implizites*Vertrauen. Zero Trust geht darum, sorgfältig eine Vertrauensbasis aufzubauen und dieses Vertrauen zu erweitern, um letztendlich ein angemessenes Zugriffsniveau zur richtigen Zeit zu ermöglichen. Es hätte vielleicht „verdientes Vertrauen“ oder „adaptives Vertrauen“ oder „null implizites Vertrauen“ genannt werden können, und diese hätten der Bewegung besser entsprochen, aber „Zero Trust“ hat mehr Pep, und es hat sich durchgesetzt. Bitte nehmen Sie das „Zero“ nicht wörtlich!

J. Garbis und J. W. Chapman, *Zero Trust Sicherheit*, https://doi.org/10.1007/979-8-8688-0105-1_1

Zero Trust ist ein wichtiger und sehr sichtbarer Trend in der Informationssicherheitsbranche, und obwohl es zu einem Marketing-Buzzword geworden ist, glauben wir, dass dahinter echte Substanz und Wert stecken. Im Kern ist Zero Trust eine Philosophie und ein Ansatz sowie eine Reihe von Leitprinzipien. Das bedeutet, dass es so viele Möglichkeiten gibt, Zero Trust zu interpretieren, wie es Unternehmen gibt. Es gibt jedoch grundlegende und universelle Prinzipien, denen jede Zero Trust-Architektur folgen wird. In diesem Buch werden wir Richtlinien und Empfehlungen für Zero Trust auf der Grundlage unserer Erfahrungen mit Unternehmen verschiedener Größen und Reifegrade auf ihrem Weg zu Zero Trust geben. Denken Sie daran, wir verwenden das Wort *Reise* absichtlich; dies soll unterstreichen, dass es sich nicht um ein einmaliges Projekt handelt, sondern um eine fortlaufende und sich entwickelnde Initiative. Und deshalb haben wir dieses Buch geschrieben – um unsere Gedanken und Empfehlungen darüber zu teilen, wie Sie Zero Trust in Ihrer Umgebung am besten angehen können und um Sie auf Ihrer Reise zu begleiten.

Wir glauben grundsätzlich, dass Zero Trust ein besserer und effektiverer Weg ist, um Unternehmenssicherheit zu erreichen. In gewisser Weise wurde Zero Trust eng mit Netzwerksicherheit in Verbindung gebracht, und obwohl Netzwerke ein Kernbestandteil von Zero Trust sind, werden wir auch die volle Breite der Zero Trust-Sicherheit erforschen, die Grenzen in Anwendungen, Daten, Identitäten, Operationen und Richtlinien überschreitet.

Als Sicherheitsleiter haben Sie die Verantwortung, Ihre Organisation dazu zu drängen, zu ziehen und zu stoßen, diesen neuen Ansatz zu übernehmen, der die Widerstandsfähigkeit Ihrer Organisation verbessern und Ihnen auch helfen wird, professionell zu wachsen. Dieses Buch – Ihr Leitfaden – ist in drei Teile gegliedert. Teil I bietet eine Einführung in die Zero Trust-Prinzipien und legt den Rahmen und das Vokabular fest, die wir verwenden werden, um Zero Trust zu definieren und IT- und Sicherheitsinfrastruktur auszurichten. Dies sind die Grundlagen dessen, was wir für notwendig halten, um die vollständige Zero Trust-Geschichte zu erzählen.

Teil II ist ein tiefer Einblick in IT- und Sicherheitstechnologien und ihre Beziehung zu Zero Trust. Hier beginnen Sie zu sehen, wie Ihre Organisation Zero Trust nutzen kann und wo Sie Ihre aktuelle IT- und Sicherheitsinfrastruktur in eine modernere Architektur integrieren können. Da Zero Trust einen identitätszentrierten Ansatz zur Sicherheit verfolgt, werden wir untersuchen, wie verschiedene Technologien beginnen können, von Identitätskontexten zu profitieren und effektiver zu werden.

Teil III bringt alles zusammen und baut auf den ersten beiden Teilen des Buches auf, die eine konzeptionelle Grundlage und eine tiefe Technologiediskussion lieferten. Dieser Teil untersucht, wie ein Zero Trust-Richtlinienmodell aussehen sollte, untersucht spezifische Zero Trust-Szenarien (Anwendungsfälle) und diskutiert schließlich einen strategischen und taktischen Ansatz, um Zero Trust erfolgreich zu machen.

Es ist auch wichtig zu beachten, dass wir uns bewusst dafür entschieden haben, Anbieter oder Anbieterprodukte im Rahmen dieses Buches nicht zu bewerten. Unsere Branche bewegt sich zu schnell – das Innovationstempo ist hoch – und solche Bewertungen hätten eine sehr kurze Haltbarkeit. Stattdessen konzentrieren wir uns auf die Erforschung architektonischer Prinzipien, aus denen Sie Anforderungen ableiten können und die Sie zur Bewertung von Anbietern, Plattformen, Lösungsanbietern und Ansätzen verwenden können.

Wenn Sie das Ende dieses Buches erreichen, sollte klar sein, dass es keinen einzig richtigen Ansatz für Zero Trust gibt. Sicherheitsleiter müssen bestehende Infrastrukturen, Prioritäten, Mitarbeiterfähigkeiten, Budgets und Zeitpläne berücksichtigen, während sie ihre Zero Trust-Initiative entwerfen. Dies mag Zero Trust kompliziert erscheinen lassen, aber seine Breite des Anwendungsbereichs hilft tatsächlich, Unternehmenssicherheit und Architektur zu vereinfachen. Als Overlay-Sicherheits- und Zugriffsmodell normalisiert es Dinge und gibt Ihnen eine zentralisierte Möglichkeit, Zugriffsrichtlinien in einer verteilten und heterogenen Infrastruktur zu definieren und durchzusetzen.

Letztendlich ist das Ziel dieses Buches, Ihnen ein solides Verständnis dessen zu vermitteln, was Zero Trust ist, und das Wissen, um die einzigartige Reise Ihrer Organisation zu Zero Trust erfolgreich zu steuern. Wenn Sie dies erreichen, waren unsere Bemühungen erfolgreich. Lassen Sie uns unsere Reise beginnen.

KAPITEL 2

Was ist ZeroTrust?

In diesem Kapitel werden wir Zero Trust als Konzept, Philosophie und Rahmenwerk einführen. Neben einem kurzen Überblick über die Geschichte und Entwicklung von Zero Trust werden wir auch einige Leitprinzipien vorstellen. Wir glauben, dass es *kern* und *erweiterte* Prinzipien gibt, die für jede Zero Trust-Initiative gemeinsam sind und die wichtig zu verstehen sind, wenn Sie Ihre Reise beginnen. Unser Ziel für dieses Kapitel ist es, Ihnen eine Arbeitsdefinition von Zero Trust auf der Grundlage dieser Prinzipien zu geben und einen Satz grundlegender Plattformanforderungen bereitzustellen.

Geschichte und Entwicklung

Traditionell wurden Sicherheitsgrenzen am Rand des Unternehmensnetzwerks in einem klassischen „Burgmauer und Graben"-Ansatz platziert. Mit der Entwicklung der Technologie wurden jedoch Remote-Mitarbeiter und Remote-Workloads immer häufiger. Sicherheitsgrenzen folgten notwendigerweise und erweiterten sich von nur dem Unternehmensperimeter auf die Geräte und Netzwerke, mit denen der Remote-Benutzer verbunden war, und die Ressourcen, mit denen sie sich verbanden. Dies zwang Sicherheits- und Netzwerkteams, diese Geschäftsanforderungen zu berücksichtigen und die Modelle anzupassen, nach denen Organisationen Sicherheit und Zugang anwendeten, mit gemischtem Erfolg.[1]

Im Jahr 2010 führte Forrester-Analyst John Kindervag den Begriff "Zero Trust" in dem einflussreichen Weißbuch "No More Chewy Centers: Introducing The Zero Trust

[1]Wir versuchen, mit dieser Aussage diplomatisch zu sein. Es ist eine unbestreitbare Tatsache, dass die Sicherheit von Unternehmensnetzwerken und Daten als Branche es nicht geschafft hat, unsere Organisationen effektiv vor Datenverlust und Systemverletzungen zu schützen. Zugegeben, wir stehen ausgeklügelten und motivierten Gegnern gegenüber, aber wir glauben, dass dieses weit verbreitete Versagen hauptsächlich auf die Mängel traditioneller Infosec-Tools und -Ansätze zurückzuführen ist und dass Zero Trust weitaus effektiver sein wird.

J. Garbis und J. W. Chapman, *Zero Trust Sicherheit*, https://doi.org/10.1007/979-8-8688-0105-1_2

Model Of Information Security"[2] ein. Dieses Papier fasste Ideen zusammen, die in der Branche seit einigen Jahren diskutiert wurden, insbesondere vom Jericho Forum gefördert. Das Forrester-Dokument beschrieb den Wandel weg von einem harten Perimeter und hin zu einem Ansatz, der erforderte, Elemente innerhalb eines Netzwerks zu inspizieren und zu verstehen, bevor sie ein Vertrauens- und Zugangsniveau verdienen konnten. Im Laufe der Zeit entwickelte Forrester dieses Konzept zu dem, was heute als *Zero Trust eXtended* (ZTX) Framework bekannt ist, das Daten, Workloads und Identität als Kernkomponenten von Zero Trust umfasst.

Zur gleichen Zeit begann Google ihre interne BeyondCorp-Initiative, die eine Version von Zero Trust implementierte und grundlegende Zero Trust-Elemente einführte, die effektiv ihre Unternehmensnetzwerkgrenze entfernten. Seit 2014 beeinflusste Google die Branche stark mit einer Reihe von Artikeln, die ihre bahnbrechende interne Implementierung dokumentierten. Ebenfalls im Jahr 2014 stellte die Cloud Security Alliance die Software Defined Perimeter (SDP) Architektur vor, die eine konkrete Spezifikation für ein Sicherheitssystem lieferte, das Zero Trust-Prinzipien unterstützt.[3] Wir werden sowohl BeyondCorp als auch SDP später im Kap. 4 durch die Linse von Zero Trust betrachten.

Im Jahr 2017 überarbeitete das Branchenanalystenunternehmen Gartner ihr Continuous Adaptive Risk and Trust Assessment (CARTA) Konzept, das viele Prinzipien mit Zero Trust gemeinsam hat. CARTA bietet nicht nur Identitäts- und Datenelemente, sondern beinhaltet auch Risiko- und Haltungselemente, die mit Identität und Geräten verbunden sind, die auf die Umgebung zugreifen.

Die branchenweite Betonung von Zero Trust setzte sich fort, als das US National Institute of Standards and Technology (NIST) eine Zero Trust Architecture-Publikation[4] und ein zugehöriges US National Cybersecurity Center of Excellence-Projekt im Jahr 2020 veröffentlichte.[5]

Zero Trust entwickelt sich weiter, da Anbieter und Normungsorganisationen Spezifikationen und Implementierungen von Zero Trust überprüfen und verfeinern und

[2]Forrester, "No More Chewy Centers: Introducing The Zero Trust Model Of Information Security", September 2010.

[3]Siehe den CSA's Architecture Guide für SDP, https://cloudsecurityalliance.org/artifacts/sdp-architecture-guide-v2/.

[4]NIST Special Publication 800.207—Zero Trust Architecture, https://csrc.nist.gov/publications/detail/sp/800-207/final, August 2020.

[5]https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture.

es als grundlegende Veränderung im Ansatz zur Informationssicherheit anerkennen. Letztendlich hat die Branche zugestimmt, dass diese Änderungen und Verfeinerungen notwendig sind, um zu verhindern, dass böswillige Akteure auf private Ressourcen innerhalb organisatorischer Grenzen zugreifen, Daten exfiltrieren und den Betrieb stören.

Wir, die Autoren dieses Buches, arbeiten in der Informationssicherheitsbranche und verbringen beide viel Zeit damit, mit Sicherheitsfachleuten über Zero Trust zu sprechen. Eine häufig gestellte Frage, die wir hören, ist: „Was ist neu an Zero Trust – wie unterscheidet es sich von dem, was bereits getan wurde?“ Es ist definitiv wahr, dass einige Elemente von Zero Trust, wie *Zugriff mit minimalen Privilegien* und *rollenbasierte Zugriffskontrolle* Prinzipien sind, die in der aktuellen Netzwerk- und Sicherheitsinfrastruktur häufig implementiert werden (und in Zero Trust-Umgebungen genutzt werden müssen), aber allein vervollständigen sie das Bild nicht.

Grundlegende Sicherheitselemente, die vor Zero Trust verwendet wurden, erreichten oft nur eine grobe Trennung von Benutzern, Netzwerken und Anwendungen. Zum Beispiel sind in den meisten Organisationen Entwicklungsumgebungen von Produktionsumgebungen getrennt. Zero Trust verstärkt dies jedoch, indem es effektiv verlangt, dass alle Identitäten und Ressourcen voneinander getrennt werden. Zero Trust ermöglicht feinkörnige, identitäts- und kontextsensitive Zugriffskontrollen, die von einer automatisierten Plattform gesteuert werden. Obwohl Zero Trust als ein eng fokussierter Ansatz begann, Netzwerkidentitäten nicht zu vertrauen, bis sie authentifiziert und autorisiert waren, hat es sich zu Recht zu einem viel breiteren Satz von Sicherheitsfähigkeiten in der Umgebung einer Organisation entwickelt.

Lassen Sie uns kurz die Zero Trust-Modelle von Forrester und Gartner betrachten, bevor wir das, was wir für die Schlüsselprinzipien von Zero Trust halten, vorstellen.

Forresters Zero Trust eXtended (ZTX) Modell

Forrester veröffentlichte ihr anfängliches Zero Trust-Modell im Jahr 2010, und in den folgenden Jahren wurde es überarbeitet und erneut als *Zero Trust eXtended* (ZTX) veröffentlicht. ZTX bietet reichhaltigeren Inhalt und ein ausgewogenes Modell, das Daten in den Mittelpunkt stellt, wie in Abb. 2-1 gezeigt. Dies spiegelt Forresters Überzeugung wider, dass die Datenexplosion sowohl in On-Prem- als auch in Cloud-Umgebungen im Zentrum dessen steht, was geschützt werden muss. Die umgebenden

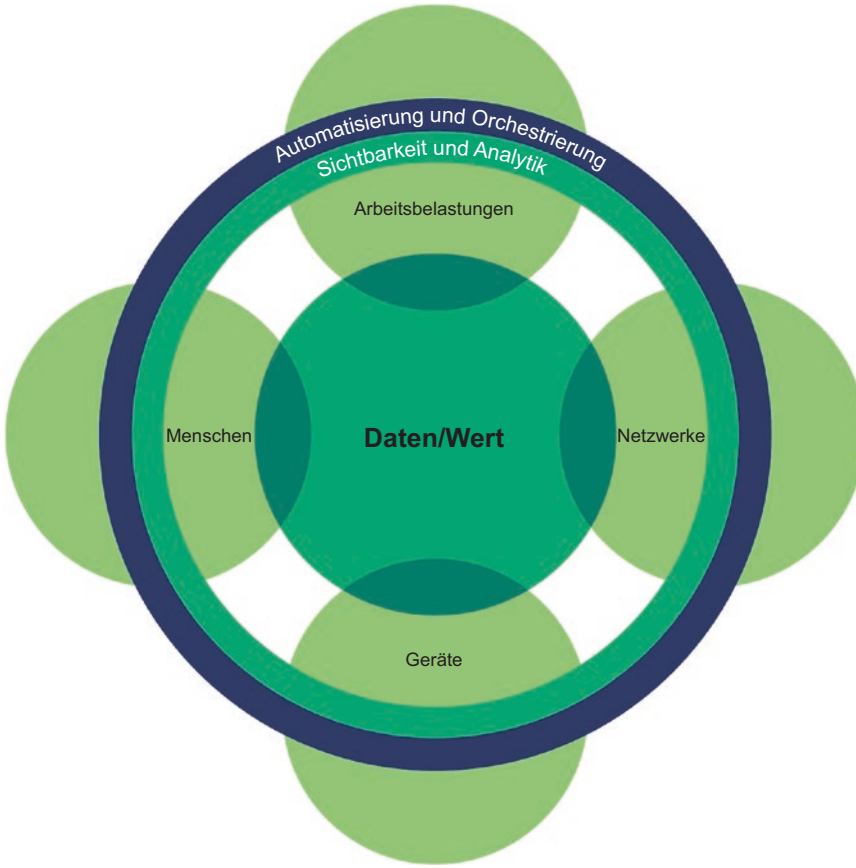

Abb. 2-1. *Forrester Zero Trust eXtended Modell. (Quelle: The Zero Trust eXtended Ecosystem: Data, Forrester Research, Inc., 11. August 2020)*

Elemente – Workloads, Netzwerke, Geräte und Menschen – sind Datenkanäle und müssen daher ebenfalls geschützt werden. Lassen Sie uns nun jedes dieser Elemente einzeln betrachten.

> Daten: *Daten* (die Forrester auch als „Wert" kennzeichnet, um ihre Bedeutung zu unterstreichen[6]) steht im Zentrum des ZTX-Modells und es beinhaltet Datenklassifizierung und -schutz als

[6]Tatsächlich sagt Forrester: „In Wahrheit ist das, was wir ausschließlich als ‚Daten' betrachtet haben, jetzt wirklich ‚Wert'. Was immer für Ihr Unternehmen von Wert ist, ist das wichtigste Gut, auf das Sie Ihre Verteidigung konzentrieren sollten, und Sie sollten diesen Wert um jeden Preis verteidigen", The Zero Trust eXtended Ecosystem: Data, Forrester Research, Inc., 11. August 2020.

Kernanforderungen zur Unterstützung des Zero Trust Modells. Im gesamten Buch betrachten wir Daten als Element der *Ressourcen*, die Zero Trust-Systeme schützen müssen. Darüber hinaus sollte Datenverlustprävention (DLP) Teil einer Zero Trust-Architektur sein und in das Richtlinienmodell eingebunden sein, mit der Möglichkeit, kontextbezogene Zugriffsrichtlinien zu erzwingen, wo immer dies möglich ist.

Netzwerke: Die *Netzwerk*-Säule des ZTX-Modells konzentriert sich hauptsächlich auf Netzwerksegmentierung – sowohl aus Benutzer- als auch aus Serverperspektive – um eine bessere Sicherheit auf der Grundlage identitätszentrierter Attribute zu gewährleisten. Es ist wichtig zu erkennen, dass Unternehmen viele bestehende Komponenten haben, die die traditionelle Netzwerksicherheitsinfrastruktur ausmachen, wie zum Beispiel Next-Generation Firewalls (NGFWs),Web Application Firewalls (WAF),Network Access Control (NAC) Lösungen und Intrusion Protection Systems (IPS). Diese Komponenten haben in der Regel alle eine Rolle in einem Zero Trust-System zu spielen. Wir werden diese Komponenten in einer repräsentativen Unternehmensarchitektur in Kap. 3 vorstellen und ihre Beziehung zu Zero Trust ausführlich in Teil II des Buches untersuchen.

Menschen: Die *Menschen*-Säule des ZTX-Modells muss mehrere Elemente des Identity and Access Managements (IAM) umfassen. Rollen- und attributbasierte Zugriffskontrolle (RBAC und ABAC) sind gut verstandene Modelle innerhalb von IAM, und Zero Trust ermöglicht die breitere und effektivere Nutzung dieser Modelle in der gesamten Unternehmensinfrastruktur. Multi-Faktor-Authentifizierung (MFA) ist eine weitere Anforderung und ist wesentlich zur Unterstützung von Zero Trust. Schließlich ist Single Sign On (SSO) – unter Verwendung moderner, offener Standards wie OAuth und SAML – ein weiteres Kernelement innerhalb der Menschen-Säule. Wie Sie im Laufe dieses Buches sehen werden, sind wir starke Befürworter davon, die Identität in jeder Zero Trust-Umgebung zentral zu machen.

Workloads: *Workloads,* wie von Forrester definiert, bestehen aus den Komponenten, die die logischen Funktionen bilden, die das Geschäft sowohl in kundenorientierten als auch in Backend-Geschäftssystemen antreiben – Container, Anwendungen, Infrastruktur, Prozesse usw. Zero Trust erfordert Metadaten-gesteuerte Workload-Zugriffskontrollen, die konsistent in hybriden Umgebungen durchgesetzt werden. Wir werden dies weiter in Kap. 17 untersuchen.

Geräte: Das Sicherheitsmodell für *Geräte* sollte die Identität, das Inventar, die Isolation, die Sicherheit und die Kontrolle des Geräts umfassen. In Kap. 3 werden wir Benutzeragenten beschreiben, die auf Geräten laufen, und wie sie für die Zero Trust-Umgebung von zentraler Bedeutung sind. Wir werden auch später, in Kap. 4, die Wege sehen, auf denen Geräte für Googles BeyondCorp-Implementierung von zentraler Bedeutung waren.

Sichtbarkeit und Analytik: *Sichtbarkeit und Analytik* innerhalb von ZTX ist der Verbrauch und die Darstellung von Daten im gesamten Unternehmen zur Unterstützung informierter Sicherheitsentscheidungen auf der Grundlage von Kontextinformationen. Wir stimmen zu, dass dies entscheidend ist, insbesondere die Konsolidierung von Daten aus mehreren unterschiedlichen Quellen. Es gibt heute keine einzige Plattform, die die notwendige Funktionsbreite abdeckt, aber dies ist ein sich entwickelnder Bereich. Wir werden dies weiter in Kap. 11 diskutieren.

Automatisierung und Orchestrierung: *Automatisierung und Orchestrierung* innerhalb von ZTX sind erforderlich, um manuelle Prozesse zu automatisieren und sie mit Sicherheitsrichtlinien und Maßnahmen zur Reaktion in Beziehung zu setzen. Wir glauben, dass dieses Element entscheidend für den Erfolg einer Zero Trust-Plattform ist – Zero Trust ist von Natur aus dynamisch und anpassungsfähig, und der einzige Weg, dies zu erreichen, ist mit Automatisierung und Orchestrierung, über die gesamte

Unternehmensumgebung hinweg. Wir werden dies weiter in der Folge diskutieren, da Automatisierung eines unserer Schlüsselprinzipien von Zero Trust Prinzipien ist.

Gartners Ansatz zu Zero Trust

Gartner hat Zero Trust durch ein Modell angegangen, das sie CARTA nennen – Kontinuierliche Adaptive Risiko- und Vertrauensbewertung. Die Prämisse von CARTA besteht darin, eine kontinuierliche Risikobewertung in Bezug auf Benutzer, Geräte, Anwendungen, Daten und Arbeitslasten aus der Perspektive von *Vorhersagen, Verhindern, Erkennen und Reagieren* bereitzustellen.

CARTA verwendet den grundlegenden Prozess des *Implementieren einer Sicherheitsposition, Überwachen der Position* und *Anpassen der Sicherheitsposition* durch verschiedene Sicherheitsebenen. Gartner ist der Ansicht, dass diese Prinzipien im gesamten Unternehmen durchgesetzt werden sollten und Sicherheits-, Richtlinien- und Compliance-Anforderungen einschließen sollten.

Gartner neigt dazu, Zero Trust etwas enger zu sehen und verwendet die Begriffe *Zero Trust Network Access*(ZTNA) für die Benutzer-zu-Server-Sicherheit und *Zero Trust Network Segmentation* (ZTNS) für die Mikrosegmentierung/Server-zu-Server-Sicherheit. Ihr gesamtes Sicherheitsframework basiert auf *CARTA*, und seine Prinzipien stimmen gut mit denen überein, die wir hier vertreten. Letztendlich spielt es keine Rolle, ob Ihre strategische Initiative *Zero Trust, CARTA, Earned Trust* oder etwas anderes heißt.[7] Die Prinzipien und Ziele von Gartners CARTA sind solide und wir glauben, dass sie mit denen übereinstimmen, die wir in diesem Buch untersuchen.

Unsere Perspektive auf Zero Trust

Zero Trust ist ein ganzheitliches Modell zur Sicherung von Netzwerk-, Anwendungs- und Datenressourcen, mit einem Fokus auf die Bereitstellung eines identitätszentrierten Richtlinienmodells zur Kontrolle des Zugriffs. Alle Unternehmen verfügen über eine

[7]Tatsächlich haben wir mit mehreren Unternehmen gesprochen, die bewusst den Begriff "Zero Trust" intern vermeiden. Sie glauben, dass er etwas irreführend ist und von Endbenutzern möglicherweise negativ als Botschaft des Sicherheitsteams interpretiert wird, dass "wir Ihnen nicht vertrauen".

Reihe von IT- und Sicherheitstools in ihrer Umgebung, aber Zero Trust verlangt, dass sie ganzheitlich betrachtet und betrieben werden, mit der Identität im Kern und mit der Fähigkeit, attribut- und kontextsensitive Richtlinien in der gesamten Umgebung durchzusetzen. Dies sollte klar werden, wenn wir als nächstes die zugrunde liegenden Prinzipien von Zero Trust untersuchen, die wir in *Kern* und *Erweiterte* Prinzipien gruppiert haben.

Kernprinzipien

In der gesamten Branche gibt es drei grundlegende Zero Trust Prinzipien, die allgemein als grundlegend und wesentlich anerkannt sind. Diese wurden ursprünglich in dem von Forrester veröffentlichten Papier "No More Chewy Centers" definiert, und wir glauben, dass sie in jeder Zero Trust Implementierung gelten müssen. Zusätzlich zu diesen Kernprinzipien haben wir die Grundsätze aus dem NIST Zero Trust Architecture Dokument aufgenommen. Wir geben hier unsere Interpretation aus der aktuellen Branchensicht.

Stellen Sie sicher, dass alle Ressourcen sicher abgerufen werden, unabhängig von ihrem Standort.

Dies ist eine kraftvolle, kompakte Aussage, die mehrere Dimensionen umfasst. Erstens erfordert sie, dass *alle* Ressourcen in den Geltungsbereich einer Zero Trust Lösung einbezogen werden. Implizit fordert dies von Organisationen einen ganzheitlichen Ansatz mit Zero Trust und dass sie Silos und Barrieren abbauen sollten, die historisch zwischen Sicherheitstools und -teams bestanden haben.

Zweitens erfordert dieses Prinzip, dass Zero Trust den Zugriff aller Identitäten (menschlich und maschinell) auf alle Ressourcen (Daten, Anwendungen, Server) sichert – unabhängig vom Standort der Identität und unabhängig vom Standort oder der Technologie der abgerufenen Ressource. Es ist dieses Prinzip, das effektiv die Auflösung des traditionellen Unternehmensperimeters und seine Ersetzung durch ein alternatives Sicherheitsparadigma erzwingt. Es bedeutet auch, dass nicht nur der Netzwerkverkehr verschlüsselt sein muss, wenn er ungesicherte Netzwerkbereiche durchquert[8] , sondern

[8]Im Kap. 3 werden wir das Konzept einer impliziten Netzwerk-Vertrauenszone einführen, die ein Nebenprodukt bestimmter Zero Trust Implementierungsmodelle ist. Verschlüsselte Anwendungsprotokolle werden das Risiko solcher Zonen reduzieren.

dass der gesamte Zugriff einem durchgesetzten Richtlinienmodell unterliegen muss – das ist das Thema des zweiten Prinzips.

Verfolgen Sie eine Strategie der minimalen Berechtigungen und setzen Sie den Zugriffskontrolle strikt durch.

Das Konzept des Zugriffs mit minimalen Berechtigungen auf Ressourcen ist nicht neu, aber es war schwierig, es vor Zero Trust breit durchzusetzen. Minimale Berechtigungen müssen konsistent über Standorte und Ressourcentypen hinweg und sowohl auf Netzwerk- als auch auf Anwendungsebene verwaltet werden, unter Verwendung von Sicherheits- und Identitätskontext.

Historisch gesehen waren Sicherheitslösungen nicht in der Lage, die Diskrepanz zwischen Netzwerk- und Anwendungssicherheit zu überbrücken. Traditionell erhielten Benutzer (und ihre Geräte) weitreichenden Zugriff auf Netzwerke, und Anwendungen stützten sich auf Zugriffskontrollen, die nur auf Authentifizierung basierten. Jeder im Unternehmen konnte auf die Anmeldeseite auf dem Finanzserver zugreifen, aber nur Finanzbenutzer hatten Konten und Passwörter. Dies ist kein ausreichendes Sicherheitsniveau mehr. Es gibt viel zu viele bekannte und kritische Schwachstellen, die keine Authentifizierung erfordern und aus der Ferne ausgenutzt werden können. Wir sagen dies laut und deutlich – die Fähigkeit, Netzwerkpakete an ein System zu senden, ist ein Privileg und muss als solches verwaltet werden. Wenn Benutzer nicht berechtigt sind, auf einen bestimmten Dienst zuzugreifen (z. B. haben sie Anmeldeinformationen, um sich per SSH in einen Server einzuloggen, oder sich an einem VPN zu authentifizieren), dürfen sie nicht die Möglichkeit haben, sich auf Netzwerkebene mit diesem Dienst zu verbinden.

Überprüfen und protokollieren Sie allen Verkehr.

Netzwerke stellen einen besonders interessanten Ort in der Sicherheits- und IT-Infrastruktur dar, da sie das Mittel sind, mit dem verteilte Komponenten sich verbinden und miteinander kommunizieren. Aus diesem Grund erfordert das letzte Kernprinzip die Überprüfung und Protokollierung des Netzwerkverkehrs. Zero Trust Systeme sind dafür gut geeignet – wie wir in Kap. 3 sehen werden, bestehen sie typischerweise aus einem verteilten Satz von Netzwerkdurchsetzungspunkten. Es ist wichtig zu beachten, dass Zero Trust Systeme den Netzwerkverkehrsmetadaten weitgehend untersuchen und protokollieren sollten, aber bei der Überprüfung des Netzwerkverkehrsinhalts aufgrund von Verarbeitungs- und Speicherkosten vorsichtiger sein sollten. (Wir werden dies in Kap. 8 weiter besprechen).

Die Informationen über den Netzwerkverkehr sollten durch das Zero Trust System angereichert werden – durch Hinzufügen von Identitäts- und Gerätekontext – und in Next-Generation Firewalls, Netzwerküberwachungstools und SIEMs eingespeist werden, um deren Fähigkeit zur Entscheidungsfindung, zur Erkennung, zum Alarmieren und zum Reagieren zu verbessern, sowie zur Unterstützung von Incident Response und anderen Alarmmechanismen.

Erweiterte Prinzipien

Zusätzlich zu den grundlegenden Zero Trust-Prinzipien, die wir diskutiert haben, glauben wir, dass es drei weitere Prinzipien gibt, die ebenso wichtig und notwendig in jeder Unternehmensklasse Zero Trust-Umgebung sind.

Stellen Sie sicher, dass alle Komponenten APIs, für Ereignis- und Datenaustausch, unterstützen.

Zero Trust muss eine ganzheitliche Sicherheitsrichtlinie und Durchsetzungsmodell bereitstellen, das weite Bereiche des IT-Ökosystems umfasst – was zum ersten Grundprinzip zurückführt. Daher muss es in der Lage sein, sich mit vielen (idealerweise allen) Komponenten dieses Ökosystems zu integrieren. Die Integration von zuvor isolierten Sicherheitsprodukten, Infrastrukturen und Geschäftssystemen ist unerlässlich. Wie Sie in unseren Diskussionen sehen werden, ermöglicht die Integration von Identitäts- und Sicherheitstools einen ganzheitlichen Sicherheitskontext, mit dem Zero Trust eine sicherere Umgebung bieten kann. Diese Integrationen werden sowohl zum Initiieren als auch zum Reagieren auf Ereignisse verwendet, sowie zum Austausch von Daten und Protokollinformationen und zur Aktivierung unseres nächsten Prinzips. Ein Korollar zu diesem Prinzip: Jede Sicherheits- und IT-Komponente, die in Ihre Zero Trust-Plattform integriert ist, erhöht ihren Wert, ihre Wirksamkeit und ihre Reichweite. Im Gegensatz dazu fügt jede isolierte (nicht integrierte) Komponente Reibung hinzu, verringert die Wirksamkeit Ihres Zero Trust-Systems und kann die Sicherheit behindern.

Automatisieren Sie Aktionen in Umgebungen und Systemen, die durch Kontext und Ereignisse gesteuert werden.

Automatisierung ist ein Schlüsselelement für eine erfolgreiche Zero Trust-Umgebung und notwendig für den Betrieb auch in kleinem Maßstab. Zero Trust basiert auf einem Satz dynamischer Zugriffskontrollregeln, die sich in Reaktion auf Identität, Gerät, Netzwerk und Systemkontext ändern. Wie wir in Kap. 3 sehen werden, erfordern

alle Zero Trust-Modelle einen zentralisierten Policy Decision Point (PDP) verbunden mit einem verteilten Satz von Policy Enforcement Points (PEPs) über einen logischen Steuerkanal. Dieser Kanal wird verwendet, um Änderungen an den durchgesetzten Richtlinien über Integration/APIs zu automatisieren und ist für ein Zero Trust-System unerlässlich.

Automatisierte Änderungen des Zugriffs können in einem Zero Trust-System viele Formen annehmen, einschließlich der Gewährung von Zugriff durch ein Identitätsmanagement-System, ein Zugriffsmanagement-System oder ein Netzwerkzugriffskontrollsystem. Andere automatisierte Aktivitäten könnten die vorübergehende oder dauerhafte Entfernung des Zugriffs auf eine bestimmte Ressource beinhalten, zum Beispiel getrieben durch ein Lebenszyklusmanagement-Ereignis oder eine Kontextänderung.

Beachten Sie, dass automatisierte Aktionen in einer Betriebsumgebung grundlegend sind, dies jedoch nicht die Möglichkeit ausschließt, manuelle Eingriffe zu nutzen oder explizite manuelle Schritte in einen Workflow vor der Initiierung einer automatisierten Antwort einzubeziehen. Das heißt, Automatisierung bedeutet nicht „automatisch". Zum Beispiel erfordern viele Zugriffsanforderungsprozesse eine Managergenehmigung, um Sicherheits- und Compliance-Richtlinien zu erfüllen. Dieser Workflow erfordert, dass ein Mensch einige Informationen liest, eine Entscheidung trifft und diese Entscheidung dem System übermittelt. Das sollte der einzige manuelle Schritt in diesem Prozess sein – der Rest des Workflows, einschließlich der Bereitstellung von Zugriffsänderungen, sollte automatisiert sein.

Liefern Sie taktischen und strategischen Wert.

Letztendlich müssen Kerninitiativen rund um Zero Trust an den Geschäftswert gebunden sein. Zero Trust-Projekte können (und tun dies in der Regel) erhebliche Auswirkungen auf Infrastrukturen, Teams, Betrieb und Benutzererfahrung haben. Die Ergebnisse sind positiv, aber dennoch sind Änderungen oft schwierig zu erreichen, technisch, kulturell und politisch. Und die Änderungen, die mit einem Zero Trust-Projekt verbunden sind, können weitreichend sein – es gibt viele Komponenten in Ihrer Umgebung, die geändert oder in Ihre Zero Trust-Umgebung als Durchsetzungspunkt oder Richtlinientreiber integriert werden.

Zero Trust ist eine Reise und eine Investition von Zeit und Geld. Ein Verständnis der Geschäftstreiber und Prioritäten Ihrer Organisation wird Ihnen helfen, Ihre strategische Vision für Zero Trust in Ihrer Unternehmensumgebung zu rechtfertigen und umzusetzen. Wenn Sie Ihre Reise beginnen, müssen inkrementelle Bereitstellungen und taktische

Siege realisiert werden. Dies wird Ihre Zero Trust-Reise vereinfachen und intern Momentum und Unterstützung aufbauen. Das heißt, indem Sie früh taktische Siege liefern – im Rahmen Ihrer strategischen Zero Trust-Architektur – ermöglichen Sie Ihrer Organisation, ihren vollen strategischen Wert zu realisieren. Jedes erfolgreiche neue Projekt eröffnet weitere Wege und baut Unterstützung für Ihre Zero Trust Initiative auf.

Eine Arbeitsdefinition

Während wir dieses Buch durchgehen und Konzepte von Zero Trust-Prinzipien, Architekturen und Arbeitsbeispielen einführen, ist es wichtig zu verstehen, was Zero Trust ist. Wir finden es nützlich, Zero Trust als Linse zu betrachten, durch die Sie Sicherheitsinitiativen und -komponenten betrachten und interpretieren können. Zu diesem Zweck schlagen wir die folgende prägnante Definition vor:

> *Ein Zero Trust-System ist eine integrierte Sicherheitsplattform, die Kontextinformationen aus Identität, Sicherheit und IT-Infrastruktur sowie Risiko- und Analysetools verwendet, um die dynamische Durchsetzung von Sicherheitsrichtlinien im gesamten Unternehmen zu informieren und zu ermöglichen. Zero Trust verschiebt die Sicherheit von einem ineffektiven, auf den Perimeter zentrierten Modell zu einem ressourcen- und identitätszentrierten Modell. Dadurch können Organisationen die Zugriffskontrollen kontinuierlich an eine sich ändernde Umgebung anpassen und verbesserte Sicherheit, reduziertes Risiko, vereinfachte und widerstandsfähige Operationen und erhöhte Geschäftsagilität erzielen.*

Diese Kerndefinition, zusätzlich zu den zuvor definierten Prinzipien, ermöglicht es uns, einen ersten Satz von Zero Trust-Anforderungen zu liefern, die wir als nächstes diskutieren.

Zero Trust Plattformanforderungen

In diesem Abschnitt stellen wir eine grundlegende Reihe von Plattformanforderungen vor, die aus den zuvor diskutierten Zero Trust-Prinzipien resultieren. Unser Ziel in diesem Abschnitt ist es nicht, die Prinzipien einfach neu zu formulieren, sondern relevante Aspekte aus einer Plattformperspektive zu beleuchten. Einige dieser Prinzipien (insbesondere APIs und Integration) lassen sich am besten als Anforderungen formulieren, die mit spezifischen IT- und Sicherheitsfunktionen verbunden sind, aber im Allgemeinen haben wir diese Anforderungen breit definiert:

1. Die Kommunikation auf der Datenebene muss verschlüsselt sein. Ausnahmen müssen bewusst sein (z. B. DNS).
2. Das System muss in der Lage sein, Zugriffskontrollen für alle Arten von Ressourcen durchzusetzen. Zugriffskontrollmechanismen müssen von identitätszentrierten und kontextbezogenen Richtlinien gesteuert werden.
3. Der Schutz von Datenressourcen sollte in der Lage sein, Identitäts- und Kontextrichtlinien zur Steuerung des Zugriffs zu verwenden.
4. System- und Richtlinienmodell müssen die Sicherung aller Benutzer an allen Standorten unterstützen. Das Richtlinienmodell und die Kontrollen müssen für Remote- und Vor-Ort-Benutzer konsistent sein.
5. Geräte müssen auf ihre Sicherheitslage und Konfiguration überprüft werden können, bevor ihnen Zugang gewährt wird, und danach regelmäßig.
6. Es muss möglich sein, BYOD von unternehmensverwalteten Geräten zu unterscheiden und das Zugriffsniveau entsprechend zu steuern.
7. Der Zugang zu jeder Netzwerkressource muss ausdrücklich durch eine Richtlinie gewährt werden. Kein Benutzer oder Gerät sollte grundsätzlich breiten Netzwerkzugang haben.
8. Zugriffskontrollen müssen in der Lage sein, zwischen verschiedenen Diensten auf der gleichen Netzwerkressource zu unterscheiden. Zum Beispiel muss der Zugang zu HTTPS getrennt vom Zugang zu SSH gewährt werden.
9. Der Zugang zu spezifischen Datenelementen innerhalb von Anwendungen oder Containern, die unterschiedliche Klassifizierungen haben, muss auf der Grundlage von Geschäfts-Richtlinien durchgesetzt werden.
10. Netzwerkverkehrs-Metadaten müssen protokolliert und mit Identitätskontext angereichert werden.

11. Netzwerkverkehr muss auf Sicherheit und Datenverlust überprüft werden können.
12. In die Cloud übertragene Workloads sollten die gleichen Zugriffskontrollrichtlinien enthalten wie von Vor-Ort-Lösungen definiert.
13. Die Automatisierung muss identitätszentrierte Details enthalten, um eine effiziente und effektive Vorfallreaktion zu ermöglichen.
14. Protokolle müssen in Analysetools enthalten sein, um eine effektive und dynamische Durchsetzung von Richtlinien zu ermöglichen.

Zusammenfassung

In diesem Kapitel haben wir die Geschichte von Zero Trust hervorgehoben, beginnend mit der Einführung des Begriffs durch Forrester im Jahr 2010, gefolgt von seiner kontinuierlichen Weiterentwicklung durch verschiedene Organisationen, einschließlich Google, NIST, CSA und anderen. Auf der Grundlage dieses historischen Hintergrunds haben wir drei Kernprinzipien von Zero Trust erklärt und verfeinert und drei erweiterte Prinzipien hinzugefügt. Zusammen genommen glauben wir, dass diese Reihe für jede Zero Trust-Initiative grundlegend sein sollte.

In unserem nächsten Kapitel werden wir ein repräsentatives Unternehmensarchitekturmodell vorstellen. Es wird nicht allumfassend sein, wird aber eine gemeinsame Basis bieten, um Zero Trust-Bereitstellungsmodelle einzuführen und zu zeigen, wie diese Modelle in das Unternehmen passen. Später, im Teil II des Buches, werden wir eine eingehende Untersuchung darüber anstellen, wie IT- und Sicherheitstechnologien von Zero Trust betroffen sind.

KAPITEL 3

Zero Trust Architekturen

Bisher haben wir die Geschichte von Zero Trust vorgestellt, unsere Sicht darauf gegeben und seine grundlegenden Prinzipien eingeführt. Zero Trust ist eine Philosophie, die viele verschiedene Arten von Architekturen (und viele, viele verschiedene Arten von kommerziellen Produkten) unterstützen kann. Es wird klar werden, dass es keine einzige richtige Architektur gibt und dass jede Organisation ihre eigenen spezifischen Anforderungen bewerten muss, um den richtigen Ansatz für ihre Reise zu Zero Trust sorgfältig zu entwickeln.[1]

Angesichts der Vielzahl von Ansätzen und der Einzigartigkeit des Ausgangspunkts jeder Organisation ist es nicht möglich, eine „Einheitsgröße" Zero Trust-Architektur zu erstellen. Dennoch haben wir uns dieser Herausforderung gestellt und nähern uns ihr, indem wir zwei Dinge tun. Erstens erstellen wir eine vereinfachte, aber repräsentative Unternehmensarchitektur, die wir in diesem Kapitel vorstellen und untersuchen werden. Diese Architektur soll ein typisches Unternehmen veranschaulichen, aber kein genaues oder detailliertes technisches Modell einer spezifischen Organisation oder eines Netzwerks sein. Ihr Ziel ist es, eine Architektur zu zeigen, die viele Elemente mit den meisten Organisationen gemeinsam hat, und die Verbindungen und Abhängigkeiten zwischen diesen verschiedenen Komponenten innerhalb eines einfachen visuellen Modells zu zeigen.

Nachdem wir die Unternehmensarchitektur vorgestellt haben, werden wir kurz jede der IT- und Sicherheitskomponenten erläutern, die in Gebrauch sind. Dies ermöglicht es uns, sie für unsere eingehende Untersuchung jeder einzelnen in Teil II des Buches vorzubereiten. Für jede werden wir untersuchen, wie sie sich auf eine Zero Trust-Architektur abbilden, mit ihr integrieren und aus der Perspektive einer Zero Trust-Architektur betrachtet werden sollten.

[1]Letztendlich ist das Ziel dieses Buches, Ihnen das Wissen zu vermitteln, genau das zu tun!

J. Garbis und J. W. Chapman, *Zero Trust Sicherheit*, https://doi.org/10.1007/979-8-8688-0105-1_3

Zweitens werden wir in diesem Kapitel ein konzeptionelles Modell einer Zero Trust-Architektur vorstellen. Dies ist auch eine Herausforderung, da es unterschiedliche Ansätze zu Zero Trust gibt, die von der zugrunde liegenden Unternehmensarchitektur und den Entscheidungen der Unternehmenssicherheitsarchitekten abhängen. Für unsere Zero Trust-Architektur werden wir mit der Zero Trust-Architektur des US National Institute of Standards and Technologies (NIST) aus der Special Publication 800-207 beginnen. Wir erweitern und verfeinern jedoch diese Architektur, um sie für Unternehmen relevanter zu machen und besser auf unseren Ansatz abzustimmen. Das heißt, wir werden diese architektonischen Konzepte im Laufe dieses Buches verwenden, um Zero Trust-Konzepte konkret und für Ihr Unternehmen nachvollziehbar zu machen.

Denken Sie so darüber nach – Ihr Unternehmensnetzwerk und Ihre Sicherheitsinfrastruktur haben viele Elemente wie Firewalls, NAC, IDS/IPS usw. Die meisten davon werden in einer Zero Trust-Architektur weiterhin existieren (obwohl einige vielleicht nicht). Aber in allen Fällen sollte die Art und Weise, wie Ihre Infrastrukturelemente konfiguriert und betrieben werden, mit Zero Trust ändern, was zu verbesserter Sicherheit und optimierten Abläufen führt. Lassen Sie uns beginnen, indem wir die Unternehmensarchitektur vorstellen.

Eine repräsentative Unternehmensarchitektur

Abb. 3-1 zeigt eine Unternehmensarchitektur, die die gängigsten IT- und Sicherheitsinfrastrukturelemente enthält und logische Verbindungen zwischen relevanten Netzwerkkomponenten darstellt. Zur Klarheit haben wir eine Menge Details aus diesem Diagramm weggelassen – wir werden jede der Komponenten sowie ihre Abhängigkeiten und Verbindungen in den relevanten Kapiteln in Teil II des Buches untersuchen. Für den Moment werden wir eine kurze Einführung in jedes der Elemente geben, seine Rolle in der Architektur hervorheben, wie unser fiktives Unternehmen es nutzt und wie sie es verbessern möchten.

Lassen Sie uns kurz die grafischen Elemente vorstellen, die wir im gesamten Buch verwenden: Logische Verbindungen zwischen Objekten werden mit einer gestrichelten Linie dargestellt. Eine sichere (verschlüsselte) Verbindung zwischen Objekten wird als fett gedruckte durchgehende Linie dargestellt. Eine durchgehende Linie (nicht fett gedruckt) repräsentiert den Datenfluss zwischen Objekten im Diagramm unter Verwendung nativer Anwendungsprotokolle (die verschlüsselt sein können oder nicht).

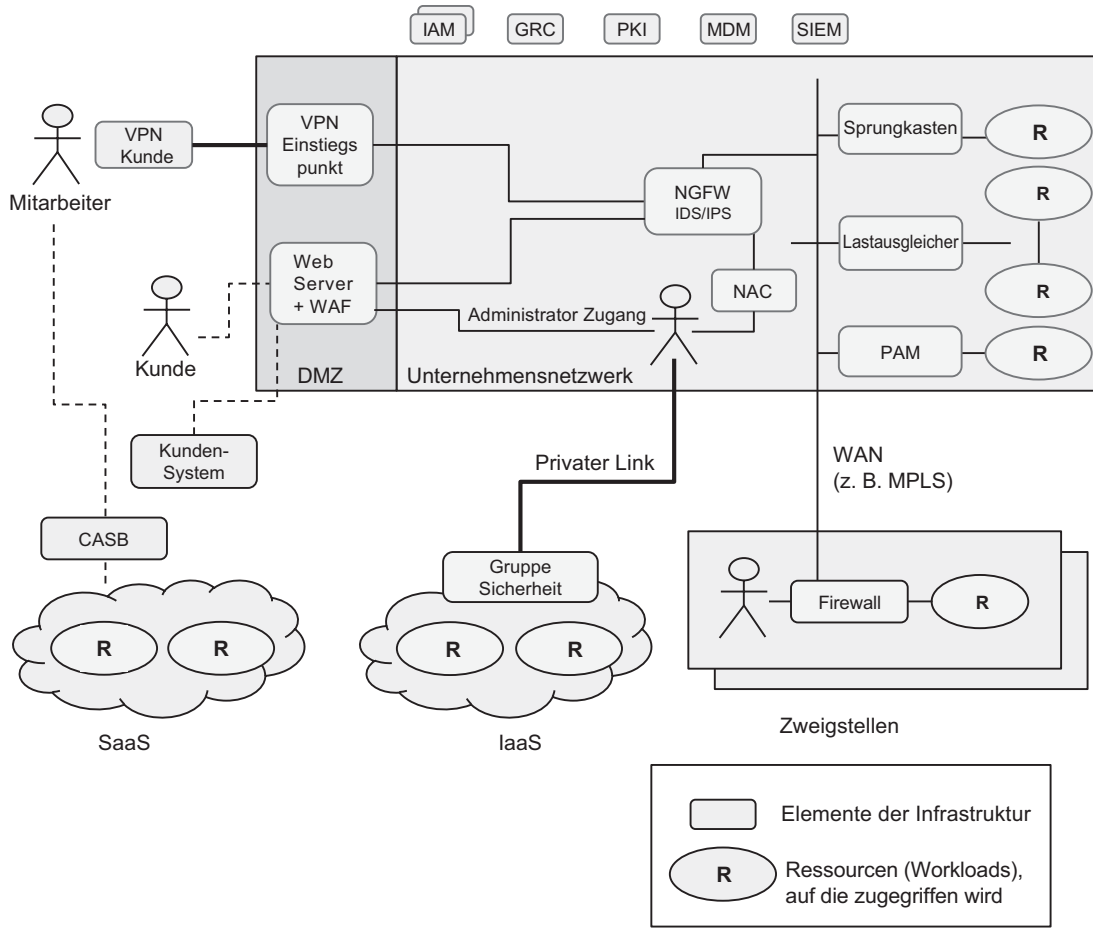

Abb. 3-1. *Eine repräsentative Unternehmensarchitektur*

Aufgerufene Ressourcen (Workloads, Dienste oder Daten) werden als „R“ dargestellt. Schließlich symbolisieren Ellipsen zwischen Ressourcen eine gemeinsame Gruppe von Ressourcen in einer Sammlung.

Das Unternehmen in unserer Architektur betreibt ein primäres Hauptquartier-Unternehmensnetzwerk und mehrere Niederlassungen. Diese physischen Standorte beherbergen jeweils eine Reihe von vernetzten Ressourcen (Workloads), auf die die Benutzer sicher zugreifen müssen, dargestellt als R. Dieses Unternehmen hat auch Workloads, die in privaten Netzwerken auf einem öffentlichen Infrastructure as a Service (IaaS) Anbieter laufen, sowie mehrere Software as a Service (SaaS) Ressourcen, auf die verschiedene Benutzergruppen zugreifen.

Wie die meisten Unternehmen hat auch dieses eine Vielzahl von Zugriffskontroll- und Netzwerkmechanismen verschiedener Art sowie ein Ökosystem von IT- und Sicherheitsinfrastrukturelementen. In den folgenden Abschnitten werden wir kurz diskutieren, warum und wie sie jedes dieser Elemente verwenden, sowie die Möglichkeiten, wie sie verbessert werden sollen.

Identitäts- und Zugriffsmanagement

Diese Organisation hat mehrere Identitätsanbieter, was heute ein häufiges Szenario für Unternehmen ist. In diesem Fall hat das Unternehmen ein primäres Identitäts- und Zugriffsmanagement (IAM) System, aber mehrere kleinere, die noch in Gebrauch sind, hauptsächlich als Ergebnis mehrerer Unternehmensübernahmen. Ihre IAM-Systeme werden verwendet, um Benutzer – hauptsächlich Mitarbeiter und einige Auftragnehmer – für Identität und Authentifizierung zu verwalten. Sie haben eine Mischung aus Multi-Faktor-Authentifizierung (MFA) Lösungen im Einsatz und ein grundlegendes Identitätsgovernance-Programm. Ihre jüngste Prüfung hat mehrere mittlere Prioritätsbefunde aufgedeckt, die sie beheben müssen.

Sie haben einen Plan, diese IAM-Systeme zu rationalisieren und zu zentralisieren, aber es gibt viele Abhängigkeiten, die diesen Prozess verlängert haben, einschließlich IAM-Integrationen mit Anwendungen, sowie automatisierte und manuelle Bereitstellungsprozesse. Welche Sicherheitsverbesserungen oder Änderungen sie auch vornehmen, sie müssen mit ihren bestehenden (unordentlichen) IAM-Infrastrukturen arbeiten – es ist nicht realistisch, darauf zu warten, dass sie zuerst rationalisiert oder zentralisiert werden.

Auch in ihrer aktuellen Situation haben sie eine gute Reihe von Rollen mit Rollbasierten Zugriffskontroll (RBAC) Tools und Prozessen implementiert, und sie möchten natürlich zusätzlichen Nutzen daraus ziehen. Ihre bestehende Sicherheitsinfrastruktur ist jedoch größtenteils nicht mit ihren IAM-Systemen integriert. Sie erkennen, dass dies eine Quelle von Reibung, Kosten, Ineffizienz und Ineffektivität ist – und es ist etwas, das sie verbessern möchten, wenn sie zu Zero Trust übergehen.

Netzwerkinfrastruktur (Firewalls, DNS, Load Balancer)

Dieses Unternehmen verfügt über eine recht typische Netzwerkinfrastruktur, einschließlich einer Vielzahl von traditionellen Firewalls und einem privaten DNS-Server zur Auflösung interner Server-Hostnamen. Sie nutzen auch verschiedene Arten von Load Balancern, einschließlich Netzwerk- und Anwendungs-Load-Balancern. Viele dieser Elemente sind seit Jahren im Einsatz und dienen dem Schutz von Diensten, der Segmentierung des Netzwerks und der Kontrolle des Zugriffs auf private Ressourcen.

Wie jedoch oft der Fall ist, haben diese Elemente und die Teams, die sie verwalten, Schwierigkeiten, mit den Veränderungen in der Art und Weise, wie Anwendungen (Workloads) entwickelt, bereitgestellt und abgerufen werden, Schritt zu halten. Insbesondere die Einführung dynamischerer (flüchtiger) Workloads in containerisierten oder virtualisierten Umgebungen vor Ort, gepaart mit einem Anstieg des Fernzugriffs, hat diese Lösungen insgesamt weniger effektiv gemacht. Im Grunde genommen sind sie gezwungen, zu breiten Netzwerkzugriff zu gewähren, da diese traditionellen Sicherheitstools – konzipiert und gebaut, um eine statischere und deterministischere IT-Infrastruktur[2] zu sichern – zunehmend nicht in der Lage sind, verschiedene Benutzer und verschiedene Ziel-Workloads richtig zu unterscheiden.

Dieser offene Netzwerkzugriff ist nun eine Priorität für sie, um ihn zu beseitigen – sie haben kürzlich einen Malware-Angriff erlitten, der sich weit im Netzwerk ausbreiten und eine erhebliche Anzahl von Systemen beeinträchtigen konnte. Sie suchen auch nach Zero Trust, um die Zugriffskontrollen in verschiedenen Teilen ihres Netzwerks besser aufeinander abzustimmen.

Jump Boxes

Dieses Unternehmen verwendet Jump Boxes (manchmal als Jump Hosts oder Jump Server bezeichnet) als gehärtete Zugangspunkte, um den Admin-Zugriff auf bestimmte hochwertige Assets im Netzwerk, wie Produktionssysteme und Backup-Systeme, zu kontrollieren, die auf einem separaten Netzwerksegment isoliert sind. Obwohl eine kürzliche Prüfung einige Sicherheitsprobleme mit ihren Jump Boxes identifizierte und

[2]Insbesondere beherbergen diese neuen Bereitstellungsmodelle nun mehrere Workloads, die unterschiedliche Zugriffskontrollen hinter einer einzigen, gemeinsam genutzten IP-Adresse erfordern. Ebenso scheinen entfernte Benutzer nun IP-Adressen zu teilen, aufgrund des NATting, das vom VPN-Gateway durchgeführt wird.

sie zwang, diese zu überwinden (z. B. gemeinsam genutzte Anmeldeinformationen und fehlende MFA), haben sie immer noch eine Reihe von Problemen, die sie angehen möchten.

Dazu gehören die Tatsache, dass die Jump Boxes vollen Netzwerkzugriff auf die hochwertigen Systeme haben, ihre Unfähigkeit, den gewünschten Geschäftsprozess (Anforderung und Genehmigung) für temporären Zugriff durchzusetzen, und ihre fehlende Integration mit Identitätssystemen. Sie möchten auch ihre Jump Boxes mit ihrem System für das Management privilegierter Zugriffe rationalisieren und abstimmen, das als nächstes diskutiert wird.

Management privilegierter Zugriffe

Dieses Unternehmen verwendet eine Lösung für das Management privilegierter Zugriffe (PAM) zur Unterstützung von Passwort-Tresoren und zur Bereitstellung von Sitzungsaufzeichnungen für den Zugriff auf mehrere hochwertige Systeme. Obwohl dies eine sichere Lösung zur Verschleierung von Passwörtern und zum sicheren Zugriff auf bestimmte Systeme innerhalb des Unternehmens bietet, wird PAM nur spärlich im gesamten Unternehmen eingesetzt, aufgrund seiner Kosten und Komplexität.

Derzeit bietet die PAM-Lösung eine begrenzte Kontextbewusstsein ohne jegliche Verbindung zu ihrer Kern-Identitätslösung. Dies begrenzt ihre Fähigkeit, eine rollenbasierte Lösung zur Kontrolle des Zugriffs auf die hochwertigen Systeme innerhalb der PAM-Lösung zu bieten.

Idealerweise würde die PAM-Lösung in der Lage sein, Kontextinformationen zu nutzen, um Zugriffskontrollentscheidungen in Übereinstimmung mit Richtlinien und Compliance-Anforderungen zu treffen. Die Integration mit ihrer IAM-Lösung ist auch eine Priorität, als Teil ihrer allgemeinen Neubewertung ihrer Verwendung von Jump Boxes und PAM für den Zugriff auf hochwertige Ressourcen.

Netzwerkzugriffskontrolle

Diese Organisation verwendet eine Lösung für Netzwerkzugriffskontrolle (NAC) zur Verwaltung des Netzwerkzugriffs für Benutzer vor Ort in ihrem Hauptsitz, sowie für den Gast-Wi-Fi-Zugriff. Dieses hardwarebasierte System – das Teil der Netzwerkinfrastruktur ist – verwendet von der Firma ausgestellte Zertifikate, um gültige Geräte zu identifizieren und ihnen VLANs zuzuweisen.

Anfangs funktionierte dies für den Hauptsitz des Unternehmens recht gut, obwohl NAC aufgrund seiner betrieblichen Komplexität nicht mit Netzwerkänderungen Schritt gehalten hat und Benutzer Zugriff auf eine breitere Palette von Workloads und Daten haben als gewünscht. Diese „Drift“ war tatsächlich die Ursache für einen kürzlichen Prüfungsbefund bezüglich des Netzwerkzugriffs auf Produktionssysteme.

Darüber hinaus ist ihre NAC-Lösung ein Silo, in mehreren Dimensionen. Erstens – hauptsächlich aufgrund von Kosten und Komplexität – haben sie sich entschieden, NAC nicht in ihre Niederlassungen zu implementieren. Infolgedessen haben Benutzer in diesen Büros unterschiedliche Arten von Zugriffskontrollen, die auf sie angewendet werden. Zweitens kann NAC offensichtlich auch nicht für den Fernzugriff oder Cloud-Umgebungen verwendet werden. Diese Umgebungen haben separate Zugriffsrichtlinienmodelle, die grobkörnig und statisch sind.

Schließlich nähert sich ihre NAC-Hardware dem Ende der Lebensdauerunterstützung. Unter Berücksichtigung all dieser Aspekte haben die Sicherheitsverantwortlichen des Unternehmens beschlossen, die NAC zu eliminieren. Dies ermöglicht es ihnen, das NAC-Budget umzuverteilen, um ihre Zero Trust-Initiative zu finanzieren, während sie gleichzeitig ihre Infrastruktur modernisieren und die Komplexität und Betriebskosten reduzieren.

Intrusion Detection/Intrusion Prevention

Wie viele Unternehmen hat diese Organisation ein netzwerkbasiertes Intrusion Detection System/Intrusion Prevention System (IDS/IPS) im Einsatz, das durch eine Kombination von Modulen, die in ihren Next-Generation-Firewalls (NGFWs) laufen, sowie durch einige Implementierungen eines Open-Source-IDS/IPS bereitgestellt wird. Diese Systeme werden verwendet, um anomales Verhalten zu erkennen und darauf zu reagieren, durch eine Kombination von automatisierten und manuellen Reaktionen ihres Security Operations Center.

Ihr IDS ist jedoch im Laufe der Zeit weniger effektiv geworden, hauptsächlich aufgrund des Wachstums in Größe und Komplexität des Netzwerks, der Einführung von Cloud-basierten Ressourcen, wo ihr IDS nicht als Inline-„Engpass“ fungieren kann, und der zunehmenden Verwendung von verschlüsselten Protokollen.

Sie möchten eine umfassendere und ganzheitlichere Möglichkeit zur Erkennung und Reaktion auf Indikatoren für Kompromittierungen in ihrer heterogenen Umgebung. Sie haben das Gefühl, dass sie zu viel Zeit und Geld aufwenden und nur begrenzte

Ergebnisse erzielen. Idealerweise hätten sie einen einzigen Ort, um IDS-Richtlinien zu definieren, und mehrere Orte, um sie in ihrem Netzwerk, Benutzergeräten und Workloads durchzusetzen. Sie möchten auch quantitative Vorteile (reduziertes Rauschen und falsche Positivmeldungen) sowie qualitative Vorteile (verbesserter Kontext für bessere Entscheidungen der Sicherheitsanalysten) erzielen.

Virtuelles privates Netzwerk

Ihr Virtuelles privates Netzwerk (VPN) ist das einzige System, das derzeit für den Fernzugriff in dieser Umgebung verwendet wird. Dieses VPN wurde für Remote-Mitarbeiter eingerichtet, um auf die Unternehmensumgebung zuzugreifen. Mit einer zunehmenden Anzahl von Remote-Mitarbeitern und wachsenden Sicherheitsbedenken hat die Organisation jedoch Leistungs- und Zuverlässigkeitsprobleme erlebt, und das VPN bietet keinen Kontext über Identitäten innerhalb der Umgebung. Darüber hinaus ist die Organisation besorgt über das rudimentäre Niveau der Zugriffskontrollen innerhalb der VPN-Lösung – Remote-Benutzer können sich mit wenigen Kontrollen im Netzwerk bewegen.

Die Organisation möchte den Sicherheitskontext erhöhen und die potenziellen Service- und Leistungsauswirkungen auf das Geschäft verringern. Um diese Sicherheit zu gewährleisten, möchten sie den Fernzugriff mit ihrem Identitätsanbieter integrieren und Benutzer- und Geräteattribute für Entscheidungen und Durchsetzung des Zugriffs nutzen.

Next-Generation Firewalls

Die Next-Generation Firewalls (NGFWs) dieses Unternehmens bestehen aus traditionellen Firewall-Funktionen, IDS/IPS, einigen Anwendungserkennungs- und Steuerungsfunktionen sowie einem Remote-Zugriffs-VPN (wurde zuvor separat besprochen). Sie sind nicht unzufrieden mit ihrer primären NGFW, kämpfen aber mit einer hybriden Infrastruktur – sie haben zwei Enklaven von NGFWs verschiedener Anbieter und konnten nie die Kapital- und Betriebskosten rechtfertigen, um dies auf einen einzigen Anbieter zu rationalisieren.

Daher haben sie unterschiedliche Fähigkeiten zwischen diesen beiden Enklaven, was zu betrieblichen Reibungen, fehl ausgerichteten Richtlinien- und Kontrollmodellen führt und technische Probleme verursacht hat, wenn der Verkehr zwischen diesen

Sicherheitsdomänen wechseln muss. Sie möchten eine Sicherheits- und Betriebslösung finden, die ihnen ein einheitliches Richtlinienmodell bietet und konsistent über diese Hardware-Infrastrukturen arbeitet. Sie möchten die Kosten für den Austausch dieser Hardware vermeiden, da sie noch mehrere Jahre Kapazität und Abschreibung übrig haben. Sie möchten auch damit beginnen, Bedrohungsintelligenz in ihre Sicherheitsplattform zu integrieren.

Sicherheitsinformationen und Ereignismanagement

Diese Organisation verwendet eine Kombination aus einem traditionellen On-Prem Sicherheitsinformationen und Ereignismanagement (SIEM) und einem neueren Cloud-basierten SIEM. Sie planen, vollständig auf das Cloud-basierte SIEM zu migrieren, haben jedoch einige On-Premises-Systeme, die sie angepasst und integriert haben. Diese Integration, obwohl sie für sie betrieblich wichtig ist, ist unflexibel und schwer zu warten.

Die Migration zum Cloud-basierten SIEM wird ihnen eine bessere Leistung und Skalierbarkeit bieten und es ihnen ermöglichen, Funktionen zu nutzen, die in dieser moderneren Plattform vorhanden sind, wie die Möglichkeit, Protokolldaten aus einer größeren Vielfalt von Quellen besser zu integrieren. Sie möchten die Informationen, die das SIEM verwenden kann, bereichern und es als Möglichkeit nutzen, den Benutzerzugriff über eine Risikobewertung zu beeinflussen. Insgesamt sind sie mit ihrem Cloud-basierten SIEM zufrieden, möchten aber, dass es mehr „Zähne“ hat – nämlich die Fähigkeit, den Benutzerzugriff automatisch zu beeinflussen. Sie suchen nach einer Verbesserung durch eine Kombination ihrer Zero Trust-Initiative und der Einführung eines Sicherheitsorchestrierungs-, Automatisierungs- und Reaktionssystems (SOAR).

Webserver und Web Application Firewall

Ein bedeutender Teil des Umsatzes dieses Unternehmens wird durch ein Web-System erzielt, das von ihren Unternehmenskunden genutzt wird – über ein Webportal sowie eine Reihe von Web-APIs. Dieses System befindet sich in ihrer DMZ und ist mit einer Reihe von Produktionssystemen im Unternehmensnetzwerk verbunden. Es wird durch eine Web Application Firewall (WAF) geschützt, die das Webportal und die API vor Anwendungs- und Netzwerkangriffen wie SQL-Injection und Cross-Site-Scripting schützt.

Es gibt mehrere Komponenten dieser Webanwendung, die hier relevant sind. Es gibt eine öffentliche Komponente, die im Grunde genommen Teil ihrer öffentlichen Website ist. Diese muss für alle zugänglich bleiben, einschließlich nicht authentifizierter und anonymer Benutzer. Sie bieten auch eine kostenlose Hands-on-Demo ihres Dienstes an, die in einem Sandbox-Demo-Mandanten ihres Systems läuft. Dies hat sich als wertvolles Geschäftsgenerierungstool erwiesen.

Die anderen Teile der Website sind privater und nur für identifizierte und authentifizierte Benutzer zugänglich. Es gibt eine umfangreiche Web-UI, auf der Kunden sich anmelden und die Anwendung nutzen, um Geschäfte mit diesem Unternehmen zu tätigen. Diese Anwendung beherbergt auch eine API, die von Kundensystemen intensiv genutzt wird, um Geschäfte zu tätigen – tatsächlich hat die API in den letzten Jahren die UI überholt und generiert nun 75 % ihres Online-Geschäfts gegenüber 25 % für die Web-UI. Sie sind zufrieden mit dem Grad der externen Sicherheit für dieses System und haben keinen dringenden Bedarf, es zu verbessern. Intern haben natürlich Systemadministratoren administrativen Zugriff auf das System. Sie haben ein relativ unreifes Set von Zugriffskontrollen für diese Administratoren, die sie im Rahmen ihrer Zero Trust Initiative verbessern möchten.

Infrastructure as a Service

Diese Organisation hat ihre Rechen- und Netzwerkfähigkeiten durch die Nutzung von Infrastructure as a Service (IaaS) verbessert und einen „privaten Link“-Tunnel zwischen dem On-Premises-Netzwerk und der Cloud-Infrastruktur erstellt; der gleiche flache Netzwerkansatz wird beibehalten, obwohl die Infrastruktur nun in der Cloud bereitgestellt wird. Obwohl dies Konnektivität bietet, bietet es keine zusätzliche Sicherheit. Tatsächlich erhöht diese Verbindung die Komplexität, weil sie ein Netzwerk, aber zwei unterschiedliche Sicherheitsmodelle und -tools haben.

Obwohl die Organisation die Möglichkeit hat, zusätzliche Überwachungs- und Netzwerkdienste zu nutzen, die der Cloud Service Provider (CSP) unterstützt, ist ihre On-Premises-Infrastruktur immer noch auf Basis von Legacy-Netzwerkdiensten aufgebaut, einschließlich einiger Elemente, die auf Layer 2 arbeiten. Diese Komponenten können nicht in einer Cloud-Umgebung arbeiten, was die Organisation dazu zwingt, zu überdenken, wie sie den Sicherheitsansatz mit IaaS angehen sollten.

Die Organisation sucht nach einer dynamischen und kontextsensitiven Sicherheit, die konsistent mit ihren On-Premises-Sicherheitsmodellen ist und mit diesen

übereinstimmt. Sie sollte identitätszentriert sein und ihnen eine ganzheitliche Möglichkeit bieten, den Zugriff sowohl in On-Prem- als auch in Cloud-Umgebungen zu kontrollieren und zu überwachen. Schließlich möchten sie die Art von Kontrolle und Automatisierung, die sie in IaaS haben, in ihrer heterogenen Umgebung replizieren, ohne alles in die Cloud migrieren zu müssen.

Software as a Service und Cloud Access Security Brokers

Die Organisation ist erheblich gewachsen und hat natürlich Software as a Service (SaaS)-basierte Anwendungen zur Unterstützung der primären Geschäftsfunktionen, einschließlich HR und anderen Funktionen, übernommen. Darüber hinaus gab es ein erhebliches Wachstum von Ressourcen, die nicht vollständig geschützt sind, da Geschäftseinheiten ihre eigenen SaaS-Anwendungen zur Unterstützung des Wachstums gekauft haben (Schatten-IT). Mit all diesem schnellen Wachstum hat die Organisation einen Cloud Application Security Broker (CASB) eingesetzt, der ihnen geholfen hat, genutzte Ressourcen zu finden und zu sichern.

Das Unternehmen möchte die Nutzung des CASB weiter fördern, um nicht nur weitere Schatten-IT zu verhindern, sondern auch Data Loss Prevention (DLP) besser und breiter durchzusetzen. Außerdem möchten sie einen sichereren und identitätszentrierten Ansatz zur Verwaltung ihrer Nutzung von SaaS-Anwendungen realisieren.

Damit schließen wir unsere Einführung in die bestehenden architektonischen Elemente dieses Unternehmens und die Wege, wie sie diese verbessern möchten. Beachten Sie, dass wir jede dieser Komponenten in Teil II des Buches aus einer Zero Trust-Perspektive weiter untersuchen werden. Jetzt stellen wir die Struktur und Zusammensetzung der Zero Trust-Architektur vor.

Eine Zero Trust-Architektur

In diesem Abschnitt stellen wir eine konzeptionelle Zero Trust-Architektur vor, die auf den im NIST-Dokument vorgestellten Arbeiten aufbaut, diese verfeinert und erweitert. In diesem Kapitel haben wir uns der gleichen Herausforderung wie die NIST-Autoren gestellt – nämlich, dass Zero Trust mit einem Satz von Prinzipien und einer Philosophie beginnt und

dass es viele verschiedene Unternehmenssicherheitsarchitekturen gibt, die zur Erreichung der Ziele von Zero Trust verwendet werden könnten. Wir erkennen an, dass es unmöglich ist, eine einzige Architektur zu erstellen oder darzustellen, die universell anwendbar ist – unser Ziel ist es, eine Reihe von architektonischen Komponenten und eine Reihe von Anforderungen vorzustellen, die Sie zur Erstellung einer relevanten und wertvollen Architektur für Ihre spezifische Organisation verwenden können.

Das NIST Zero Trust Modell

Wie wir im vorherigen Kapitel erwähnt haben, hat NIST eine logische Reihe von Zero Trust-Komponenten eingeführt, die in Abb. 3-2 dargestellt sind. Dieses Diagramm enthält einige der Kernkonzepte und Komponenten, die wir in diesem Buch verwenden werden.

Zunächst gibt es den Begriff eines **Subjekts** – definiert von NIST als entweder ein Benutzer, eine Anwendung oder ein Gerät – das auf (oder mit) einem Computersystem arbeitet und Zugang zu einer **Unternehmensressource** hat. Diese Ressource kann eine Anwendung, Daten, ein Dokument oder eine Arbeitslast sein, die unter der Kontrolle des Unternehmens steht und durch das Zero Trust-System geschützt ist. Wir bezeichnen dies im Allgemeinen als *Ressource* in diesem Buch.

Das Subjekt wird vermutet, in einer nicht vertrauenswürdigen Umgebung auf einem nicht vertrauenswürdigen Netzwerk zu arbeiten, und darf die Ressource nur über einen **Policy Enforcement Point** (PEP) zugreifen. Der PEP kontrolliert den Zugang des Subjekts

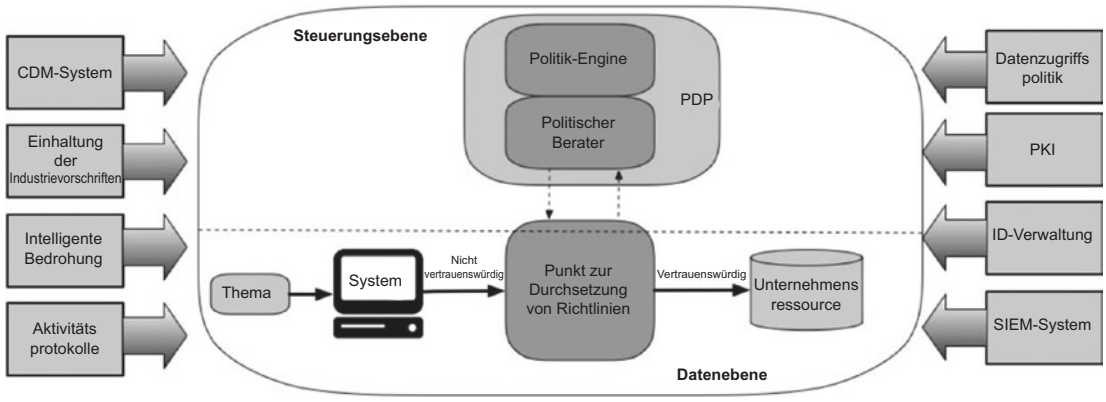

Abb. 3-2. *Logische Zero Trust-Komponenten. (Quelle: NIST: Zero Trust Architecture, SP 800-207)*

zur Ressource über das, was NIST als *implizite Vertrauenszone* bezeichnet, die wir später weiter diskutieren werden. Der PEP speichert oder trifft keine Richtlinienentscheidungen – diese Arbeit wird vom **Policy Decision Point** (PDP) durchgeführt.[3]

Beachten Sie, dass das Subjekt mit der Unternehmensressource über das, was als *Datenplane* bezeichnet wird, kommuniziert, das sich von der *Control Plane* unterscheidet – wie NIST feststellt, kommunizieren der PDP und PEP „auf einem Netzwerk, das logisch getrennt ist und nicht direkt von Unternehmensressourcen und -assets zugänglich ist. Die Datenplane wird für den Anwendungsdatenverkehr verwendet."

Die zusätzlichen Elemente, die zuvor als außerhalb des Systems dargestellt wurden (z. B. das CDM und PKI), müssen tatsächlich als logischer Teil eines Zero Trust-Systems betrachtet werden – oder zumindest mit einem Satz von bidirektionalen Pfeilen, die verschiedene Grade der Integration anzeigen. Diese Elemente sind wichtige Eingaben (Kontext) in das Zero Trust-System und beeinflussen definitiv seine Richtlinienentscheidungen. In diesem Buch – insbesondere in Teil II – werden wir argumentieren, dass all diese Systeme Produzenten und Konsumenten von Daten und Ereignissen sein müssen, die miteinander verknüpft sind. Es gibt viel zu besprechen, wenn wir untersuchen, wie diese Elemente mit dem PDP und den PEPs interagieren und sie beeinflussen können.

Es ist auch wichtig, die Schlüsselkonzepte des PDP und der PEPs zu untersuchen – wir möchten sicherstellen, dass Sie in der Lage sind, darüber nachzudenken, wie verschiedene Elemente Ihrer IT- und Sicherheitsinfrastruktur tatsächlich als PEPs innerhalb Ihrer zu realisierenden Zero Trust-Architektur betrachtet werden sollten. Dies ist der Grund, warum wir im Architekturdiagramm, das in Abb. 3-3 gezeigt wird, viele verschiedene konzeptionelle PEPs im gesamten Unternehmen haben, die wahrscheinlich verschiedene Dinge tun und verschiedene Rollen spielen. Tatsächlich glauben wir, wie wir später in diesem Kapitel einführen, dass es mehrere verschiedene Arten von PEPs gibt. Lassen Sie uns nun diese konzeptionelle Architektur untersuchen.

[3]Beachten Sie, dass NIST eine logische Trennung zwischen zwei Komponenten vornimmt, die einen PDP bilden – einen Policy Engine und einen Policy Administrator. Für dieses Buch halten wir diese Unterscheidung nicht für relevant und beziehen uns einfach auf den PDP als eine Einheit.

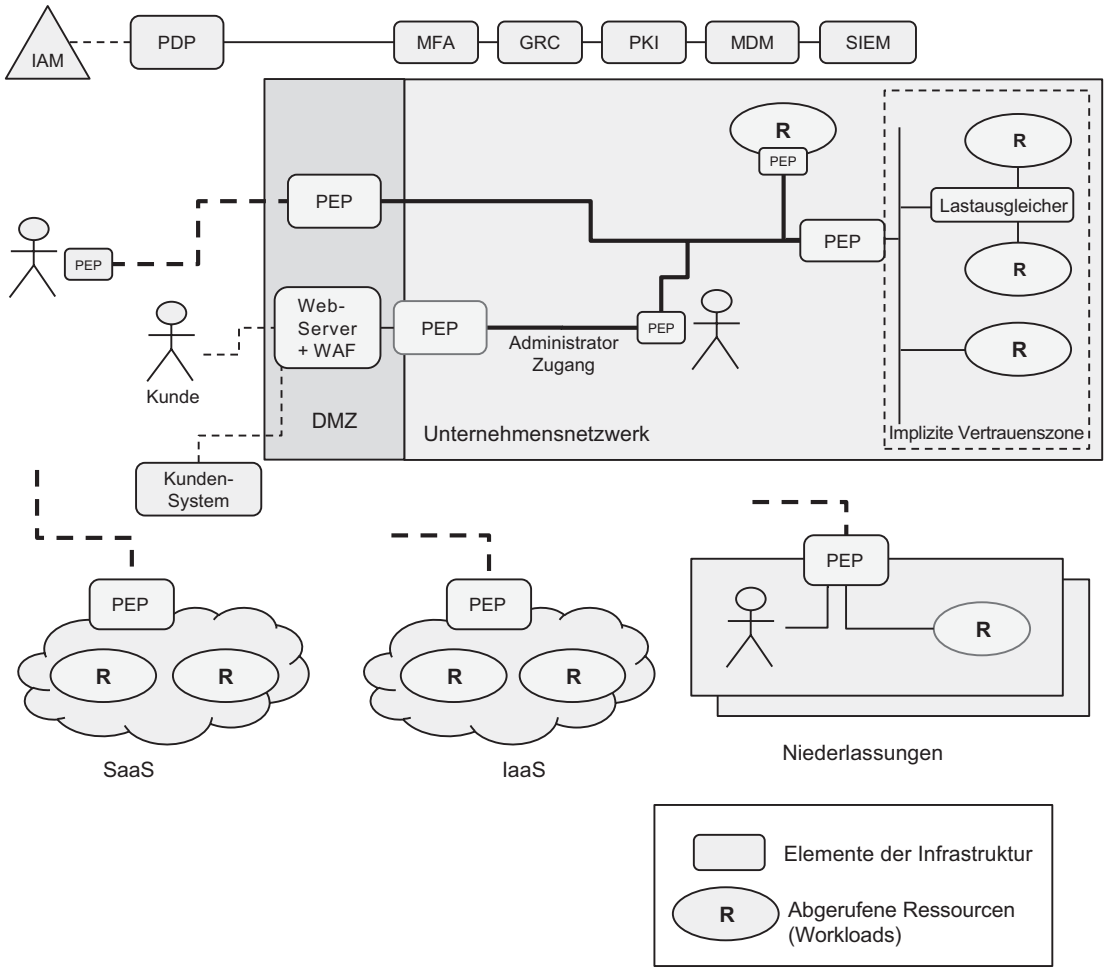

Abb. 3-3. *Konzeptionelle Zero Trust-Architektur*

Eine konzeptionelle Zero Trust-Architektur

In Abb. 3-3 stellen wir eine konzeptionelle Zero Trust-Architektur vor, die die Sicherheits- und IT-Infrastruktur aus unserem repräsentativen Unternehmen darstellt, aber aus einer Zero Trust-Perspektive neu konzipiert wurde.

Das Erste, was zu beachten ist, ist, dass es einen logisch zentralisierten Policy Decision Point gibt, der das Herzstück eines jeden Zero Trust-Systems bildet. In der Praxis – in einem realen Unternehmenssystem, das weiterentwickelt wird, um Zero Trust zu unterstützen – wird der PDP wahrscheinlich eine Kombination aus verschiedenen

technischen Systemen sein, die durch Integrationen und Geschäftsprozesse zusammengehalten werden.

Zero Trust ist natürlich ein sehr identitätszentriertes System, und jeder PDP muss eine enge, vertrauenswürdige Beziehung zu den Identitätsanbietern der Organisation haben. Technisch gesehen kann der PDP eine direkte Netzwerkverbindung mit dem IAM-Anbieter haben (d. h., wenn er LDAP oder RADIUS verwendet), oder eine indirekte Verbindung (d. h., wenn er SAML verwendet).

Was wichtiger ist, ist, dass erstens der PDP so konfiguriert sein muss, dass er den Daten, die er entweder direkt oder indirekt vom Identitätsanbieter erhält, vertrauen kann. Typischerweise wird dies durch die Konfiguration des PDP mit einem Servicekonto zur Durchführung von API-Aufrufen in den Identitätsanbieter oder durch die Konfiguration des PDP mit dem öffentlichen Zertifikat des Identitätssystems erreicht, so dass er die Daten validieren kann.

Zweitens muss der PDP in der Lage sein, Identitätsattribute vom Identitätsanbieter (oder Anbietern) in seine interne Darstellung zu mappen, da sie innerhalb des Richtlinienmodells des PDP verwendet werden. Wir werden das Richtlinienmodell in Kap. 17 ausführlich untersuchen, aber wir werden hier eine leichte Einführung geben.

Das NIST-Dokument bietet einen guten Ausgangspunkt: Es stellt als eines der grundlegenden Zero Trust-Prinzipien fest, dass „der Zugang zu Ressourcen durch eine dynamische Richtlinie bestimmt wird – einschließlich des beobachtbaren Zustands der Client-Identität, der Anwendung und des anfordernden Assets – und kann andere Verhaltensattribute einschließen." Anders ausgedrückt, wenn ein Subjekt auf eine Ressource zugreifen kann, muss es eine Richtlinie geben, die ausgewertet wurde und die dem Subjekt den Zugang zur betreffenden Ressource zum aktuellen Zeitpunkt gewährt.

Das NIST Zero Trust-Dokument besagt auch, dass „Unternehmensressourcen nicht erreichbar sein sollten, ohne auf einen PEP zuzugreifen", weshalb in Abb. 3-3 PEPs in der gesamten Unternehmensarchitektur verteilt sind. In unserem Diagramm beachten Sie auch, dass die PEPs an verschiedenen Orten sind und verschiedene Funktionen ausführen. Obwohl sie alle PEPs sind, sind sie von verschiedenen Typen und haben unterschiedliche Rollen und Funktionen bei der Durchsetzung von Richtlinien.

Unsere Sichtweise ist, dass ein effektives Zero Trust-System eine Reihe von zentral verwalteten PEPs haben wird, die über das gesamte Unternehmensökosystem verteilt sind. Das System muss das Verhalten der PEPs durch eine Reihe von Richtlinien steuern, die dynamisch und kontextsensitiv sind und im gesamten Umfeld durchgesetzt werden.

Wie wir jedoch bereits früher bemerkt haben, können diese PEPs von verschiedenen Typen sein, mit unterschiedlichen Rollen und Funktionen.

Zum Beispiel hat der PEP, der in der DMZ sitzt, die Verantwortung, nur autorisierten und authentifizierten Benutzern den Zugang zu dem entsprechenden Satz interner Ressourcen zu erlauben. Dies muss er tun – mit Durchsetzung auf der Netzwerkebene – basierend auf dem Satz von Berechtigungen, die ihm vom PDP gegeben wurden, die der PDP aus Richtlinien ableitet, basierend auf verschiedenen Eingaben einschließlich Benutzer- und Systemkontext. Wir werden die Mechanismen, durch die dies geschehen kann, später im Buch untersuchen.

Hier ist ein weiteres Beispiel – der PEP, der innerhalb der Ressource in der oberen rechten Ecke des Diagramms läuft, muss den Satz von Berechtigungen durchsetzen, die ihm vom PDP gegeben wurden. Dieser PEP kann für die Kontrolle des eingehenden (und möglicherweise ausgehenden) Netzwerkverkehrs verantwortlich sein oder kann für die Durchsetzung von rollenbasierten Berechtigungen innerhalb der Anwendung verantwortlich sein.

In beiden Fällen erhalten die PEPs ihre Anweisungen – die Richtlinien, für deren Durchsetzung sie verantwortlich sind – vom PDP. Wir werden Richtlinien in Kap. 17 eingehend untersuchen, aber es ist notwendig, die Dinge hier zu rahmen. Wir sind hier spezifischer als NIST, weil wir glauben, dass diese zusätzliche Struktur lohnenswert ist und Ihnen einen nützlichen Rahmen bietet, um über ein Zero Trust-Plattform in Ihrem Unternehmen nachzudenken, Anforderungen zu definieren, Lösungen auszuwählen und letztendlich zu implementieren.

Richtlinienkomponenten

Wir definieren eine Richtlinie als eine deklarative Aussage, die besagt, dass ein **Subjekt** berechtigt ist, eine **Aktion** auf ein **Ziel** auszuführen, wenn und nur wenn bestimmte **Bedingungen** erfüllt sind. Dies wird in Tab. 3-1 gezeigt.

Lassen Sie uns diese Richtlinienstruktur untersuchen. *Subjektkriterien* werden verwendet, um den Satz von Identitäten (Subjekten) zu definieren, auf die diese Richtlinie anwendbar ist. Subjekte – die Personen oder Nicht-Personen-Entitäten (NPE) sein können – müssen authentifizierte Entitäten sein und müssen in irgendeinem Identitätsverwaltungssystem existieren. Subjekte haben viele Attribute, die aus Quellen wie ihrem authentifizierenden Identitätssystem, Geräteprofil und Netzwerk- oder

Tab. 3-1. *Richtlinienkomponenten*

Komponente	Beschreibung
Subjektkriterien	Subjekte sind die Entitäten, die Aktionen ausführen (initiieren). Subjekte müssen authentifizierte Identitäten sein, und Richtlinien müssen *Subjektkriterien* enthalten, die die Subjekte bestimmen, auf die diese Richtlinie anwendbar ist.
Aktion	Die Aktivität, die vom Subjekt ausgeführt wird. Dies muss entweder eine Netzwerk- oder eine Anwendungskomponente enthalten und kann möglicherweise beide enthalten.
Ziel	Das Objekt (Ressource), auf das die Aktion ausgeführt wird. Dies kann statisch oder dynamisch innerhalb der Richtlinie definiert sein und kann in seinem Umfang breit oder eng sein, obwohl eng bevorzugt wird.
Bedingung	Die Umstände, unter denen das Subjekt berechtigt ist, die Aktion auf das Ziel auszuführen. Das Zero Trust-System muss die Definition von Bedingungen unterstützen, die auf mehrere Arten von Attributen zurückgreifen, einschließlich Subjekt-, Umgebungs- und Zielattributen.

Geolokalisierungsinformationen, unter anderem, gezogen werden. Diese Attribute werden in den Subjektkriterien verwendet, um zu bestimmen, ob eine Richtlinie einer gegebenen Identität zugewiesen werden sollte (beachten Sie, dass Attribute auch in Bedingungen verwendet werden, die wir in Kürze besprechen werden). Es sollte klar sein, dass ein Zero Trust-Richtlinienmodell Attributbasierte Zugriffskontrolle (ABAC) in vielerlei Hinsicht durchsetzt.[4]

Aktionen definieren die tatsächliche Aktivität, die diese Richtlinie dem Subjekt erlaubt auszuführen. Sie muss entweder eine Netzwerk- oder Anwendungsaktion enthalten und kann beide enthalten.

[4]Tatsächlich ist NIST SP 800-162 zum Thema ABAC, das 2014 veröffentlicht wurde, in vielerlei Hinsicht ein Vorläufer dieses Zero Trust-Modells und besagt: „Wenn ein Subjekt Zugang anfordert, kann die ABAC-Engine eine Zugriffskontrollentscheidung treffen, basierend auf den zugewiesenen Attributen des Anforderers, den zugewiesenen Attributen des Objekts, Umgebungsbedingungen und einem Satz von Richtlinien, die in Bezug auf diese Attribute und Bedingungen festgelegt sind."

Tab. 3-2. *Ein Beispiel für eine Richtlinie*

Richtlinie: Benutzer in der Abrechnungsabteilung müssen in der Lage sein, die Webanwendung für die Abrechnung zu nutzen	
Subjektkriterien	Benutzer, die Mitglieder der Gruppe Dept_Billing im Identity Provider sind.
Aktion	Benutzer müssen in der Lage sein, auf die Web-UI auf Port 443 über HTTPS zuzugreifen.
Ziel	Die Abrechnungsanwendung mit dem FQDN billing.internal.company.com.
Bedingung	Benutzer können vor Ort oder remote sein. Remote-Benutzer müssen vor dem Zugriff (zum Zeitpunkt der Authentifizierung) zur MFA aufgefordert werden. Benutzer müssen auf diese Anwendung von einem firmeneigenen Gerät mit laufender Endpunktsicherheitssoftware zugreifen.

Ziele sind das System oder die Komponente, auf die eingewirkt wird. Diese können statisch definiert sein (z. B. mit einem festen Hostnamen oder einer IP-Adresse[5]), oder dynamisch über Attribute wie Hypervisor- oder IaaS-Labels oder Tags, die zur Laufzeit aufgelöst werden. Sie können eng definiert sein (z. B. ein einzelner Dienst, der auf einem einzelnen Server läuft) oder breiter definiert (z. B. Zugang zu einer Klasse von Servern oder einem Subnetz). *Bedingungen* bestimmen, wann das Subjekt tatsächlich die Aktion auf das Ziel ausführen darf und können eine sehr breite Vielfalt von Umständen einschließen. Lassen Sie uns ein Beispiel einführen, um dies zu verdeutlichen und Ihnen zu helfen, darüber nachzudenken, wie sie vom PDP interpretiert werden und wie verschiedene Arten von PEPs funktionieren könnten.

Tab. 3-2 zeigt ein Beispiel für eine Richtlinie, die den Zugang zu einer internen Webanwendung steuert. Wir werden dieses und andere Beispiele im Kap. 17 ausführlich untersuchen.

[5]Ja, Hostnamen werden tatsächlich dynamisch über DNS aufgelöst und können sich durch den Einsatz von Load Balancern unterschiedlich auflösen. Für unsere Zwecke betrachten wir sie als statisch.

Arten von Richtliniendurchsetzungspunkten

Nachdem wir kurz die Richtlinien vorgestellt haben, wollen wir uns die PEPs genauer ansehen. Wie wir bereits erwähnt haben, wird die Richtliniendurchsetzung von PEPs auf verschiedenen Ebenen und von verschiedenen Typen durchgeführt – dargestellt in Abb. 3-4.

Wir glauben, dass es tatsächlich drei Arten von PEPs gibt, wie in dieser Abbildung dargestellt: Benutzeragenten-PEPs, Netzwerk-PEPs und Anwendungs-PEPs. Netzwerk-PEPs sind vielleicht die einfachsten, konzeptionell, in Zero Trust Modellen, da Zero Trust Networking typischerweise der häufigste Ausgangspunkt ist und weitgehend die Ausrichtung des NIST-Dokuments ist. Netzwerk-PEPs sind auch bereits in vielen Organisationen vorhanden – in gewissem Maße können Unternehmensfirewalls (Next-Generation Firewalls) als Zero Trust PEPs betrachtet werden, wenn auch mit einigen Einschränkungen, wie wir später diskutieren werden. Da diese PEPs auf der Netzwerkebene arbeiten, können sie die Durchsetzung von Netzwerkverkehr inline durchführen, weshalb sie natürliche Durchsetzungspunkte sind. Sie können auch eine Inspektion des Verkehrs durchführen, entweder Metadaten oder die tatsächlichen Verkehrsdaten.

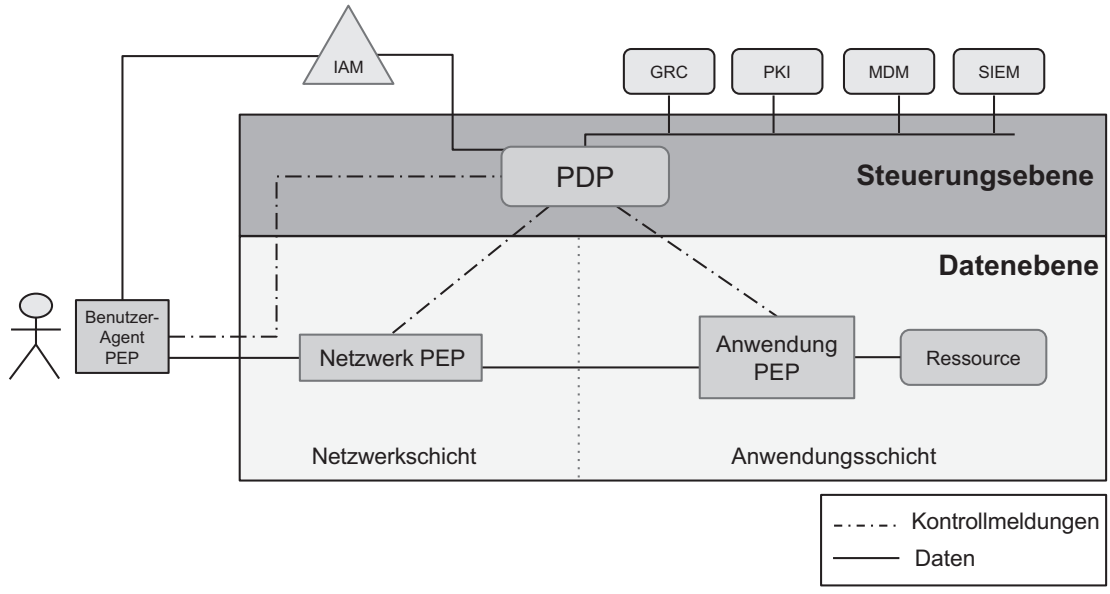

Abb. 3-4. *Kontroll-Ebene, Daten-Ebene und Richtliniendurchsetzungsschichten*

Anwendungs-PEPs können extern zu Anwendungen sein (z. B. ein PAM- oder DLP-System) oder intern, wie ein Agent, der auf einer Arbeitslast läuft. Im letzteren Fall kann der PEP verwendet werden, um Richtlinien lokal auf dem Host durchzusetzen, wie z. B. lokale OS-Firewall-Regeln. Zusätzlich könnte der PEP logisch Teil der Anwendung selbst sein, der sich auf externe Attribute oder Aktionen stützt, um die Anwendung zu beeinflussen. Dies ist ein wichtiger Aspekt – PEPs müssen eine gewisse Integration mit dem PDP haben und in der Lage sein, Elemente der Richtlinien durchzusetzen, die ihm vom PDP zur Verfügung gestellt werden. Diese Durchsetzung kann ausschließlich innerhalb der Anwendung erfolgen (z. B. sicherstellen, dass eine bestimmte Identität ein Konto mit einer bestimmten Anwendungsrolle hat). Wir haben Beispiele dafür in modernen Anwendungen gesehen, die beispielsweise eine Just-in-Time-Provisionierung auf Basis des Inhalts einer SAML-Behauptung unterstützen. Diese Provisionierung kann die Form einer neuen Kontenerstellung mit einer anfänglichen Rolle annehmen oder eine Änderung der Rollen eines Benutzers.

Benutzeragenten-PEPs sind Komponenten, die auf einem Benutzergerät laufen und Funktionen bereitstellen, die oft für Zero Trust-Systeme notwendig sind, wie zum Beispiel die Herstellung einer verschlüsselten Verbindung über ein nicht vertrauenswürdiges Netzwerk (NIST bezeichnet dies als „Koordinierung der Verbindungen“). Diese PEPs werden oft verwendet, um das Gerät zu inspizieren und Informationen zu erhalten, die als Eingabe in Richtlinien verwendet werden (z. B. Gerätekonfiguration und Sicherheitsstatus). Der PEP kann auch mit dem Subjekt (Endbenutzer) interagieren, indem er sie zum Beispiel zur zusätzlichen Authentifizierung auffordert oder sie benachrichtigt. Obwohl dieser PEP als optional betrachtet werden sollte – viele (wirklich, die meisten) kommerziellen Zero Trust-Systeme bieten einen Benutzeragenten (Client) zur Installation auf Benutzergeräten an. Die meisten kommerziellen Zero Trust-Systeme haben *auch* typischerweise Optionen für clientlosen oder webbasierten Zugriff, mit einem gewissen Grad an eingeschränkter Funktionalität.[6] In den Abbildungen in diesem Buch wird ein Benutzeragenten-PEP dargestellt.

Beachten Sie, dass es in einigen Fällen eine unscharfe Linie zwischen diesen Arten von PEPs gibt und es kann eine Überschneidung in den von ihnen ausgeführten

[6]Und einige kommerzielle Systeme teilen den Unterschied, indem sie ihre Benutzeragenten-Software als Browsererweiterung bereitstellen.

Funktionen geben. Zum Beispiel ist unsere Branche gut darüber informiert, dass IDS/IPS netzwerkbasiert oder hostbasiert sein können. Ebenso können DLP-Funktionen in einem Netzwerkgerät, wie einem NGFW, oder auf einem Host implementiert sein. Ob spezifische Durchsetzungspunkte, wie DLP und PAM, auf der Netzwerkebene oder der Anwendungsebene (oder beiden) agieren, ist nicht so wichtig. Was wichtig ist, ist, dass sowohl DLP als auch PAM als Teil des Zero Trust PEP betrachtet werden sollten und ihre Richtlinien logischerweise Teil des Zero Trust-Modells sein sollten. Idealerweise gäbe es eine Integration zwischen ihnen und dem Zero Trust-System, um dies zu steuern. Dies könnte durch Identitätsattribute/Rollen oder über ein separates Zero Trust-Richtlinienmodell gesteuert werden – das hängt wirklich von der Implementierung ab.

Letztendlich wird die Funktionalität und das Verhalten Ihrer PEPs von der Plattform abhängen, die Sie wählen, und davon, wie Sie sie einsetzen. In diesem Buch beschreiben wir im Kern, wie Ihre aktuelle Infrastruktur und Architektur als eine Reihe von Zero Trust-PEPs betrachtet werden sollte. Eine erfolgreiche Zero Trust-Reise bedeutet, dass alle Ihre PEPs integriert sind, ein Richtlinienmodell teilen und betrieblich verbunden sind. Aber das ist ein Ziel, kein Ausgangspunkt, und Sie sollten im Hinterkopf behalten, dass es immer noch viele bestehende Infrastrukturelemente geben wird, die keine PEPs sind und nicht logisch in Ihr Zero Trust-Richtlinienmodell eingebunden sind.

Zum Beispiel zeigt Abb. 3-3 immer noch einen Lastverteiler, der auch innerhalb der Zero Trust-Architektur eine nützliche Funktion erfüllt. In diesem Fall arbeitet der Lastverteiler auf einer einfachen Netzwerkebene und kann seine Funktion ohne Änderung trotz der Einführung von Zero Trust in der restlichen Architektur weiterhin ausführen. Es gibt keinen Grund, es übermäßig zu komplizieren, und seine Funktion muss nicht durch Benutzer- oder Systemkontext geändert werden. Dies wird für viele Elemente Ihrer Infrastruktur der Fall sein – also während Zero Trust Ihnen die Möglichkeit geben kann und sollte, Ihre Sicherheits- und Integrationsarchitektur neu zu denken, bedeutet das nicht, dass jedes Element geändert werden muss. Anders ausgedrückt, es ist realistisch, Zero Trust schrittweise zu übernehmen und Richtlinien an Schlüsselpunkten in Ihrer Infrastruktur durchzusetzen, während störende Veränderungen vermieden werden. Dies führt uns zu unserem nächsten Thema: Richtlinien.

Was ist ein Policy Enforcement Point?

Richtlinien sind das Herzstück jedes Zero Trust-Systems und werden kontinuierlich von PDPs bewertet und von den PEPs durchgesetzt. Aber das wirft eine interessante und etwas philosophische Frage auf – was macht eine Sicherheitskomponente zu einem Zero Trust Policy Enforcement Point? Zum Beispiel, kann eine 5 Jahre alte, grundlegende Firewall als PEP betrachtet werden? Wie bei den meisten interessanten Fragen lautet die Antwort „es kommt darauf an", und die Erkenntnis ergibt sich aus den Denkprozessen, die bei der Untersuchung der Abhängigkeiten beteiligt sind, also tauchen wir ein.

Unsere grundlegende Firewall ist natürlich ein „Netzwerk-Durchsetzungspunkt" im Sinne, dass sie Zugriffskontrollregeln hat, die sie durchsetzt, wie zum Beispiel „Erlaube TCP-Verkehr auf Port 443 von der Quell-Subnetz 10.5.0.0/16 zum Ziel-Subnetz 10.3.0.0/16". Wir argumentieren jedoch, dass diese Firewall kein Zero Trust PEP ist – sie erfüllt nicht die folgenden Anforderungen:

- Die Fähigkeit haben, das identitätszentrierte und kontextsensitive Richtlinienmodell der PDPs durchzusetzen
- Automatisch auf Richtlinienänderungen reagieren, die vom PDP gesteuert werden
- Einen Kontrollkanal für die Kommunikation mit dem PDP nutzen

Es sollte klar sein, dass eine traditionelle Firewall diese Anforderungen nicht erfüllt – tatsächlich werden wir später im Buch untersuchen, dass die Fähigkeit eines PEP, programmgesteuert vom PDP zu sein und seine Richtlinien auf automatisierte Weise anzupassen, eine Schlüsselkompetenz bei der Realisierung von Zero Trust ist. Das heißt, unsere grundlegende Prämisse ist, dass ein Zero Trust-System in der Lage sein muss, identitäts- und kontextsensitive dynamische Richtlinien durchzusetzen. Die Implikation davon ist, dass jeder PEP in der Lage sein muss, laufende Updates vom PDP zu erhalten und die Richtlinien, die er durchsetzt, nahezu in Echtzeit und ohne menschliches Eingreifen automatisch anzupassen. Dies ist der einzige Weg, um die reaktive, dynamische Natur von Zero Trust zu erreichen, selbst in kleinem Maßstab.

Also, lassen Sie uns unser Gedankenexperiment fortsetzen. Was ist, wenn unsere 5 Jahre alte Firewall, die in einem Verdrahtungsschrank sitzt und mit Staub bedeckt ist, eine Richtlinien-gesteuerte Automatisierungsschicht hat, die auf ihr implementiert wurde? In diesem Fall würden wir argumentieren, dass jetzt diese Firewall – in Kombination mit der Netzwerksicherheitsautomatisierungssoftware – als Zero Trust PEP

betrachtet werden könnte, solange die Netzwerksicherheitsautomatisierungslösung selbst in den PDP eingebunden ist und die zuvor beschriebenen Kriterien erfüllt. Das heißt, das Wesen eines Zero Trust PEP besteht darin, dass es eine automatisierte Integration mit dem PDP hat und schnell auf Richtlinienänderungen reagieren kann. Zero Trust Policy Enforcement Points können nicht von einem Richtlinienmodell oder betrieblichen Standpunkt aus isoliert sein.

Beachten Sie, dass wir hier den Begriff *automatisiert* verwendet haben. Automatisiert bedeutet nicht unbedingt *vollständig* automatisch – es ist völlig in Ordnung, manuelle Schritte einzubeziehen, wie zum Beispiel eine Geschäftsprozessgenehmigung für bestimmte Änderungen oder manuelle Genehmigung von außergewöhnlichen „Notfall"-Situationen. Aber es müssen automatische Änderungen für die täglichen (oder stündlichen, oder sogar minütlichen) Änderungen vorgenommen werden, die dieser Durchsetzungspunkt kontrolliert.

Zum Beispiel, erinnern Sie sich an unsere Beispielrichtlinie aus Tab. 3-2. Betrachten Sie, was passiert, wenn die Benutzerin Jane zur Dept_Billing Verzeichnisgruppe hinzugefügt wird. Kurz darauf muss sie in der Lage sein, auf die Abrechnungs-App auf Netzwerkebene zuzugreifen und ein aktives Konto auf Anwendungsebene zu haben. In Wirklichkeit kann die Bereitstellung des Kontos für Jane ein manueller Prozess sein, aber wir glauben, dass die Netzwerkzugriffsänderungen automatisiert sein müssen. Um dies zu veranschaulichen, stellen Sie sich vor, dass Jane ein paar Tage später versehentlich auf einen Phishing-Link klickt und Malware auf ihrem Laptop installiert, die Netzwerkerkundungen durchführt. Die Sicherheitssysteme des Unternehmens erkennen dies als Anzeichen für einen Kompromiss und reagieren, indem sie automatisch ihren Netzwerkzugriff auf das geschäftskritische Abrechnungssystem blockieren, um zu verhindern, dass die Malware es möglicherweise kompromittiert.

Diese Reaktion muss schnell und automatisch vom Netzwerk-PEP durchgeführt werden – dies kann nicht auf einen Geschäftsprozess warten. Beachten Sie, dass in unserem Beispiel sehr wahrscheinlich nur der Zugriff auf Netzwerkebene durch den Netzwerk-PEP blockiert wird. Es besteht kein Grund, Änderungen innerhalb des Anwendungs-PEP vorzunehmen – dies ist ein vorübergehendes Problem mit Janes Laptop. Tatsächlich würde ein gut konzipiertes Zero Trust-System weiterhin erlauben, dass Jane von einem anderen Gerät (z. B. einem Desktop-Computer) auf die Abrechnungsanwendung zugreift, während der Laptop weiterhin blockiert wird. Wir werden diese Themen weiter in Kap. 5 und 17 untersuchen.

Zero Trust Bereitstellungsmodelle

Als nächstes werden wir mehrere Zero Trust-Bereitstellungsmodelle untersuchen – darunter zwei aus dem NIST Zero Trust-Dokument, plus zwei weitere für die Vollständigkeit. Diese Modelle geben uns die nächste Stufe der Spezifität darüber, wie Zero Trust-Systeme tatsächlich bereitgestellt werden könnten, obwohl natürlich die realen Bereitstellungsarchitekturen von den Fähigkeiten der gewählten Technologie abhängen werden. Wir glauben, dass viele der von Anbietern bereitgestellten Unternehmensmodelle für Zero Trust mit einem oder mehreren der in den folgenden Texten dargestellten Bereitstellungsmodelle übereinstimmen werden. Das heißt, diese Bereitstellungsmodelle werden als nützliches Framework dienen, mit dem Sie potenzielle Anbieter bewerten und ihre Vor- und Nachteile untersuchen können. Sie sind nicht dazu gedacht, erschöpfend zu sein, aber sie sollen repräsentativ sein. Sie sind auch nicht unbedingt gegenseitig ausschließend – einige Systeme können durchaus Elemente von mehreren dieser Modelle kombinieren. Beachten Sie, dass wir uns in den folgenden Diskussionen auf den Kontrast zwischen diesen Modellen konzentrieren, anstatt auf das, was sie gemeinsam haben.

Schließlich beachten Sie, dass wir zur Klarheit in den folgenden Diagrammen die Verbindung des PDP zur Identitätsverwaltung und anderen Unternehmenssicherheitssystemen, wie zuvor dargestellt, weglassen. Diese Verbindungen müssen weiterhin bestehen, unabhängig davon, welches Zero Trust-Bereitstellungsmodell Sie wählen.

Ressourcenbasiertes Bereitstellungsmodell

Unser erstes Modell ist das *ressourcenbasierte Bereitstellungsmodell* – dargestellt in Abb. 3-5.[7]

Was an diesem Modell wichtig ist, ist erstens, dass normalerweise ein Benutzeragent auf das System des Subjekts bereitgestellt wird und als Benutzeragent PEP fungiert.[8] Zweitens, dass es einen Inline-PEP (das Gateway) gibt, der (laut NIST) „**auf** der

[7]Beachten Sie, dass NIST dies als das etwas umständliche *Geräteagenten/Gateway-Modell* bezeichnet.

[8]Wie wir bereits bemerkt haben, ist dieser Agent ein Bestandteil der meisten kommerziellen Zero Trust-Lösungen, obwohl er streng genommen optional ist. Die meisten Anbieter unterstützen eine „clientlose“ Option, mit einigen damit verbundenen Kompromissen in der Funktionalität.

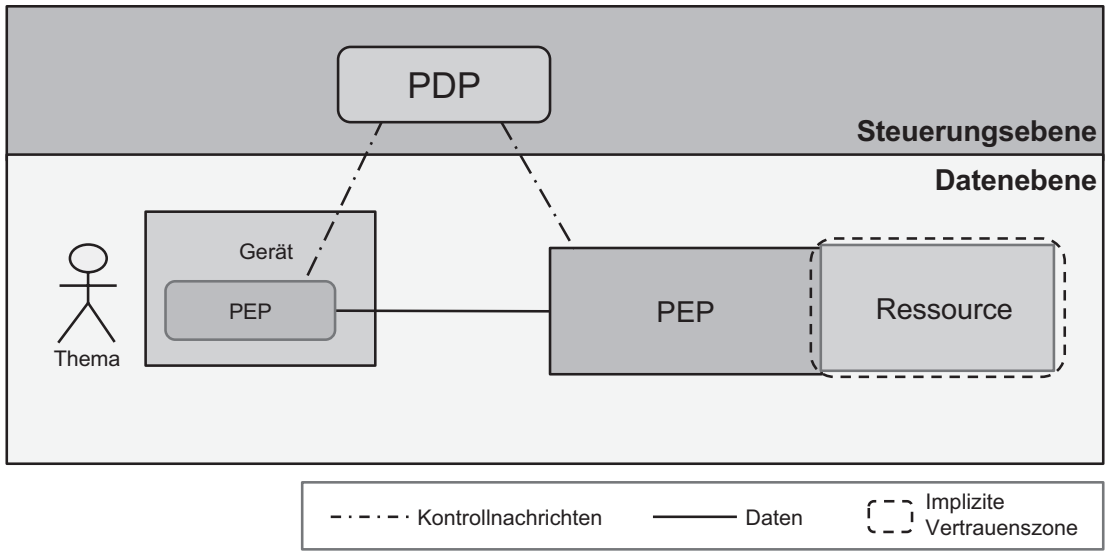

Abb. 3-5. *Ressourcenbasiertes Bereitstellungsmodell*

Ressource oder als Komponente **direkt vor** einer Ressource“ bereitgestellt wird (Hervorhebung von uns).

Dieses Diagramm führt auch eine visuelle Darstellung der *impliziten Vertrauenszone* ein, die ein Bereich hinter einem gegebenen PEP ist, innerhalb dessen alle Ressourcen (Entitäten) im gleichen Maße vertraut werden. Dies stellt die Grenze des Sicherheitsbereichs dar, für den dieser PEP verantwortlich ist. Per Definition finden alle Interaktionen zwischen Komponenten, die innerhalb der impliziten Vertrauenszone bleiben, außerhalb der Kontrolle des PEP statt. Im vorherigen Beispiel, wenn der PEP auf dem lokalen Ressourcen-Betriebssystem läuft, umfasst die implizite Vertrauenszone die Menge der lokalen Prozesse und ihre Interaktionen innerhalb des lokalen Betriebssystems. Natürlich möchten Sie die Größe der impliziten Vertrauenszone minimieren – in dem Verständnis, dass es Kompromisse bei jedem der Bereitstellungsmodelle gibt.

Ressourcenbasiertes Bereitstellungsmodell: Vorteile

- End-to-End-Kontrolle des Anwendungszugriffs und des Netzwerkverkehrs
- Sehr kompakte implizite Vertrauenszone, die “hinter” dem Gateway liegt

Dieses Modell stellt sicher, dass alle Netzwerkkommunikationen zwischen Benutzergeräten und der Zielressource verschlüsselt sind und dass Zugriffskontrollrichtlinien durchgesetzt werden. Es stellt auch sicher, dass *alle* Netzwerkkommunikationen mit der Ressource durch den PEP (und daher durch das Zero Trust-Sicherheitsmodell der Organisation) durchgesetzt werden. Dieses Modell hat jedoch auch eine Reihe von Nachteilen, die berücksichtigt werden müssen.

Ressourcenbasiertes Bereitstellungsmodell: Nachteile

- Erfordert die Bereitstellung der PEPs sowohl auf Benutzergeräten als auch auf Ressourcen.
- Potenzial für technische Konflikte zwischen Ressourcenkomponenten und PEPs.
- PEPs müssen auf eine große Vielfalt von möglicherweise veralteten/legacy Betriebssystemen bereitgestellt werden können.
- Potenzial für Widerstand von Anwendungsressourcenbesitzern.
- Erfordert eine 1:1: Beziehung zwischen PEPs und Ressourcen.
- End-to-End sichere Tunnel können bestehende Inline-Sicherheitskontrollen blenden.
- PEP muss für Remote-Benutzer sichtbar und verfügbar sein.

Erstens erfordert dieses Modell, dass ein PEP auf jeder Ressource in der Umgebung bereitgestellt wird, was potenziell problematisch ist. In jeder Umgebung von mehr als minimaler Größe wird dies wahrscheinlich einen hohen Grad an Automatisierung erfordern, insbesondere für virtualisierte oder Cloud-Umgebungen. Lokal bereitgestellte PEPs haben auch das Potenzial für technische Konflikte innerhalb desselben Betriebssystems, zum Beispiel mit Komponenten, die die Kontrolle über Netzwerk- oder Festplatten-I/O übernehmen, wie Webserver oder Datenbanken.

Dieses Modell erfordert auch, dass PEPs auf 100 % der geschützten Ressourcen bereitgestellt werden. Dies stellt oft eine mehrdimensionale Herausforderung dar. Erstens, technisch gesehen, erfordert es, dass die PEP-Software auf allen Workloads unterstützt und bereitstellbar ist. Viele Organisationen haben Legacy-Anwendungen, die auf Mainframes oder Minicomputern laufen, die wahrscheinlich keinen PEP unterstützen können. Ironischerweise – und argumentativ – sind diese Legacy-Anwendungen oft diejenigen, die am dringendsten besser gesichert werden müssen!

Und zweitens werden viele Sicherheitsteams auf Widerstand von Anwendungseigentümern stoßen, die zögern werden, zusätzliche Software auf ihre umsatzgenerierenden oder geschäftskritischen Anwendungen zu installieren.

Aus betrieblicher Sicht erfordert dieses Modell einen PEP, der für jede verwaltete Ressource bereitgestellt wird, was eine erhebliche Verwaltungslast für das Zero Trust-System und das dafür verantwortliche Team darstellen kann. Zum Beispiel, wenn eine virtualisierte oder Cloud-Umgebung aus vielen vergänglichen Workloads besteht, ist das ständige Onboarding und Offboarding dieser Ressourcen etwas, vor dem man vorsichtig sein sollte. In diesem Fall müssten Sie sicherstellen, dass das Zero Trust-System ausreichend automatisiert ist, um diesen Wechsel bewältigen zu können.

Als ein zentraler Grundsatz von Zero Trust stellt dieses Modell sicher, dass der Netzwerkverkehr vom Benutzeragenten PEP zum Ressourcen PEP verschlüsselt ist.[9] In vielen kommerziellen Zero Trust-Systemen wird dies durch die Verwendung eines verschlüsselten Tunnels erreicht. Dies ist sicher und effektiv, hat aber in der Regel den Nebeneffekt, dass all dieser Verkehr für jeden Vermittler undurchsichtig wird. Dies ist vorteilhaft, wenn der Vermittler ein Angreifer ist, aber nachteilig, wenn es sich um eine vom Unternehmen bereitgestellte Sicherheitskomponente handelt, wie eine netzwerkbasierte IDS/IPS.

Schließlich – und vielleicht am wichtigsten – muss der PEP, der die Ressource schützt, natürlich für die Subjekte zugänglich sein, einschließlich Remote-Benutzer. Da der PEP in diesem Modell Teil der Ressource ist, bedeutet dies, dass entweder alle Subjekte im selben physischen Netzwerk wie jeder PEP sind oder dass alle PEPs direkt aus der Ferne zugänglich sind. Die erste Option wird selten zutreffen, und die zweite Option ist wahrscheinlich nicht machbar, da viele dieser Ressourcen auf privaten Netzwerksegmenten vorhanden sind. In der Realität werden Zero Trust-Bereitstellungen, die diesem Modell folgen, eine separate sichere Remote-Zugriffsfähigkeit benötigen – idealerweise als Teil der Zero Trust-Plattform.[10]

Wir erkennen an, dass es den Anschein haben könnte, dass wir die negativen Aspekte dieses Modells überbetont haben, aber wir möchten nicht, dass Sie diesen

[9]Der Verkehr „hinter“ dem PEP ist möglicherweise nicht verschlüsselt – er durchquert die implizite Vertrauenszone in seinem nativen Protokoll.

[10]Kommerzielle Zero Trust-Plattformen nähern sich diesem in der Regel mit einer Kombination aus einem Edge-PEP und einem erforderlichen Benutzeragenten-PEP. Seien Sie vorsichtig bei Architekturen, die dies außerhalb des Rahmens des Zero Trust-Modells lösen, wie zum Beispiel die Anforderung eines traditionellen VPN.

Eindruck bekommen – es gibt sicherlich erhebliche Vorteile dieses Ansatzes. Wir möchten nur sicherstellen, dass Sie sich dieser *potenziellen* Nachteile bewusst sind und Sie in die Lage versetzen, informierte Entscheidungen zu treffen und intelligente Fragen zu Ihrer Architektur oder Ihrem Zero Trust-Anbieter zu stellen. Wir verfolgen einen ähnlichen Ansatz bei den anderen Bereitstellungsmodellen, also tauchen wir ein und schauen uns das nächste an, das Enklaven-basierte Bereitstellungsmodell an.

Enklavenbasiertes Bereitstellungsmodell

Das zweite Modell ist das *enklavenbasierte Bereitstellungsmodell*, dargestellt in Abb. 3-6. In diesem Fall sitzt das PEP vor mehreren Ressourcen – bezeichnet als *Ressourcen-Enklave*. Diese Sammlung von Ressourcen kann physisch zusammen lokalisiert sein (z. B. in einem On-Premises oder Co-Located Data Center) oder logisch verwandt sein (z. B. eine Gruppe von Cloud-basierten oder virtualisierten Servern). Wie das vorherige Modell hat das Subjekt ein optional lokal installiertes Benutzeragent PEP.

Wichtig zu verstehen ist, dass in diesem Modell die implizite Vertrauenszone mehrere vernetzte Ressourcen enthält, die sehr wahrscheinlich untereinander

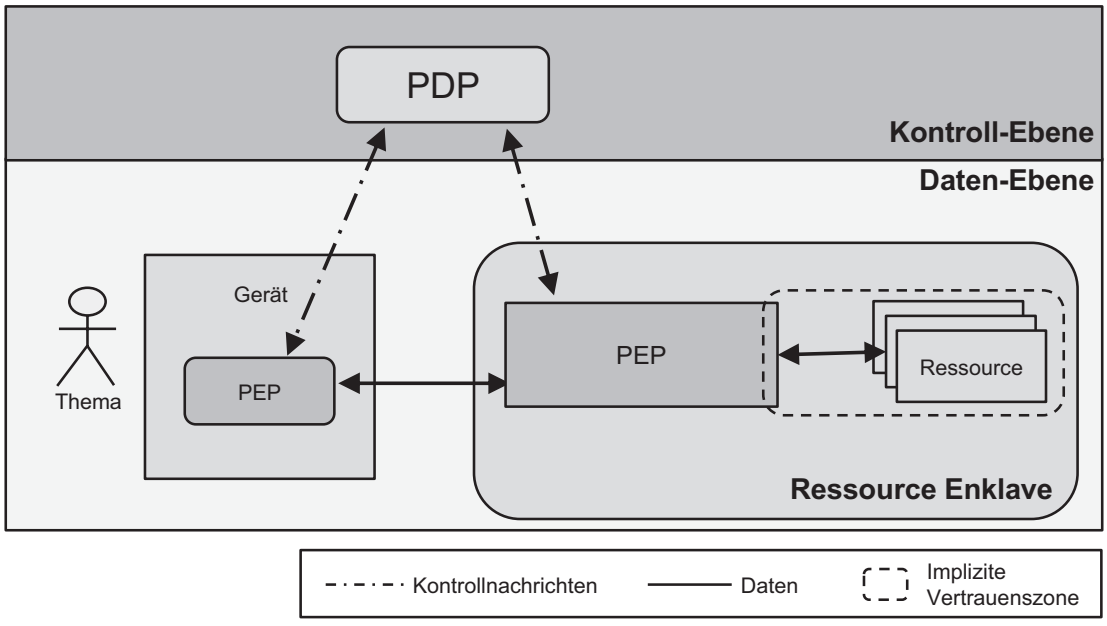

Abb. 3-6. *Enklavenbasiertes Bereitstellungsmodell*

kommunizieren. Das heißt, es ist entscheidend, dass in diesem Modell die Ressourcen-Enklave ausschließlich auf einem logischen privaten Netzwerk läuft, das unter der Kontrolle des Unternehmens steht. Wir sagen „logisch", da dies natürlich in einer öffentlichen IaaS-Umgebung oder einer gemeinsam genutzten Co-Located-Umgebung laufen kann, aber der Netzwerkverkehr ab Schicht drei und höher muss privat für das Unternehmen sein.

Obwohl die Ressourcen innerhalb der Enklave miteinander kommunizieren können und dies wahrscheinlich auch tun, außerhalb der Sichtbarkeit und Kontrolle des PEP, ist der einzige Weg für Subjekte außerhalb der Vertrauenszone, mit ihr zu kommunizieren, über das PEP, und daher wird dies durch die Richtlinie kontrolliert. Das heißt, mit diesem Modell müssen Unternehmen sicherstellen, dass sie die Daten- und Kommunikationsmuster der Ressourcen gründlich verstehen. Beachten Sie auch, dass dieses Bereitstellungsmodell eher einen „Benutzer-zu-Service"-Ansatz zur Zero Trust verfolgt.

Enklavenbasiertes Bereitstellungsmodell: Vorteile

- Einfacher PEPs zu implementieren – keine Änderungen an den Ressourcen.
- Weniger PEPs implementiert.
- Behandelt ephemere Workloads und dynamische Umgebungen gut.
- PEPs können am Rand des Netzwerks (DMZ) laufen und als natürliche Eingangspunkte dienen.

Dieses Modell ist im Allgemeinen einfacher zu implementieren als das vorherige, da es eine Größenordnung weniger PEPs gibt, dank der Eins-zu-vielen-Beziehung zwischen PEPs und Ressourcen. Die Eliminierung der Notwendigkeit, zusätzliche Software auf den Ressourcen zu implementieren, vereinfacht nicht nur die Dinge betrieblich, sondern vermeidet auch die meisten technischen oder politischen Konflikte mit Anwendungen und Anwendungsbesitzern. Es hat auch den Vorteil, dass die PEPs am Rand des Unternehmensnetzwerks implementiert werden können, so dass sie als natürlicher Eingangspunkt für Remote-Benutzer dienen können. Sie dienen natürlich auch als Policy Enforcement Point für lokale Benutzer, deren Verkehr vollständig innerhalb des Unternehmens bleibt.

Je nachdem, wie die PEPs implementiert sind, kann dieses Modell möglicherweise ephemere oder dynamische Workloads leicht unterstützen. Der Ansatz besteht darin,

dass die PEPs auf Änderungen unter den geschützten Ressourcen reagieren können, wie zum Beispiel durch die Erkennung der Instantiierung neuer Ressourcen und die Verwendung von Ressourcenattributen (Metadaten), um Richtlinien auf sie anzuwenden. Zum Beispiel könnte ein PEP, das eine On-Premises-Virtualisierungsumgebung schützt, einen API-Aufruf vom Hypervisor erhalten, der anzeigt, dass eine neue Instanz erstellt wurde. Basierend auf den Attributen dieser Instanz könnte das PEP sofort die richtige Richtlinie anwenden und nur dem autorisierten Satz von Benutzern Zugang gewähren. Ein PEP, das in einer IaaS-Umgebung eines Unternehmens läuft, kann genau dieselbe Funktion ausführen.

Enklavenbasiertes Bereitstellungsmodell: Nachteile

- Potenziell große, undurchsichtige oder lärmende implizite Vertrauenszone.
- PEPs stellen einen neuen Typ von Eingangspunkt in das Unternehmensnetzwerk dar.

Die größte Herausforderung bei diesem Modell ist die Größe und der Umfang der impliziten Vertrauenszone, die natürlich davon abhängt, wie und wo Sie diese PEPs implementieren. Mit einem fokussierten Satz von Ressourcen mit gut verstandenen und gut verwalteten Kommunikationswegen ist dieses Modell eine solide Grundlage für Zero Trust. Organisationen, die in neueren (insbesondere IaaS-basierten) Umgebungen arbeiten oder programmgesteuerte Infrastrukturen verwenden (wie DevOps), sind besonders gut für dieses Modell geeignet. Organisationen mit geringerer betrieblicher Reife, geringerer Sichtbarkeit oder komplexen Legacy-Netzwerken müssen möglicherweise mehr PEPs implementieren, um die Größe und den Umfang jeder impliziten Vertrauenszone zu reduzieren. Alternativ können sie einen hybriden Ansatz verfolgen, der von einigen Zero Trust-Anbietern unterstützt wird, indem sie dieses Modell mit dem später diskutierten Mikrosegmentierungsmodell kombinieren.

Ein weiterer potenzieller Nachteil dieses Modells ist weniger technisch, aber oft politischer. In diesem Modell wird das PEP typischerweise in der DMZ einer Organisation platziert, am Rand ihres Unternehmensnetzwerks. Das heißt, es ist absichtlich vom Internet aus zugänglich, dem am wenigsten vertrauenswürdigen Ort im bekannten Universum. Dies ist notwendig, damit Remote-Benutzer auf geschützte Ressourcen zugreifen können, stellt aber auch – wie ein VPN-Konzentrator – einen potenziellen Angriffsweg dar. Sicherheits- und Netzwerkteams sollten neue Edge-Geräte

bewerten und prüfen, aber manchmal lehnen sie aus nicht-technischen Gründen ab. Es ist wichtig, dass Zero Trust-Teams sich dessen bewusst sind und ausreichende Managementunterstützung für ihr Projekt erhalten, damit diese neuen Edge-Geräte fair und objektiv bewertet werden können. Als Randnotiz bieten einige Edge-PEPs tatsächlich eine bessere Netzwerksicherheit als traditionelle Edge-Geräte, so dass zukunftsorientierte Netzwerk- und Sicherheitsteams die Gelegenheit für Veränderung tatsächlich begrüßen sollten.

Cloud-Routed-Bereitstellungsmodell

In diesem nächsten Modell durchläuft der gesamte Verkehr vom Subjekt eine Cloud-Umgebung, bevor er letztendlich die Ressource erreicht, daher der Name "Cloud-Routed". Dieses Modell ist ein gängiger Ansatz, den viele kommerzielle Anbieter als Dienstleistung betreiben. Dieses Modell ist in Abb. 3-7 dargestellt.

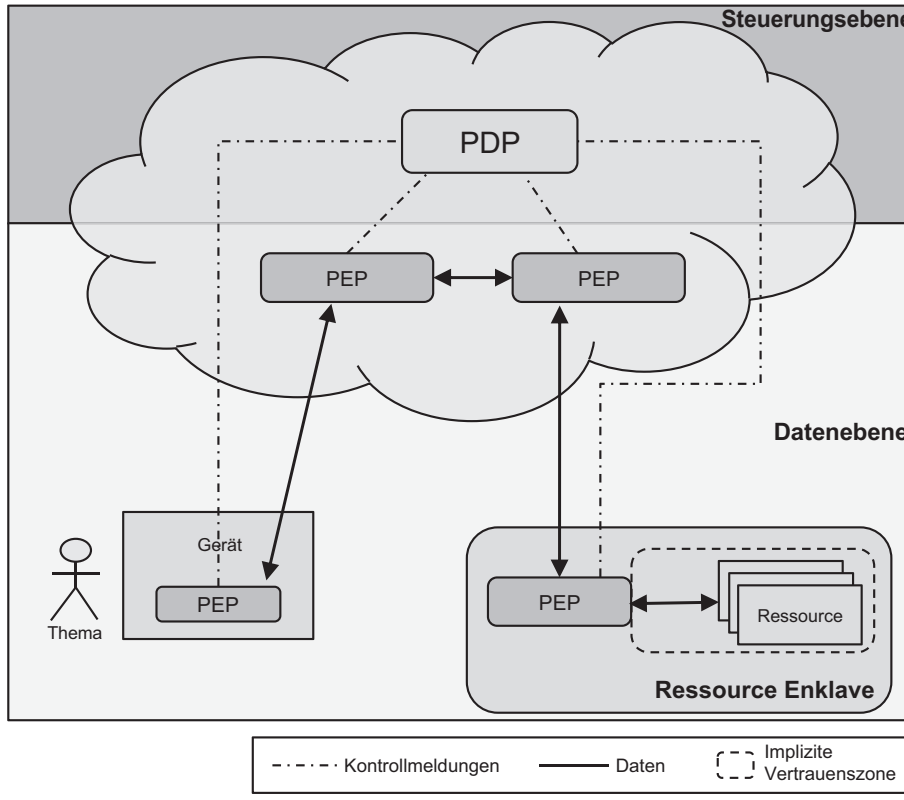

Abb. 3-7. *Cloud-Routed-Bereitstellungsmodell*

In diesem Modell agieren die PEPs, die vor den Ressourcen-Enklaven des Unternehmens sitzen, ähnlich wie die PEPs im hier gezeigten Modell. Diese PEPs haben jedoch einen wichtigen Unterschied – sie dienen nicht als Eingangspunkt in das Unternehmensnetzwerk. Diese Funktion wurde logisch auf die PEPs verschoben, die in der Cloud-Umgebung des Anbieters laufen. In diesem Modell fungieren die PEPs, die innerhalb des Unternehmens sitzen, als *Connectors,* die ausgehende Verbindungen zur Cloud-basierten PEP herstellen. Da diese On-Premises-Connectors keine eingehenden Verbindungen benötigen, vereinfachen sie oft die Bereitstellung dieses Modells – im Austausch gegen einige Einschränkungen, wie im folgenden Text besprochen.

Wenn das Subjekt mit der Ressource kommunizieren möchte, authentifiziert es sich zunächst beim PDP, und dann wird sein Verkehr zu einem der Cloud-basierten PEPs geleitet, in der Regel zu dem, der geografisch am nächsten liegt (oder vielleicht die geringste Latenz aufweist). Ihr Verkehr durchläuft dann die PEPs innerhalb der Cloud bis zum PEP, der eine Verbindung zur Zielressource Enklave hat. Der On-Premises-PEP sichert eine Ressourcen-Enklave genau so wie im vorherigen Modell.

Cloud-Routed-Bereitstellungsmodell: Vorteile

- Einfacher für Unternehmen einzurichten.
- As-a-Service-Plattform reduziert den operativen Aufwand für das Unternehmen.
- Einige Anbieter mit diesem Modell bieten auch einen Secure Web Gateway (SWG) Service an.

Da die On-Premises-PEPs in diesem Modell nur ausgehende Verbindungen herstellen, ist ihre Bereitstellung in der Regel sehr unkompliziert. Sie können auch die Prüfung durch Netzwerk- und Compliance-Teams vermeiden, da sie keine Änderungen an den DMZ-Firewall-Regeln erfordern oder die Bereitstellung von Software in der DMZ. Diese PEPs können überall innerhalb des Unternehmens bereitgestellt werden und bieten einen Remote-Zugriff auf dieses Netzwerk. Während dies ein potenzieller Vorteil ist, ist es auch ein potenzieller Nachteil. Teams dürfen diese technische Fähigkeit nicht als Ausrede oder Mittel nutzen, um die Sicherheits-, Netzwerk- oder GRC-Überwachung zu umgehen. Wenn sie als „Schatten-IT“ bereitgestellt werden, kann dies eine erhebliche Schwachstelle für die Organisation darstellen. Selbst nach der Genehmigung müssen die Sicherheitsteams natürlich eine angemessene Reihe von Richtlinien definieren und das Prinzip der geringsten Privilegien durchsetzen. Die einfache Bereitstellung darf keine Ausrede für schlechte Sicherheitskontrollen sein.

Schließlich kombinieren einige Anbieter mit diesem Modell es mit einem Secure Web Gateway Service, um den Benutzerzugriff auf öffentlich zugängliche Websites zu sichern. Diese Kombination kann für einige Unternehmen attraktiv sein, da sie die Bereitstellung und Betrieb vereinfachen kann.

Cloud-Routed-Bereitstellungsmodell: Nachteile

- PEPs können ohne angemessene Sicherheits-, Netzwerk- oder Compliance-Überwachung bereitgestellt werden.
- Fügt dem Benutzerverkehr Latenz hinzu.
- Unterstützt in der Regel nur begrenzte Netzwerkprotokolle.
- Nicht geeignet für On-Premises-Benutzer, die auf On-Premises-Ressourcen zugreifen.
- Potenziell große, undurchsichtige oder lärmende implizite Vertrauenszone.

Es gibt mehrere andere Nachteile dieses Modells, zusätzlich zum Risiko, dass dies zu einem „Schatten-IT"-Remote-Zugriff wird. Erstens muss der gesamte Benutzerverkehr die Cloud des Anbieters durchlaufen, was Latenz hinzufügt und möglicherweise den Durchsatz reduziert. Für einige Anwendungsfälle und Anwendungen kann dies ein ernsthaftes Hindernis sein. Sie müssen definitiv ein detailliertes Verständnis der Netzwerkleistung der Anbieterplattform erlangen und einige Tests durchführen, bevor Sie dies für Produktionsbenutzer bereitstellen. Zweitens unterstützen Cloud-Routed-Modelle in der Regel nur eine Teilmenge von Netzwerkprotokollen – am häufigsten nur TCP/IP (und in einigen Fällen nur einige Anwendungsprotokolle wie HTTPS, SSH und RDP). Wenn Ihre Benutzer und Anwendungen andere Protokolle benötigen, wie UDP, oder serverinitiierte Verbindungen zu Benutzern erfordern, passt dieses Modell möglicherweise nicht. Und wie das zuvor besprochene Enklaven-basierte Modell teilt dieses Modell die gleichen Vorsichtsmaßnahmen bezüglich der impliziten Vertrauenszone.

Am wichtigsten ist, dass dieses Modell im Allgemeinen nur für Remote-Benutzer gut geeignet ist, da der gesamte Verkehr die Cloud des Anbieters durchlaufen muss. Wenn Benutzer vor Ort sind und auf Ressourcen vor Ort zugreifen, muss ihr Verkehr unnötigerweise durch die Cloud des Anbieters "hairpinned" werden, was Latenz hinzufügt, den Durchsatz reduziert und die Bandbreitennutzung und Kosten des Unternehmens erhöht.

Microsegmentation Deployment Model

Das endgültige Implementierungsmodell konzentriert sich auf den Server-zu-Server-Anwendungsfall, bezeichnet als *Microsegmentation*. Dieses Modell nähert sich dem Problem aus der Perspektive von *Ressourcen* anstatt von *Benutzern*. Tatsächlich werden die Ressourcen in Abb. 3-8 als primäre Subjekte (Non-Person Entities, oder NPEs) betrachtet, um die die Richtlinien erstellt und durchgesetzt werden müssen. Wir stellen auch ein menschliches Subjekt dar, um die Vollständigkeit zu gewährleisten und weil viele der kommerziell erhältlichen Lösungen sie unterstützen, aber sie sind in diesem Modell typischerweise von sekundärer Bedeutung.

Dieses Modell ist tatsächlich eine Variante des ersten Modells, das wir zuvor besprochen haben – das ressourcenbasierte Modell – mit dem wichtigen Unterschied, dass die Ressourcen tatsächlich auch Subjekte (authentifizierte Identitäten) sind. Dies

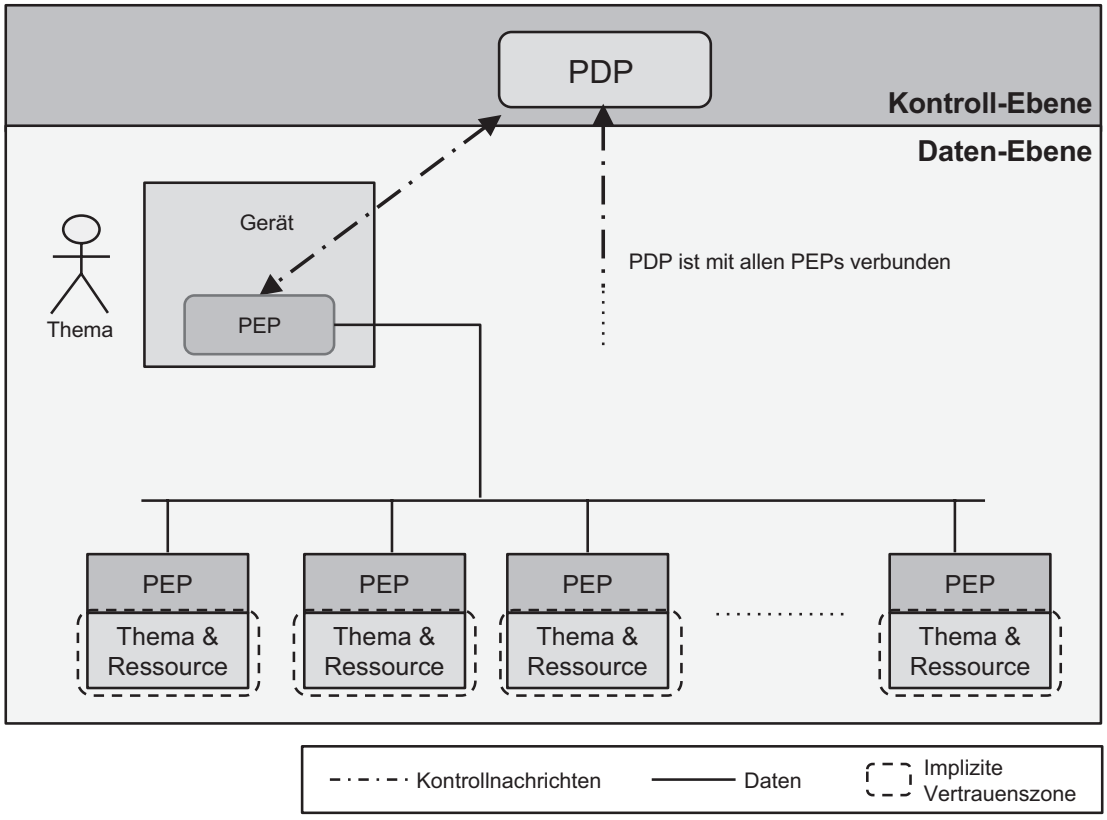

Abb. 3-8. *Microsegmentations-Implementierungsmodell*

hat erhebliche Auswirkungen auf das Richtlinienmodell und die Durchsetzungsfähigkeiten des PEP sowie auf die Ressourcenentdeckungs- und Visualisierungsfähigkeiten, die kommerzielle Implementierungen typischerweise bieten.

Im Allgemeinen haben die NPE-Subjekte schwächere Identitätsformen als menschliche Subjekte – oft zertifikatsbasiert und offensichtlich auf einem einzigen Authentifizierungsfaktor basierend.[11] Am häufigsten wird dieses Zertifikat von der Zertifizierungsstelle (PKI) des Unternehmens generiert und verwaltet.

Microsegmentation: Vorteile

- Kleine implizite Vertrauenszone
- Präzise, bidirektionale Kontrolle des Ressourcenzugriffs (für Server oder Mikrodienste)

Wie das erste Modell hat dieser Ansatz natürlich eine kleine implizite Vertrauenszone, die in der Regel nur auf die Ressource selbst beschränkt ist. Dadurch kann es eine feinkörnige Kontrolle des Ressourcenzugriffs bieten und bidirektionale Richtlinien durchsetzen. Das heißt, da der PEP lokal zur Ressource läuft, können seine Richtlinien sowohl ausgehende als auch eingehende Netzwerkkommunikation steuern. In kommerziellen Implementierungen können diese Richtlinien oft auf Ressourcen auf Serverebene sowie auf Mikrodienste angewendet werden.

Microsegmentation: Nachteile

- Erfordert die Bereitstellung der PEPs sowohl auf Benutzergeräten als auch auf Ressourcen.
- Potenzial für technische Konflikte zwischen Ressourcenkomponenten und PEPs.
- PEPs müssen auf eine große Vielfalt von möglicherweise veralteten oder Legacy-Betriebssystemen bereitgestellt werden können.
- Potenzial für Widerstand von Anwendungsressourcenbesitzern.
- Erfordert eine 1:1: Beziehung zwischen PEPs und Ressourcen.

[11] Obwohl man argumentieren könnte, dass die Tatsache, dass sie auf unternehmenskontrollierter Infrastruktur bereitgestellt werden, selbst ein zusätzlicher Faktor ist.

- Ist möglicherweise nicht gut geeignet für Benutzer-zu-Ressource Zugriff.
- Kein Remote-Zugriff ist eingebaut; es erfordert direkten Zugriff auf PEPs durch Subjekte.

Dieser Ansatz hat die gleichen Nachteile wie das erste Modell – nämlich die Bereitstellung und Verwaltung von PEPs auf jeder Ressource, die Schutz benötigt – daher werden wir die Diskussion hier nicht wiederholen. Es gibt auch einen weiteren möglichen Nachteil, nämlich dass eine auf diesen Bereich fokussierte Anbieter- (oder Open-Source-) Implementierung funktionale oder architektonische Mängel im Zusammenhang mit dem Benutzer-zu-Dienst-Szenario aufweisen kann. Dies kann für jede spezifische Implementierung der Fall sein oder auch nicht, aber Sie sollten dies definitiv in Ihre Liste der Bewertungskriterien aufnehmen.

Zusammenfassung

Obwohl die grundlegenden Konzepte von Policy Decision Points und Policy Enforcement Points schon seit einigen Jahren in der Branche kursieren, ist ihre Verwendung innerhalb eines Zero Trust-Sicherheitsmodells relativ neu. Wir ermutigen Sie, diesen Ansatz zu nutzen, um Ihr Denken und Ihre Architektur zu prägen und Ihre Anforderungen und Prioritäten zu bestimmen. Um dies zu tun, ist es wichtig, dass Sie beginnen, die bestehenden Komponenten in Ihrer Unternehmenssicherheitsarchitektur als PEPs in Ihrer entstehenden Zero Trust-Architektur zu betrachten. Dieses Buch ist zu diesem Zweck konzipiert – um Ihnen zu helfen, sie aus der Perspektive der Funktionen, die sie ausführen, zu betrachten, anstatt als getrennte Komponenten, die zufällig eine Reihe von Funktionen ausführen. Dies ist in etwa vergleichbar mit dem Sprichwort „Die Leute wollen keine Viertelzoll-Bohrer, sie wollen Viertelzoll-Löcher“ – der Fokus liegt auf dem Wert und nicht auf den Mitteln, ihn zu erreichen.

Um dies auf die Sicherheit zurückzuführen – anstatt zu denken „Ich brauche eine Firewall“, sollten Sie denken „Ich brauche einen Policy Enforcement Point, der den Netzwerkverkehr kontrollieren kann, und eine Möglichkeit, diese Richtlinie in meiner Infrastruktur zu definieren“. Oder, aus einem anderen Blickwinkel – anstatt zu denken „Ich muss hier ein IDS einsetzen, um meinen Web-App-Verkehr auf SQL-Injektionen zu untersuchen“, sollten Sie denken „Ich muss sicherstellen, dass der Web-App-Verkehr auf

SQL-Injektionen gescannt wird, bevor er von der App verarbeitet wird. Ich habe mehrere PEPs in meiner Architektur, die dieses Ziel erreichen könnten.“ Diese Denkweise sollte Ihnen auf Ihrer Reise helfen.

Dieses Kapitel lieferte viele Hintergrundinformationen zu Zero Trust-Architekturen – wir stellten eine repräsentative Unternehmensarchitektur vor und untersuchten sie, diskutierten eine generalisierte Zero Trust-Architektur, führten kurz ein Richtlinienmodell ein und untersuchten verschiedene Zero Trust-Implementierungsmodelle. Im nächsten Kapitel werden wir uns drei Fallstudien ansehen und untersuchen, wie diese Unternehmen Zero Trust in der Praxis angegangen sind.

KAPITEL 4

Zero Trust in der Praxis

Jetzt, da wir die Prinzipien von Zero Trust eingeführt und mehrere Modelle untersucht haben, werfen wir einen Blick auf einige reale Beispiele von Zero Trust-Systemen. Zwei davon – Googles BeyondCorp und das PagerDuty Zero Trust-System – wurden öffentlich beschrieben und sind gute Beispiele für Zero Trust-Architekturen und -Systeme, die intern in zwei sehr unterschiedlichen Unternehmen mit sehr unterschiedlichen Ansätzen implementiert wurden.

Wir können viel aus diesen Fallstudien lernen, auch wenn wir keine Zero Trust-Architektur einsetzen können, die einer dieser beiden entspricht. Da die ersten beiden Beispiele gut dokumentiert wurden, konzentrieren wir unsere Bemühungen darauf, ihre Perspektiven, Ziele und Kompromisse durch die Linse der Zero Trust-Prinzipien und -Architekturen, die wir gerade eingeführt haben, zu kontrastieren. Unser drittes Beispiel ist ein Unternehmen, das die Software-Defined Perimeter-Architektur erfolgreich genutzt hat, um Zero Trust zu erreichen, was uns helfen wird, die Vorteile dieses Ansatzes zu untersuchen. Lassen Sie uns eintauchen und einen Blick auf unsere erste Fallstudie werfen, das interne Google-Projekt, das wohl für viel Aufmerksamkeit in der Branche auf Zero Trust verantwortlich ist.

Googles BeyondCorp

BeyondCorp, Googles interner Name für ihre Netzwerksicherheits-Transformationsinitiative, ist eine bemerkenswerte Leistung und hat zurecht einen bedeutenden Einfluss auf die Branche gehabt. Google hat nicht nur ihre interne Sicherheitsarchitektur neu erfunden und Netzwerkzugriffskontrollen für Zehntausende von Benutzern bereitgestellt, sondern dies auch öffentlich in einer Reihe von USENIX

J. Garbis und J. W. Chapman, *Zero Trust Sicherheit*, https://doi.org/10.1007/979-8-8688-0105-1_4

;login: Artikeln dokumentiert, beginnend im Jahr 2014 und fortgesetzt über sechs Artikel bis 2018.[1]

Diese gut geschriebenen und gründlichen Artikel haben einen überproportionalen Einfluss auf die Branche gehabt, und es ist wichtig für uns, Google dafür zu würdigen, dass sie die Konzepte hinter Zero Trust gefördert haben. Wir ermutigen Sie, die Originalartikel zu lesen – wir geben hier nur einen kurzen Überblick. Im Grunde genommen hat Google über mehrere Jahre hinweg ein komplexes Zero Trust-System in großem Maßstab geschaffen und implementiert. Mit ihren Worten haben sie „ein neues Modell geschaffen, das auf ein privilegiertes Unternehmensnetzwerk verzichtet. Stattdessen hängt der Zugang ausschließlich von Geräte- und Benutzeranmeldedaten ab, unabhängig vom Netzwerkstandort des Benutzers…Der gesamte Zugang zu Unternehmensressourcen ist vollständig authentifiziert, vollständig autorisiert und vollständig verschlüsselt, basierend auf dem Gerätezustand und den Benutzeranmeldedaten."[2]

Das Endergebnis ihrer Reise ist, dass das Unternehmensnetzwerk kein inhärentes Vertrauen gewährt – der gesamte Zugang basiert auf Identität, Gerät und Authentifizierung, basierend auf robusten zugrundeliegenden Geräte- und Identitätsdatenquellen. Effektiv haben sie das *inhärente* Vertrauen in das Netzwerk durch *verdientes* Vertrauen in das Gerät ersetzt – sie haben ein echtes Zero Trust-Netzwerk, und alle internen Apps werden über das BeyondCorp-System aufgerufen, unabhängig davon, ob der Benutzer in einem Google-Büro oder remote arbeitet. Sie haben sich auch dafür entschieden, den Zugang nur von verwalteten Geräten zu erlauben – nicht verwaltete und BYOD-Geräte haben keinen Zugang zu internen Anwendungen. Es ist auch wichtig zu beachten, dass dieses Projekt ausschließlich auf die Kontrolle des Zugangs von Benutzern zu Servern ausgerichtet war, nicht auf Server-zu-Server.

Diese Designentscheidungen hatten mehrere Auswirkungen auf das Projekt – insbesondere ist es sehr abhängig von hochwertigen Daten rund um das Geräteinventar, und um dies zu unterstützen, haben sie eine ausgeklügelte Datenbank für das Geräteinventar erstellt. Sie verlassen sich auf unternehmenseigene Zertifikate, die in jedem Gerät im Trusted Platform Module (TPM) gespeichert sind, als Vertrauenswurzel

[1] Siehe `https://research.google/pubs/` und suchen Sie nach „BeyondCorp".
[2] „BeyondCorp: Ein neuer Ansatz für Unternehmenssicherheit," *;login: Dezember 2014, Vol. 39, Nr. 6.*

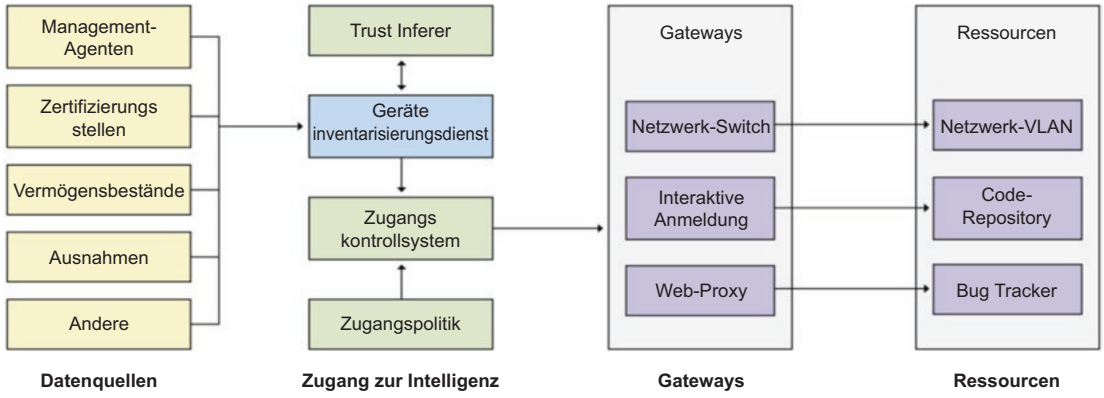

Abb. 4-1. *BeyondCorp Infrastrukturkomponenten*[3]

und nutzen auch ein zentralisiertes Identitätssystem mit SSO, das kurzlebige Zugriffstokens ausstellt. Ihr Identitätsmanagementsystem wird für Gruppen- und Rolleninformationen der Benutzer verwendet und versorgt ihre Policy-Entscheidungspunkte mit Identitätskontext. Und ihr Identitätssystem ist an HR-Prozesse gebunden, so dass es zuverlässig und aktuell ist. Die BeyondCorp-Infrastrukturkomponenten sind in Abb. 4-1 dargestellt.

Die Schlüsselelemente in BeyondCorp sind wie folgt. Erstens entsprechen die Datenquellen (logisch) den externen Datenquellen, die in den Zero Trust-Modellen in Kap. 3 dargestellt sind. Die Ressourcen entsprechen natürlich den Ressourcen in unserem Modell (und sind das, was NIST als Unternehmensressourcen bezeichnet). Google hat einen interessanten hybriden Ansatz mit den anderen beiden Abschnitten gewählt. Effektiv machen ihre *Access Intelligence* Komponenten den Policy Decision Point (PDP) aus, und ihre *Gateways* bilden den Policy Enforcement Point (PEP) – jedoch ist auch ihre Access Control Engine technisch gesehen Teil ihres PEP. Ihre Ressourcen können auch als Application PEPs fungieren, die feingranularen Zugang durchsetzen, abhängig von der Anwendung. Wir stellen diese überlagerte Ansicht in Abb. 4-2 dar, die Abb. 4-1 mit den Zero Trust-Architekturkomponenten kombiniert, die wir in Kap. 3 eingeführt haben.

Der BeyondCorp Access Proxy (bestehend aus den Gateways und einem Teil der Access Control Engine) fungiert als ein PEP, der sowohl für Remote- als auch für On-

[3]BeyondCorp: Design bis Einsatz bei Google, ;login: Frühjahr 2016 Vol. 41, Nr. 1.

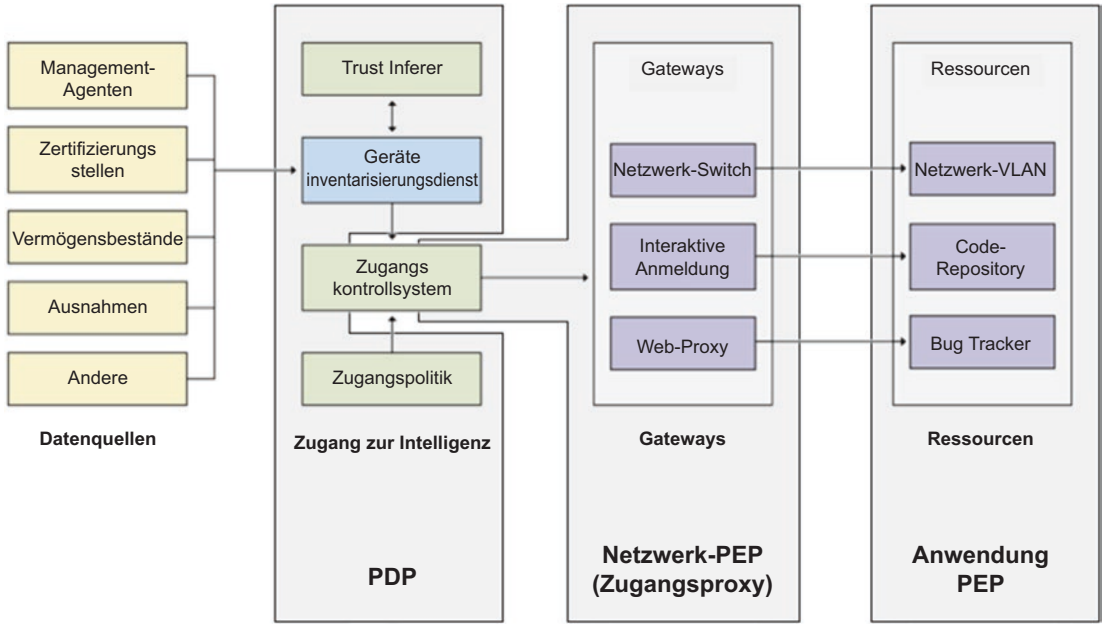

Abb. 4-2. *Annotierte BeyondCorp Infrastrukturkomponenten*

Premises-Benutzer weltweit zugänglich ist. Das System nutzt mehrere Datenquellen, um ein Vertrauensniveau zu etablieren, mit dynamischer Durchsetzung innerhalb des Access Proxies zum Zeitpunkt des Zugriffs. Dies ist ein großartiges Beispiel für dynamisches Verhalten und gut abgestimmt auf die NIST-Grundsätze – zum Beispiel Richtlinien, die Gruppenmitgliedschaft und Geräteattribute verwenden. Googles Artikel beschreiben die Access Control Engine, die Entscheidungen auf einer pro-Anfrage-Basis trifft. Dies ist interessant – einer von zwei Bereichen, in denen die BeyondCorp-Implementierung die Grenzen zwischen einigen der Komponenten verwischt, die in dem Zero Trust-Architekturmodell logisch unterschiedlich sind (dies ist üblich – wir werden später in diesem Kapitel ebenfalls einige unscharfe Linien sehen, wenn wir über den Software-Defined Perimeter sprechen).

Google beschreibt den Access Proxy als grobkörnige Durchsetzung an der Frontend, wobei die Autorisierung am Backend (innerhalb der Ressource) durchgesetzt wird, obwohl die Google-Artikel nicht spezifizieren, in welchem Maße die Anwendungs-PEPs in die Zugriffsrichtlinie oder in Datenquellen wie IAM eingebunden sind. Es ist interessant zu bemerken, dass ihr On-Premises Network Access Control System die dynamische VLAN-Zuweisung auf Basis von Gerätezertifikaten verwendet, um

verwaltete Geräte von nicht verwalteten Geräten zu unterscheiden. Obwohl sehr grobkörnig, ist dies eine effektive Methode, um ihr 802.1x-basiertes NAC in ihr Zero Trust-Netzwerk zu integrieren.[4]

BeyondCorp ist auch interessant, weil es das Enklaven-basierte Modell mit dem Ressourcen-basierten Modell kombiniert. Der Access Proxy verwendet HTTP-Header, um zusätzliche Sicherheitsmetadaten an die aufgerufenen Ressourcen zu übertragen. Die Schönheit der Verwendung von HTTP-Headern zur Übertragung dieser Metadaten besteht darin, dass sie von Ressourcen, die sie nicht erwarten oder nicht verarbeiten können, stillschweigend ignoriert werden. Dieser Ansatz reduzierte den Aufwand, dies über viele hundert Anwendungen bei Google auszurollen – es ermöglichte, dass die meisten Anwendungen ohne Änderungen onboarding konnten, während optional die Verwendung dieser Daten für verbesserte Sicherheit in einigen Anwendungen ermöglicht wurde. Beachten Sie, dass dieser Ansatz tatsächlich Steuernachrichten in die Datenplane mischt. Das ist nicht „falsch" – es ist eine kluge Designwahl, die innerhalb der BeyondCorp-Architektur viel Sinn macht und als Beispiel für die Wege dient, auf denen das konzeptionelle Zero Trust-Modell über viele verschiedene Implementierungsarchitekturen angepasst werden kann.

Das Google-Team gibt frei zu, dass BeyondCorp eine komplizierte, umfassende, mehrjährige Bereitstellung und organisatorische Umstellung war. Ein Teil des Grundes war die schiere Größe und Komplexität, die in Googles Organisation und Netzwerk inhärent sind. Ein weiterer Aspekt war, dass dieses Team ganz einfach ein Pionier war – es erfand, lernte, machte Fehler und iterierte während des gesamten Prozesses. Die gute Nachricht für den Rest der Sicherheitsbranche ist, dass sie so viel über ihre Implementierung geteilt haben und dass wir als Ganzes ein Ökosystem von kommerziellen und Open-Source-Tools, Technologien, Plattformen und Ansätzen geschaffen haben, die Unternehmen dabei helfen, viele der gleichen Vorteile schnell zu erzielen, basierend auf strukturierteren, vorhersehbareren und wiederholbaren Ansätzen.

Dies führt uns zur nächsten, offensichtlichen Frage – *Kann ich BeyondCorp für meine Organisation einsetzen?* Die Antwort darauf ist „Nein, und Ja". Klarerweise ist BeyondCorp ein internes Google-Programm und -Plattform, und es steht nicht zur Lizenzierung oder Wiederverwendung zur Verfügung. Ihre veröffentlichten Artikel

[4] Wir diskutieren NAC und 802.1x später, in Kap. 7.

erklären, wie tief BeyondCorp als Teil von Googles Unternehmensarchitektur, technischer Infrastruktur und HR-Prozessen eingebettet ist. Also, wenn Ihre Frage lautet *„Kann ich die BeyondCorp-Plattform für meine Organisation einsetzen?“* ist die Antwort „nein“. Aber eine bessere Frage ist *„Kann ich ein Sicherheitssystem einsetzen, das ähnliche Vorteile wie BeyondCorp für meine Organisation bietet?“* für die die Antwort ein klares „ja“ ist. Es gibt zahlreiche kommerzielle und Open-Source-Zero Trust-Lösungen zur Verfügung, die darauf ausgelegt sind, diese Vorteile zu liefern. Sie auf diese Initiative vorzubereiten und zu schulen ist natürlich das Hauptziel dieses Buches.

Tatsächlich hat Google einige Elemente von BeyondCorp kommerzialisiert – nicht die gesamte Plattform, aber einige Elemente – und sie als Teil ihrer Google Cloud Platform (GCP) über den Identity-Aware Proxy und BeyondCorp Enterprise Services zur Verfügung gestellt. Wir gehen davon aus, dass Google weiterhin innovieren und im Laufe der Zeit neue Fähigkeiten zu ihrem kommerziellen Angebot hinzufügen wird, so dass sie bei Ihrer Zero Trust-Evaluierung berücksichtigt werden sollten.

Wenn Sie an den Details und Denkprozessen des Google-Teams interessiert sind – in viel mehr Tiefe, als wir sie hier abgedeckt haben – empfehlen wir Ihnen, die ursprünglichen BeyondCorp-Artikel zu lesen. Als nächstes werden wir uns eine weitere interne Unternehmens-Zero Trust-Implementierung aus einer ganz anderen Perspektive ansehen.

PagerDutys Zero Trust Netzwerk

Die Fallstudie von PagerDuty, die erstmals im renommierten Buch *Zero Trust Networks* veröffentlicht wurde,[5] bietet einen soliden Kontrast zum BeyondCorp-Beispiel. Zunächst einmal konzentriert sich das Netzwerk von PagerDuty auf die Sicherung des Server-zu-Server-Zugriffs, im Gegensatz zum Fokus von BeyondCorp auf das Szenario Benutzer-zu-Server. Zweitens musste PagerDuty den Zugriff zwischen Ressourcen, die in mehreren öffentlichen Cloud-Umgebungen laufen, sichern, anstatt den Zugriff auf Ressourcen in einem Unternehmensnetzwerk zu schützen. Da diese unterschiedlichen Cloud-Plattformen eine breite Palette von Sicherheitsfunktionen (von gut bis schlecht) boten, vereinfachte ihr Zero Trust-System die Dinge, indem es als Normalisierungsschicht fungierte. Wir haben gesehen, dass Zero Trust-Systeme

[5]Evan Gilman und Doug Barth, *Zero Trust Networks* (O’Reilly, 2017).

innerhalb von Unternehmen einen ähnlich positiven Effekt haben, indem sie den Betrieb und die Konfiguration über ein einheitliches Richtlinienmodell in mehreren heterogenen und hybriden Umgebungen vereinfachen.

Das System von PagerDuty ist stark abhängig von ihrem Konfigurationsmanagement-System, das bereits vor ihrer Zero Trust-Initiative vorhanden war, um ihre virtuellen Server zu automatisieren und zu steuern. Dies war eine wichtige Grundlage für sie – es diente als „Quelle der Wahrheit" für alle ihre Ressourcen und auch als Automatisierungsplattform. Effektiv ist dies eine Kombination aus dem Policy Decision Point und dem Kontrollkanal. Interessant an diesem Punkt ist die Parallele zu BeyondCorp, wo die Quelle der Wahrheit eine Kombination aus ihrem rigorosen Gerätemanagementsystem und ihren Identitätssystemen war. Server-zu-Server Zero Trust-Systeme erfordern in der Regel eine solide Configuration Management Database (oder sie verlassen sich auf Netzwerkentdeckungsfunktionen), um einen autoritativen Ressourcenkatalog zu haben. Im Gegensatz dazu verlassen sich Benutzer-zu-Server-Systeme in der Regel auf Identitätsmanagement als ihre autoritativen Systeme.

Das Modell von PagerDuty verwendet einen zentralen PDP, der auf ihrem Konfigurationsmanagement- und Automatisierungssystem basiert.[6] Sie haben eine verteilte Reihe von PEPs, die tatsächlich lokale *iptables* Firewall-Regeln auf Hosts verwenden, was ihnen einen konsistenten Mechanismus für die Durchsetzung in unterschiedlichen Cloud-Umgebungen bietet. Dieser Ansatz sollte bekannt vorkommen – es ist im Grunde das Mikrosegmentierungs-Bereitstellungsmodell aus Kap. 3. In diesem Fall fungieren die eingebauten hostbasierten lokalen Firewalls als PEPs, unter der Leitung ihres Konfigurationssystems (der PDP). Ihre Plattform verwendet ein Netz von IPsec-Verbindungen zwischen allen Servern in ihrem Netzwerk, um Netzwerkprivatsphäre zu erreichen.

Dieses Modell und die Architektur haben nach allen Berichten gut für PagerDuty funktioniert, obwohl es nicht ohne Probleme war, wie man es bei jedem neu gebauten und komplexen System erwarten würde. Sie haben nicht viele Details über ihr Richtlinienmodell geteilt, aber im Grunde weisen sie jedem Server eine Rolle zu, die die Zugriffsregeln steuert, und alle Server in einer gegebenen Rolle haben identische Konfigurationen. Dieser Ansatz macht Sinn für eine Server-zu-Server-Umgebung – Server unterscheiden sich sehr von Benutzergeräten, da sie in der Regel an festen Standorten eingesetzt werden und zu 100 % unter der Kontrolle des Unternehmens

[6]Ursprünglich verwendeten sie Chef, später wechselten sie jedoch zu einem separaten System.

stehen. Das heißt, ein gut geführtes System – insbesondere eines, das von einem automatisierten Konfigurationssystem wie Chef gesteuert wird – hat die vollständige Kontrolle über das Image, die Konfiguration und das Netzwerk jedes Servers. Dies steht in starkem Kontrast zu Benutzergeräten, die in der Regel mobil sind, auf nicht vertrauenswürdigen Netzwerken und in nicht vertrauenswürdigen Umgebungen laufen und oft ein „wilder Westen“ von willkürlichen und einzigartigen Konfigurationen sind. (BYOD macht die Zugriffskontrolle von Benutzer zu Server noch herausfordernder).

Wir loben PagerDuty für ihre Innovation und möchten Evan und Doug dafür danken, dass sie sie in ihrem Buch mit uns geteilt haben. Dies war eine erfolgreiche Initiative für PagerDuty und ein interessanter Kontrast zu den Designentscheidungen und dem Problemraum im Vergleich zu BeyondCorp, angesichts ihres unterschiedlichen Fokus auf den Server-zu-Server-Anwendungsfall. Wir schätzen besonders ihren Ansatz, Richtlinien auf der Grundlage von Daten aus ihrem Konfigurationsmanagementsystem zu definieren, die eingelesen, bewertet und in Firewall-Regelsätze umgewandelt werden, die von den PDPs durchgesetzt werden. Richtlinien, die Metadaten von Zielressourcen als Eingabe verwenden, sind ein häufiges (und empfohlenes) Muster, das wir in Kap. 17 eingehend untersuchen.

Der Software-Defined Perimeter und Zero Trust

Der Software-Defined Perimeter (SDP) ist eine offene Sicherheitsarchitektur, die ursprünglich 2014 von der Cloud Security Alliance veröffentlicht und durch zusätzliche verwandte Publikationen erweitert wurde.[7] Die Architektur selbst ist neu, besteht aber aus bewährten Sicherheitselementen. Tatsächlich zogen die Autoren dieser ursprünglichen SDP-Spezifikation aus ihren Erfahrungen mit der Sicherung von klassifizierten (“high-side”) Netzwerken in der US-Geheimdienstgemeinschaft.

SDP ist darauf ausgelegt, mehrere Probleme in der Unternehmenssicherheit zu lösen und hat viel gemeinsam mit den Zielen von BeyondCorp und den Prinzipien von Zero Trust, die wir bereits vorgestellt haben: „SDPs erfordern, dass Endpunkte sich zuerst authentifizieren und autorisieren, bevor sie Netzwerkzugriff auf geschützte Server erhalten. Dann werden verschlüsselte Verbindungen in Echtzeit zwischen anfordernden

[7]Einer der Co-Autoren dieses Buches, Jason, ist derzeit Co-Vorsitzender der SDP Zero Trust Working Group bei der CSA. Er trat der Arbeitsgruppe 2015 bei, nach der Veröffentlichung der ursprünglichen Spezifikation.

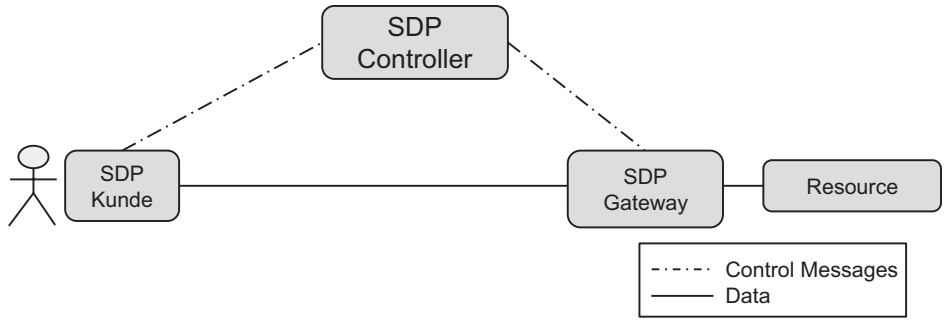

Abb. 4-3. *Software-Defined Perimeter Architektur*

Systemen und Anwendungsinfrastruktur erstellt."[8] SDP hat viele potenzielle Anwendungen, einschließlich identitätsgesteuerter Netzwerkzugriffskontrolle, Netzwerkmikrosegmentierung und sicherer Fernzugriff (für eine vollständige Liste siehe den *Software-Defined Perimeter Architecture Guide*[9]).

SDP ist eine Architektur mit mehreren Bereitstellungsmodellen (und mit mehreren kommerziellen Implementierungen verfügbar). Diese Bereitstellungsmodelle stimmen weitgehend mit den Zero Trust-Modellen überein, die in Kap. 3 beschrieben sind, und den Zero Trust-Konzepten. Das hochrangige SDP-Konzeptmodell ist in Abb. 4-3 dargestellt, das das Client-to-Gateway SDP-Bereitstellungsmodell zeigt, das für unsere Diskussionen hier am relevantesten ist.[10]

Es gibt mehrere Dinge zu beachten. Erstens, wie Zero Trust, stützt sich SDP auf unterschiedliche *Steuerungs-* und *Daten* Kanäle. Der SDP-Controller fungiert als Zero Trust Policy-Entscheidungspunkt und die SDP-Gateways sind Policy-Durchsetzungspunkte. Sie werden sofort bemerken, dass dieses SDP-Modell im Wesentlichen identisch mit dem Enklaven-basierten Zero Trust-Modell ist, das in Kap. 3 eingeführt wurde. Dies ist kein Zufall; das NIST Zero Trust-Team nutzte Ideen und Ansätze von SDP, als sie ihr Architekturdokument erstellten.

[8]Software-Defined Perimeter Specification 1.0, Cloud Security Alliance, 2014.
[9]Software-Defined Perimeter Architecture Guide, Cloud Security Alliance, 2019.
[10]Für eine Einführung in alle SDP-Bereitstellungsmodelle, siehe den Software-Defined Perimeter Architecture Guide.

SDP erfordert zwei Sicherheitskomponenten, die unserer Meinung nach in jeder Zero Trust-Bereitstellung enthalten sein sollten – *Gegenseitige TLS-Kommunikation*[11] und *Einzel-Paket-Autorisierung*, die wir als nächstes besprechen werden.

Gegenseitige TLS-Kommunikation

Gegenseitige TLS-Kommunikation, oder *mTLS,* ist einfach ein Ansatz, der sowohl vom Client (Verbindungsinitiator) als auch vom Server (Verbindungsakzeptor) verlangt, die Zertifikate des anderen zu validieren. Dies ist eine erhebliche Verbesserung gegenüber dem Standard-TLS (wie es beispielsweise durch eine Browserverbindung zu einem Webserver initiiert wird), bei dem nur der Client das Zertifikat des Servers validiert, aber nicht umgekehrt.

mTLS bietet eine erheblich verbesserte Sicherheit für das System und schließt im Wesentlichen die Möglichkeit eines Man-In-The-Middle-Angriffs aus und ermöglicht sichere Kommunikation selbst über die unzuverlässigsten Netzwerke. Natürlich setzt es voraus, dass eine gegenseitige Vertrauenswurzel für die kommunizierenden Parteien eingerichtet wird – eine Zertifizierungsstelle, der beide Komponenten vertrauen, um die Zertifikate auszustellen. Gegenseitige Authentifizierung wie mTLS muss in Zero Trust-Implementierungen vorhanden sein, als grundlegendes Element für sichere Kommunikation.

Einzel-Paket-Autorisierung

TCP/IP ist ein grundsätzlich offenes Netzwerkprotokoll, das darauf ausgelegt ist, die einfache Konnektivität und zuverlässige Kommunikation zwischen verteilten Rechenknoten zu erleichtern. Es hat uns gut gedient, um unsere hypervernetzte Welt zu ermöglichen, aber – aus verschiedenen Gründen – beinhaltet es Sicherheit nicht als Teil seiner Kernfähigkeiten.[12] Interessanterweise konzentriert sich viel von der Diskussion und

[11]SDP gibt an, dass die Verwendung von IPSec über IKE mit gegenseitiger Authentifizierung ebenfalls akzeptabel ist.

[12]Für eine faszinierende und nuancierte Analyse der Geschichte des Internets und seiner Sicherheitsherausforderungen empfehlen wir das Washington Post eBook *Das bedrohte Netz: Wie das Web zu einem gefährlichen Ort wurde* (insbesondere Teil I). Die talentierten und engagierten Menschen, die diese Internetworking-Protokolle erfunden haben, verdienen großen Respekt dafür, dass sie mit sehr begrenzter Technologie in den 1960er und 1970er Jahren etwas Erstaunliches geschaffen haben. Die Einbindung von Verschlüsselung wäre technisch unmöglich gewesen, angesichts der begrenzten Rechenkapazität der damaligen Zeit, und selbst jetzt, 50 Jahre später, gibt es keine gute, allgemeine Lösung für das Schlüsselverteilungsproblem.

Debatte über Netzwerksicherheit auf Verschlüsselung, anstatt auf eine andere Lücke – das „Verbinden vor Authentifizieren"-Modell.

Von Design her kann jedes Gerät, das IP-Netzwerkpakete mit jedem anderen Gerät austauschen kann, eine TCP-Verbindung herstellen, solange das zuhörende Gerät das hat, was man einen *offenen Port* nennt. Dies geschieht über den etwas berühmten dreifachen Handshake von TCP. Aus Sicherheitssicht ist das Wichtigste zu verstehen, dass diese Verbindungsherstellung rein auf Netzwerkebene erfolgt, ohne Identität, Authentifizierung oder Autorisierung. Die Schönheit dieses Modells besteht darin, dass es jedem mit einem Browser ermöglicht, sich problemlos mit jedem öffentlichen Webserver auf dem Planeten zu verbinden und eine Webseite aufgerufen zu bekommen, ohne dass eine vorherige Registrierung oder Erlaubnis erforderlich ist. Dies ist ein perfekter Ansatz für einen öffentlichen Webserver, aber ein schrecklicher Ansatz für eine private Anwendung und eine schreckliche Idee für einen Zugangspunkt mit breitem Zugang zu Unternehmensnetzwerken. Und doch ist dies genau die Art und Weise, wie Unternehmens-VPNs arbeiten – mit offenen Ports, die böswillige Benutzer einladen, sich zu verbinden und Schwachstellen auszunutzen. Leider ist dies keine theoretische Schwachstelle—Angreifer haben dies immer wieder erfolgreich erreicht,[13] und haben erfolgreich Unternehmensnetzwerke in erster Linie aufgrund der offenen Natur von TCP durchbrochen.

SDP überwindet diese Schwäche durch den cleveren Einsatz eines Einmalpasswort-Algorithmus basierend auf einem gemeinsamen Schlüssel, in dem, was als *Einzel-Paket-Autorisierung (SPA)* bezeichnet wird. Im Wesentlichen verwenden die Systeme ein OTP, das von einem Algorithmus erzeugt wird,[14] und betten das aktuelle Passwort in das erste Netzwerkpaket ein, das vom Client an den Server gesendet wird. Die SDP-Spezifikation erwähnt die Verwendung des SPA-Pakets nachdem eine TCP-Verbindung hergestellt wurde, während die Open-Source-Implementierung von den Erstellern von SPA[15] ein UDP-Paket vor der TCP-Verbindung verwendet. Kommerzielle SDP-Implementierungen können entweder Ansatz verwenden.

---

[13]Hier ist nur ein aktuelles Beispiel: www.zdnet.com/article/iranian-hackers-have-been-hacking-vpn-servers-to-plant-backdoors-in-companies-around-the-world/.

[14]SDP verwendet RFC 4226—HOTP: Ein HMAC-basierter Einmalpasswort-Algorithmus: https://tools.ietf.org/html/rfc4226.

[15]Siehe www.cipherdyne.org/blog/2012/09/single-packet-authorization-the-fwknop-approach.html.

In jedem Fall ist die Wirkung dramatisch, insbesondere bei UDP-basierter SPA – die betreffenden Server werden für nicht autorisierte Clients unsichtbar. Clients, die kein gültiges HOTP vorlegen, können keine TCP-Verbindung herstellen und (abhängig von der Implementierung) erhalten keine Bestätigung, dass überhaupt ein Server auf dem Port lauscht. Autorisierte Clients – die den gemeinsamen Schlüssel haben – können ein gültiges HOTP generieren, und der Server wird die Herstellung einer TCP-Verbindung erlauben (gefolgt natürlich von einer mTLS-Verbindung). SPA hat einen zusätzlichen Vorteil – es ist für Server sehr rechenleicht, nicht autorisierte Clients zu bewerten und abzulehnen. Es verbraucht um Größenordnungen weniger Serverressourcen, um ein 64-Bit-HOTP in einem UDP-Paket zu bewerten, im Vergleich zur Untersuchung der Authentifizierung nach dem Aufbau einer TCP- und TLS-Verbindung. Dies macht SPA-geschützte Server widerstandsfähiger gegen DDoS-Angriffe.

Schließlich, bedenken Sie, dass SPA zwar eine ausgezeichnete erste Verteidigungslinie ist, es ist jedoch nur die erste Schicht. Nach SPA, das dazu dient zu beweisen, dass der Client das gemeinsame Geheimnis besitzt, erfordert das SDP-System immer noch den Aufbau einer gegenseitigen TLS-Verbindung mit Zertifikatsvalidierung und Identitätsauthentifizierung, bevor der Zugang zu einer geschützten Ressource erlaubt wird.

SDP ist eine solide Architektur, die gut mit Zero Trust übereinstimmt. Das heißt, Sie können Zero Trust-Prinzipien mit einer Lösung erreichen, die auf der SDP-Architektur basiert. Obwohl SDP (als Spezifikation) begrenzt ist, gibt es kommerziell verfügbare SDP-Implementierungen, die die Lücken füllen und eine unternehmensbereite Plattform bieten. Als nächstes werden wir untersuchen, wie ein Unternehmen SDP für ihre Zero Trust-Reise genutzt hat.

SDP Fallstudie

In dieser Fallstudie untersuchen wir, wie ein US-amerikanisches multinationales Unternehmen ihren Zero Trust-Weg mit SDP angegangen ist. Dieses Unternehmen, das seit den 1970er Jahren tätig ist, bietet Dienstleistungen für Verbraucher an und hat weltweit über 14.000 Mitarbeiter. Frustriert über ihre traditionelle Sicherheitsinfrastruktur und inspiriert von BeyondCorp, startete ihr CISO eine strategische Zero Trust-Initiative. Sein Ziel war es, sensible Kundendaten besser zu sichern, Kosten zu senken und das Unternehmen in die Lage zu versetzen, neue digitale Plattformen für Medien und Kundenservice zu nutzen.

Ihre Infrastruktur bestand aus 2 primären Rechenzentren (eines in den USA und eines in Europa), 4 US-Niederlassungen zusätzlich zum Hauptsitz, 8 internationalen regionalen Niederlassungen und über 700 Einzelhandelsstandorten weltweit. Die Organisation unterstützte etwa 2000 Mitarbeiter in ihrer Hauptverwaltung, weitere 2000 Benutzer insgesamt in allen 12 regionalen Niederlassungen und etwa 10.000 Teilzeitmitarbeiter an den Einzelhandelsstandorten. Die Organisation hatte IaaS angenommen, mit mehreren Dutzend intern entwickelten Anwendungen, die von vor Ort migriert wurden und derzeit in der Cloud in Produktion liefen.

Ihre ursprüngliche IT-Infrastruktur litt unter einer Reihe von Mängeln, die alle mit ihrer strategischen Einführung von Zero Trust behoben werden sollten. Es ist jedoch wichtig zu beachten, dass sie dieses Projekt schrittweise angegangen sind und fast sofortigen Nutzen aus ihren Bemühungen gezogen haben. Tatsächlich war ein Teil der Bewertungskriterien dieses Unternehmens die Fähigkeit der Sicherheitsplattform ihres ausgewählten Anbieters, sich schnell in ihre bestehende Infrastruktur zu integrieren und ihre Entwicklung zu Zero Trust im Laufe der Zeit reibungslos zu unterstützen. Beispielsweise befand sich die Organisation in den frühen Stadien der Migration von einem vor Ort befindlichen Active Directory zu einem cloudbasierten SAML-Identitätsanbieter und benötigte ihre SDP-Plattform, um beide Anbieter gleichzeitig zu unterstützen.

Ein Schlüsselelement der Zero Trust-Initiative und -Vision war es, alle “off net” zu verschieben und eine verteilte Reihe von SDP-Gateways (PEPs) in ihrer heterogenen Unternehmensinfrastruktur zu verwenden. Das Sicherheitsteam bewertete eine Reihe verschiedener Zero Trust-Anbieter und -Lösungen und wählte eine unternehmensklassige SDP-Implementierung, die dem Enklaven-basierten Modell folgte.

Ihre erste Phase war ein taktischer Ersatz für ihr alterndes und problematisches VPN, das Verbindungsprobleme verursachte und Beschwerden von zwei Benutzergruppen hervorrief. Die erste Gruppe bestand aus etwa 750 allgemeinen Unternehmensbenutzern, die einen Remote-Zugriff auf Ressourcen im Unternehmensnetzwerk und im Hauptrechenzentrum benötigten. Die zweite Gruppe bestand aus etwa 250 Entwicklern, die SSH-, RDP- und Datenbankzugriff auf Dev-, Test- und Produktionsressourcen benötigten, die in einer IaaS-Cloud-Umgebung liefen. Obwohl diese erste Bereitstellung einfache, weit offene Richtlinien verwendete, brachte sie dennoch sofortige Vorteile, indem sie das Benutzererlebnis verbesserte, die Verbindungsgeschwindigkeiten erhöhte und den Sicherheits- und Netzwerkteams

Vertrauen und Erfahrung mit ihrer Zero Trust-Plattform gab. Es ermöglichte den Entwicklern auch gleichzeitigen Zugriff auf mehrere IaaS-Konten und Standorte bei gleichzeitiger Aufrechterhaltung der Sicherheit.

Nachdem diese Phase erfolgreich eingeführt worden war, begann das Sicherheitsteam, die Gruppenmitgliedschaft ihres cloudbasierten Identitätsanbieters zu nutzen, um den Zugriff für Unternehmensbenutzer im Netzwerk zu beschränken. Sie entwickelten nur wenige grundlegende Rollen, darunter Allgemeiner Mitarbeiter, IT, Finanzen, Netzwerkadministrator und Datenbankadministrator. Alle Mitarbeiter erhielten Zugang zu Standarddiensten (z. B. DNS, Druck, Dateifreigaben), während die anderen Gruppen Zugang zu rollenspezifischen Ressourcen gewährten.

Als Nächstes begannen sie, ihre 2000 regionalen Niederlassungsmitarbeiter vom Unternehmensnetzwerk zu entfernen und die Dinge so zu verschieben, dass ihr gesamter Zugriff durch Zero Trust-Richtlinien kontrolliert wurde. Im Wesentlichen wurden alle Netzwerk- und Sicherheitssoftware, Hardware und Verkabelung, die in diese 12 Niederlassungen eingesetzt wurden, entfernt und durch handelsübliches Geschäftsbreitband-Internet und Wi-Fi ersetzt. Da die überwiegende Mehrheit ihrer Produktionssysteme in einem einzigen Rechenzentrum im Nordosten der USA untergebracht war und Unternehmensbenutzer bereits einen sicheren Tunnel zu diesem Rechenzentrum benötigten, um auf Geschäftsanwendungen zuzugreifen, konnten sie bereits vorhandene Sicherheitssoftware nutzen, die IDS- und SWG-Funktionen für den Internet-gebundenen Verkehr der Benutzer im Rechenzentrum ausführte. Dies hatte den zusätzlichen Nebeneffekt, ihre Infrastruktur- und Kommunikationskosten um über 500.000 Dollar pro Jahr zu senken.

Für jede ihrer Niederlassungen implementierten sie ein lokales SDP-Gateway (Zero Trust PEP), das den Benutzern den Zugriff auf lokale Dateifreigaben ermöglichte, die durch Richtlinien kontrolliert wurden. Mit ihrer SDP-Systemarchitektur erhielten die Benutzer eine direkte, sichere Verbindung zum lokalen PEP für den Zugriff auf diese Dateifreigaben. Diese Architektur ermöglichte es, dass der Benutzerverkehr im Büro für die Dateifreigabe vollständig im lokalen Netzwerk verblieb.

Wie alle Organisationen wurde auch diese durch den Ausbruch der COVID-19-Pandemie Anfang 2020 erheblich beeinträchtigt. Alle ihre über 700 weltweiten Einzelhandelsstandorte mit über 10.000 Teilzeitmitarbeitern mussten vorübergehend geschlossen werden. Vor COVID verbanden sich diese Einzelhandelsmitarbeiter über das lokale drahtlose Netzwerk im Geschäft, das sie wiederum über ein Site-to-Site-VPN von jedem Geschäft zum Hauptunternehmensrechenzentrum mit zentralisierten

Anwendungsservern verband. Das Sicherheits- und Netzwerkteam reagierte schnell und implementierte den SDP-Client auf allen Geräten dieser Mitarbeiter, die eine Kombination aus unternehmensverwalteten und BYOD-Geräten waren. Diese Teilzeitbenutzer konnten sofort von zu Hause aus zu arbeiten beginnen und das Unternehmen unterstützen, als es schnell auf die virtuelle Bereitstellung ihrer Dienstleistungen umstellte. Ein interessanter Vorteil für diese Organisation war, dass sie dann den Prozess der Abschaltung der über 700 Site-to-Site-VPNs beginnen konnten, da nun der gesamte Benutzerzugriff über die sicheren SDP-Tunnel erfolgte. Dies wird voraussichtlich weitere Kosteneinsparungen für sie generieren, als einen weiteren Nebeneffekt.

Der nächste Schritt für diese Organisation auf ihrem Zero Trust-Weg besteht darin, den SDP-Client auf ihren Linux-Servern zu implementieren und das Mikrosegmentierungs-Bereitstellungsmodell für eine bessere Zugriffskontrolle in ihren Serverumgebungen zu verwenden.

Insgesamt hat diese Organisation klare und überzeugende Vorteile, sowohl sicherheitstechnisch als auch finanziell, durch die Einführung von Zero Trust durch eine Software-Defined Perimeter-Architektur erzielt. Ihre Unternehmensumgebung ist viel sicherer, da alle Benutzer "off net" sind und die Zugangspunkte zu ihrem Unternehmensnetzwerk für nicht autorisierte Benutzer verborgen sind. Die Pandemie hatte fast keine Auswirkungen auf ihre Vollzeit-Unternehmensbenutzer, da zu diesem Zeitpunkt fast alle die Zero Trust-Lösung nutzten und aus Netzwerksicht bereits immer "remote" waren.

Zero Trust und Ihr Unternehmen

Trotz der ersten beiden Fallstudien, die intern entwickelte Plattformen darstellen, möchten wir klarstellen, dass die meisten Unternehmen, insbesondere auf dem heutigen Zero Trust-Sicherheitsmarkt, den Ansatz des Unternehmens in der SDP-Fallstudie verfolgen. Das heißt, sie lizenzieren und verwenden kommerzielle Software, anstatt sie selbst zu implementieren, so wie Google und PagerDuty es getan haben. Als eine anspruchsvolle, hochprofitable und technisch fortschrittliche Organisation ist Google eindeutig in einer eigenen Liga, während das Kerngeschäft und die Kernkompetenzen von PagerDuty um den Betrieb eines komplexen, dynamischen

Netzwerks kreisen. Vielleicht am wichtigsten ist, dass beide Organisationen ihre Reisen begonnen haben, bevor es weit verbreitete kommerzielle Zero Trust-Plattformen gab.

Die heutige Welt ist anders. Beide Autoren arbeiten eng mit kleinen, mittleren und großen Unternehmen an ihrem Zero Trust-Ansatz zusammen – und sie setzen fast ausnahmslos auf kommerziell verfügbare oder Open-Source-Sicherheitslösungen als Kern ihrer Plattform, anstatt ihre eigene zu erstellen. Es gibt heute eine Vielzahl von fähigen Angeboten, und Unternehmen können und sollten eine Kombination aus Plattform, Best-of-Breed und vor Ort, cloudbasierten oder hybriden Modellen bewerten.

Beachten Sie auch, dass dieses Buch nicht das richtige Medium ist, um Anbieter- oder Open-Source-Angebote zu analysieren oder zu kritisieren – diese Produkte und Plattformen ändern sich ständig, da Anbieter neue Produkte und Innovationen einführen oder ergänzende Technologien erwerben. Aber dieses Buch *ist* das richtige Medium, um Ihnen ein solides Fundament der Zero Trust-Prinzipien zu bieten, ein Verständnis dafür, wie es in Ihrer Umgebung eingesetzt werden kann, und einen Satz von Anforderungen, aus denen Sie ziehen, formen und konsolidieren können. Letztendlich werden die Anforderungen in diesem Buch es Ihnen ermöglichen, die richtigen Entscheidungen für Ihr Unternehmen zu treffen.

Zusammenfassung

In diesem Kapitel haben wir drei verschiedene Fallstudien zur Implementierung von Zero Trust untersucht, die jeweils eine einzigartige Perspektive auf Zero Trust bieten. Googles internes BeyondCorp sicherte nicht nur ihr Unternehmen, sondern hatte dank der hervorragenden Bemühungen des Teams, ihre Erfahrungen zu veröffentlichen, einen signifikanten und positiven Einfluss auf die Branche. Die Fallstudie von PagerDuty bot eine weitere Perspektive darauf, wie eine service- und netzwerkzentrierte Organisation ihre Sicherheitsherausforderungen von Server zu Server bewältigte. Schließlich stellten wir den Software-Defined Perimeter vor, eine offene Architektur, die die Prinzipien von Zero Trust umsetzt. Nachdem wir beschrieben haben, wie SDP funktioniert, präsentierten wir eine Fallstudie über eine Organisation, die diese Architektur zur Bereitstellung von Sicherheits- und Betriebsvorteilen in ihrem multinationalen Unternehmen eingesetzt hat. Alle drei dieser Beispiele bieten

praktische Anleitungen und visionäre Elemente, die zeigen, wie Zero Trust-Sicherheit ein integraler Bestandteil dieser verschiedenen Arten von Organisationen gewesen ist. Sie sollten als Inspiration dienen und eine Quelle für Ideen sein, wie Ihre Organisation auf ihrer Zero Trust-Reise vorgehen kann.

TEIL II

Zero Trust und Komponenten der Unternehmensarchitektur

Im Teil I des Buches haben wir die Geschichte und den Hintergrund von Zero Trust vorgestellt, eine repräsentative Unternehmensarchitektur mit einer Zero Trust-Architektur verglichen und drei verschiedene Zero Trust-Fallstudien untersucht. Im Teil II werden wir die wichtigsten Funktionsbereiche der IT- und Sicherheitsinfrastruktur durch unsere Zero Trust-Linse betrachten. Für jeden werden wir seine Ziele und Funktionen diskutieren und untersuchen, wie diese sich ändern und in Ihre neue Zero Trust-Welt integriert werden sollten.

Während wir diese Analyse durchführen, möchten wir, dass Sie dies aus der Perspektive betrachten, wie Zero Trust in Ihrem Unternehmen eingeführt werden kann. Identifizieren Sie die technischen und nichttechnischen Einschränkungen in Ihrer Organisation, die zu Hindernissen werden könnten, und denken Sie darüber nach, wie Sie diese überwinden können. Und stellen Sie sicher, dass Sie die Auswirkungen von Zero Trust auf Netzwerke, Managementsysteme und Infrastruktur verstehen. Wenn Sie diese Dinge tun, sind Sie gut auf Ihre Reise zu Zero Trust vorbereitet.

KAPITEL 5

Identitäts- und Zugriffsmanagement

Identity and Access Management (IAM) ist ein breites Gebiet innerhalb der Informationssicherheit, das sowohl die technischen als auch die geschäftlichen Aspekte der Zugangskontrolle umfasst, indem es die richtigen Zugriffsrechte zur richtigen Zeit an die richtige Person vergibt. In vielerlei Hinsicht ist die Identität – und ein vernünftig geführtes Identitätsmanagementprogramm – der Schlüssel zum Erfolg eines Zero Trust-Programms. Zero Trust bietet im Kern einen identitätszentrierten Ansatz zur Sicherheit, und daher ist das Verständnis und die Verwaltung von Identitäten ein unglaublich wichtiger Faktor in jedem Zero Trust-Programm. Und dennoch sollten und dürfen sich Organisationen keinen unzumutbaren Standard auferlegen oder Perfektion von ihren Identitätsteams und -systemen verlangen, bevor sie ihre Zero Trust-Reise beginnen.

Identitätsmanagementsysteme sollten als autoritative Informationsquelle über Identitäten (Personen und nicht-personenbezogene Einheiten) dienen und als „Schlüssel"-System für viele technische Integrationen sowie Geschäftsprozesse verwendet werden. Das ist nicht einfach – die Unternehmen von heute sind komplex und verfügen möglicherweise nicht über ein einziges, zentralisiertes Identitätssystem. Das ist in Ordnung und sollte nicht als Hindernis für die Einführung von Zero Trust angesehen werden. Tatsächlich kann Zero Trust, durch seine Natur als Überlagerungssystem, helfen, die Lücken zwischen mehreren Identitätssystemen zu überbrücken. Wir werden dies später in diesem Kapitel im Abschnitt *IAM und Zero Trust* diskutieren. Aber zuerst geben wir einen Überblick über die Hauptkomponenten von IAM, die für die Diskussionen über Zero Trust im gesamten Buch grundlegend sind.

J. Garbis und J. W. Chapman, *Zero Trust Sicherheit*, https://doi.org/10.1007/979-8-8688-0105-1_5

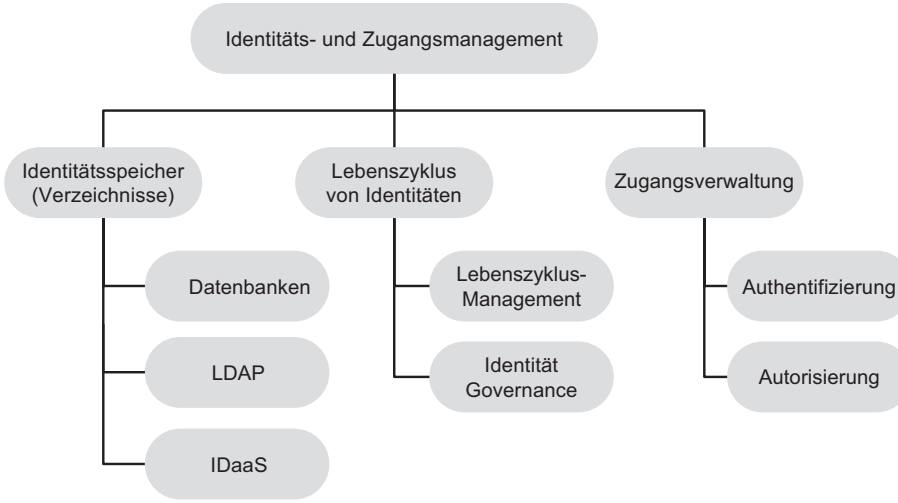

Abb. 5-1. *Identitätsmanagementsystem Umfang*

IAM im Überblick

Obwohl jedes Identitätsmanagementsystem unterschiedlich ist, basierend auf der einzigartigen Kombination jedes Unternehmens und seiner gewählten Technologien, enthalten Identitätsmanagementsysteme gemeinsame Elemente, die in Abb. 5-1 dargestellt sind. Lassen Sie uns jeden der Bereiche erkunden, für einen Rundgang durch die Breite der IAM-Programme.[1]

Identitätsspeicher (Verzeichnisse)

Das Kernelement jedes Identitätsmanagementsystems ist sein Identitätsspeicher, oft als *Verzeichnis* (formeller, ein *Verzeichnisdienst*). bezeichnet. Hier werden logischerweise die autoritativen Informationen über Entitäten[2] gespeichert – Attribute, die die Entität beschreiben und aussagekräftige Daten über die Entität liefern, die für den Gebrauch

[1]Beachten Sie, dass einige Organisationen dies als ICAM bezeichnen – Identity, Credential, and Access Management.

[2]Verzeichnisse speichern Entitäten und Attribute. Beachten Sie, dass Entitäten sowohl (menschliche) Benutzer als auch Nicht-Personen-Entitäten wie Server oder Dienste sein können, die ebenfalls authentifiziert werden und Berechtigungen erhalten. Wir haben dies kurz in Kap. 3 besprochen.

durch menschliche und automatisierte Konsumenten dieser Informationen bestimmt sind.

Verzeichnisse begannen Ende der 1980er Jahre formalisiert zu werden, teilweise getrieben durch die Einführung von PC-basierten lokalen Netzwerken in der Unternehmens-IT. Diese Verzeichnisse dienten dazu, Benutzer für den Netzwerkzugriff zu authentifizieren und stellten eine durchsuchbare und autoritative Liste von Informationen über Benutzer bereit. Dies beinhaltete Benutzeranmeldedaten, wodurch Verzeichnisse zu einer zentralisierten und zentral verwalteten Quelle wurden, gegen die Benutzer authentifiziert wurden.

Wir glauben, dass es fair ist zu sagen, dass aus dieser Kernverzeichnisfunktion das gesamte moderne IAM-Ökosystem gewachsen ist. Wie in vielen Bereichen, ist es auch standardisierter geworden, als es gereift ist. Für Verzeichnisse begann dieser Prozess mit der X.500-Spezifikation zur Speicherung von Entitätsinformationen, mit anfänglicher Konnektivität durch das Directory Access Protocol (DAP). Dies basierte nicht auf TCP/IP-Netzwerken und war für Clients sehr komplex zu nutzen, was zu einer begrenzten Akzeptanz führte. Als Reaktion darauf wurde eine „leichtere“ Version von DAP erstellt: Lightweight Directory Access Protocol (LDAP), das wir in Kürze besprechen.

Verzeichnisse und die Identitätsmanagementsysteme, die sie umgeben, haben in den letzten Jahrzehnten deutlich an Fähigkeiten und Umfang zugenommen. Die heutigen Verzeichnisse unterstützen viele verschiedene und komplexe Szenarien, einschließlich Metaverzeichnisse und föderierte Verzeichnisse, die mehrere disparate Verzeichnisse verbinden (wenn auch auf unterschiedliche Weise). Als nächstes stellen wir die drei hauptsächlich verwendeten Arten von Verzeichnissen vor.

Datenbanken

Datenbanken können technisch gesehen einen zentralisierten Identitätsspeicher bereitstellen, auf den über ein Netzwerk zugegriffen werden kann. Allerdings haben die meisten modernen Unternehmen davon abgesehen, rohe Datenbanken als ihre Verzeichnisse zu verwenden, aus mehreren Gründen. Fernanwendungen Datenbankzugriff auf Benutzerinformationen (insbesondere Anmeldedaten) zu geben, ist kein gutes Design, selbst wenn es nur lesbar ist.

Letztendlich stützen sich natürlich auch standardbasierte Verzeichnisse auf eine zugrunde liegende Datenbank. Aber es gibt einen signifikanten Unterschied zwischen

rohem Datenbankzugriff und standardisierten Protokollen und APIs zur Interaktion mit Verzeichnissen. Diese Arten von angepassten Identitätsspeichern müssen vermieden werden und sollten, falls vorhanden, im Rahmen einer Zero Trust-Initiative ausgemustert werden.

LDAP

Lightweight Directory Access Protocol (LDAP) ist eine Protokollspezifikation, die eine Reihe von Nachrichten (effektiv eine API) für die Interaktion mit Verzeichnisdiensten über ein Netzwerk definiert. LDAP ist ein etablierter Standard, der in einer Reihe von RFCs vom Internet Engineering Task Force (IETF) dargelegt ist.[3] LDAP v3, ursprünglich 1997 veröffentlicht, ist ein sehr erfolgreicher Standard, in dem Sinne, dass viele Verzeichnisanbieter (sowohl Open Source als auch kommerziell) das Protokoll unterstützen und Komponenten von verschiedenen Anbietern erfolgreich zusammenarbeiten können.

LDAP bietet eine einfache API für Operationen gegen die Menge der Entitäten im Verzeichnis und wird auch sehr häufig verwendet, um Benutzeranmeldedaten (Passwörter) zu authentifizieren. LDAP ist heute sehr weit verbreitet und unterstützt, mit breiter Unterstützung von Identitäts-, Sicherheits-, Anwendungs- und Infrastrukturanbietern. Zum Beispiel unterstützt Microsofts Active Directory – wohl das am weitesten verbreitete Verzeichnis in der Branche – eine LDAP-API.

Obwohl wir erwarten, dass LDAP-fähige Verzeichnisse und Anwendungen noch sehr lange erfolgreich laufen werden, glauben wir, dass neuere, standardbasierte Authentifizierungs- und Autorisierungsprotokolle LDAP mit der Zeit ersetzen werden. Insbesondere erfordert LDAP direkte API-Aufrufe an das Verzeichnis, während moderne Protokolle indirekte tokenbasierte Mechanismen unterstützen, die besser für die heutige verteilte Umgebung geeignet sind. Trotzdem ist es wahrscheinlich, dass Ihr Unternehmen weiterhin ein oder mehrere LDAP-basierte Verzeichnisse in Betrieb haben wird, und Ihre Zero Trust-Plattform muss in der Lage sein, mit diesen Diensten zu interagieren, ohne dass sie geändert werden müssen. Es ist nichts grundsätzlich Falsches daran, LDAP weiterhin zu verwenden, solange es Ihren funktionalen Bedürfnissen entspricht.

[3]Siehe https://tools.ietf.org/html/rfc4510 für das “Roadmap”-Übersichtsdokument des IETF.

Identity-as-a-Service

Der Wechsel zu cloudbasierten Diensten hat natürlich auch die Anbieter von Identitätsmanagement einbezogen, was zu einem erfolgreichen und schnell wachsenden Industriezweig namens Identity-as-a-Service (IDaaS) geführt hat. Diese Anbieter stellen cloudbasierte Verzeichnisse bereit, die Organisationen davon befreien, Verzeichnisserver vor Ort betreiben zu müssen, bieten eine moderne webbasierte Benutzeroberfläche und liefern benutzerfreundliche Funktionen wie Single Sign On (SSO) und zunehmend passwortlose Authentifizierung.

Diese Dienste bieten in der Regel sowohl neuere APIs wie SAML als auch ältere APIs wie LDAP und RADIUS. Diese Dienste sind gut positioniert für weiteres Wachstum, da die Akzeptanz und Reife von cloudbasierten Sicherheitsdiensten zunehmen. Beachten Sie, dass diese Anbieter in vielen Fällen vor Ort Software (Agenten) bereitstellen, um spezifische Funktionen auszuführen, einschließlich Föderation oder Datenreplikation und Integration mit älteren Verzeichnissen und Authentifizierungsschemata.

Letztendlich wird jede Organisation einen (und oft mehrere) Identitätsspeicher haben. Zero Trust-Systeme müssen sich damit integrieren und die Realität akzeptieren, dass Organisationen eine Möglichkeit benötigen, zu standardisieren und zu normalisieren über mehrere disparate Identitätsspeicher hinweg. Dies gilt insbesondere bei der Sicherung des Zugriffs für Dritte, mit ihren eigenen Identitätsspeichern. Wir werden dies weiter untersuchen, wenn wir *Authentifizierung* innerhalb des *Zugriffsmanagement*-Abschnitts dieses Kapitels besprechen. Davor möchten wir über den Identitätslebenszyklus sprechen, ein weiterer wichtiger Teil von IAM.

Identitätslebenszyklus

Jede Identität hat einen Lebenszyklus, ob er nun explizit und formal definiert ist oder nicht. Identitäten werden erstellt, sie existieren für einen bestimmten Zeitraum, sie haben möglicherweise im Laufe der Zeit verschiedene Rollen und schließlich werden sie zerstört. Organisationen müssen technische Werkzeuge und Geschäfts-/IT-Prozesse haben, um Identitätslebenszyklen zu verwalten und zu kontrollieren. Diese Bereiche innerhalb von IAM, bekannt als Lifecycle Management und Identity Governance, sind indirekt Teil einer Zero Trust-Initiative.

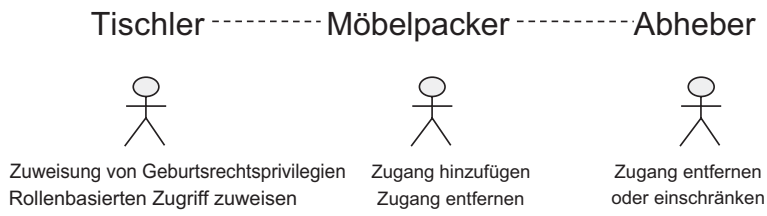

Abb. 5-2. *Der Benutzeridentitätslebenszyklus*

Lifecycle Management

Wenn wir über menschliche Benutzer sprechen, bezeichnen wir den Identitätslebenszyklus typischerweise als „Joiners, Movers und Leavers".[4] Eine menschliche Entität (Benutzer) durchläuft typischerweise den in Abb. 5-2 dargestellten Lebenszyklus. Dies beinhaltet die Bereitstellung von „Geburtsrecht"-Privilegien, die den Zugang darstellen, der automatisch zugewiesen wird, wenn jeder Benutzer *(Joiner)* erstmals in das Unternehmensverzeichnis aufgenommen wird. Natürlich erhalten Benutzer in der Regel Zugriffsrechte über diese hinaus, die auf der Grundlage der Rolle zugewiesen werden sollten. Organisationen müssen vorsichtig sein, Benutzern nicht übermäßig weitreichende Berechtigungen zuzuweisen, insbesondere den Fehler zu machen, die Rechte eines bestehenden Benutzers als Vorlage für neue Benutzer zu verwenden (das „Sally soll aussehen wie Jimmy"-Problem). Dies führt dazu, dass Benutzer mehr Zugang haben als notwendig, was potenziell Sicherheits- und Compliance-Probleme schafft. Ein gut geführtes Identitätsmanagementprogramm wird dieses Problem durch Rollen und Identitätsgovernance vermeiden, wie wir gleich besprechen.

Wenn ein Benutzer sich *(Mover)* innerhalb einer Organisation bewegt, entweder seitlich oder hierarchisch, ändert sich sein Zugang, da ihm im Rahmen seiner neuen Rolle zusätzlicher Zugang gewährt wird. Das Hinzufügen von Zugang ist unkompliziert – es gibt offensichtliche Auslöser dafür, da der Benutzer Zugang benötigt (und fordert), um seine neue Arbeit zu erledigen. Das Entfernen von Zugang ist subtiler, insbesondere da es in der Regel eine Übergangszeit gibt, in der ein Benutzer sowohl neuen als auch alten Zugang benötigt. Da dieser Zeitraum Wochen oder Monate dauern kann, müssen

[4]Es ist allgemein vorzuziehen, Mitarbeiter als „beitretend" und „verlassend" zu bezeichnen, anstatt als „erstellt" und „zerstört".

Geschäftsprozesse vorhanden sein, um dies zu verfolgen und zu verwalten (dies ist in der Regel Teil eines Identitätsgovernance-Programms).

Benutzer in der letzten Lebenszyklusphase sind als *Leavers* bekannt. Diese Phase kann aus verschiedenen Gründen eingeleitet werden, einschließlich geplanter freiwilliger Abgang (Wechsel zu einem anderen Job oder Ruhestand) oder unfreiwilliger Abgang (sofortige Kündigung). In vielen Fällen werden Benutzer für eine bestimmte Zeit in einem Identitätsmanagementsystem existieren, zum Beispiel, damit Manager auf die E-Mail des ausgeschiedenen Mitarbeiters zugreifen können. In einigen Fällen können ausgeschiedene Benutzer für längere Zeiträume (z. B. um auf persönliche Gehalts-, Versicherungs- oder Steuerunterlagen zugreifen zu können) oder sogar auf unbestimmte Zeit in Systemen existieren (wie z. B. ein *Student,* der zu einem *Alumnus* einer Bildungseinrichtung wird).

Ein Identitätsmanagement System muss die Zuweisung, Bereitstellung und Deaktivierung des Benutzerzugriffs auf der Grundlage dieser Lebenszyklusereignisse verwalten und idealerweise automatisieren. Die meisten Organisationen machen einen guten Job bei HR und Payroll Onboarding und Offboarding. Die damit verbundenen IT-Prozesse hinken jedoch oft in Reife und Effektivität hinterher. Zum Beispiel ist es anekdotisch ungewöhnlich, dass Menschen weiterhin bezahlt werden, nachdem sie eine Organisation verlassen haben. Es ist jedoch recht häufig, dass Benutzer nach ihrem Ausscheiden Zugang zu IT-Systemen (insbesondere zu SaaS-Anwendungen) behalten.

Die Verwaltung von nicht-menschlichen Konten (Service-Konten) erfordert eine etwas andere Art von Sorgfalt, da diese Systeme in der Regel von offensichtlichen externen oder HR-getriebenen Auslösern, wie Einstellung oder Entlassung, getrennt sind. Service-Konten sind einfach Konten, die für Server oder Infrastrukturcode erstellt werden, anstatt für menschliche Benutzer.[5] Diese nicht-menschlichen Zugangsmechanismen können nicht nur Konten, sondern auch andere Zugangskontrollmechanismen wie API-Schlüssel oder Zertifikate umfassen.

Wie bei regulären Benutzerkonten müssen diese Konten Privilegien und Rollen haben, die aktiv verwaltet werden müssen. Auch wie bei Benutzerkonten müssen diese Konten nur das minimale Set an Privilegien haben. Dies ist oft eine größere Herausforderung für Service-Konten, da sie oft systemweite Aktivitäten durchführen und

[5]Die Wiederverwendung von Benutzeranmeldedaten für Service-Konten oder in Skripten ist eine außergewöhnlich schlechte Idee.

es möglicherweise kein robustes Modell gibt, um ihre Privilegien im Zielsystem zu begrenzen. Allzu oft werden diesen Konten volle Admin-Rechte gewährt, entweder aus Notwendigkeit oder aus dem Bedürfnis, ein Problem schnell zu lösen („Keine Sorge…wir werden es später beheben"). Und diese Kontodaten werden oft geteilt, im Klartext gespeichert und in der Regel nicht rotiert. Der klare Schluss ist, dass Service-Konten in die Identitätsgovernance-Prozesse einbezogen werden müssen, genau wie Benutzerkonten, und dass Zero Trust-Systeme verwendet werden sollten, um Zugriffsrichtlinien für diese Konten durchzusetzen. Beachten Sie, dass Privileged Access Management (PAM) Lösungen oft Service-Konten-Tresore und Dienste haben, die bei der Lösung einiger dieser Probleme helfen können. Wir werden PAM in einem späteren Kapitel behandeln.

Identitätsverwaltung

Die Richtlinien (oder, wenn Sie so wollen, Regeln), die bestimmen „wer Zugang zu was bekommen sollte" als Teil des zuvor diskutierten Identitätslebenszyklus, werden als *Identitätsverwaltung* bezeichnet und sind ein weiterer Teil des typischen Umfangs von IAM-Programmen. Die Verwaltung wird in der Regel sowohl durch Compliance- als auch durch Sicherheitsanforderungen getrieben, oft mit einem stärkeren Compliance-Treiber. In vielen Fällen konzentrieren sich diese Compliance-Anforderungen auf Finanzanwendungen und -kontrollen, insbesondere bei börsennotierten Unternehmen.

Anbieter auf diesem Markt haben Produkte zur Identitätsverwaltung entwickelt, um bei der Erfüllung dieser Compliance-Anforderungen zu helfen, und Unternehmen setzen diese Lösungen in der Regel als Teil ihrer Initiativen zur Identitätsverwaltung ein. Natürlich haben nicht alle Organisationen formelle Programme zur Identitätsverwaltung – kleinere oder unregulierte Unternehmen benötigen sie möglicherweise nicht. Aber *alle* Organisationen treffen Entscheidungen darüber „wer Zugang zu was haben sollte" – entweder implizit oder explizit – als Teil der Prozesse des Identitätslebenszyklus. Letztendlich werden diese Entscheidungen als Änderungen an den zugrunde liegenden Softwaresystemen umgesetzt – wie Änderungen an Benutzerattributen oder Gruppenmitgliedschaften in Verzeichnissen oder die Erstellung, Löschung oder Autorisierungsänderungen an Benutzerkonten innerhalb von Anwendungen.

Diese Zugriffskontrollentscheidungen können durch ein Bereitstellungssystem automatisiert oder durch manuelle IT- und Geschäftsprozesse implementiert werden. In

beiden Fällen müssen die Richtlinien zur Identitätsverwaltung mit den Zero Trust-Richtlinien abgestimmt sein. Wir werden dieses Thema und die Beziehung zwischen diesen Schichten im folgenden Text untersuchen, wenn wir über Autorisierung sprechen.

Zugriffsmanagement

Zugriffsmanagement steht im Mittelpunkt des Identitätsmanagements und besteht aus zwei Hauptkomponenten: erstens, die Mittel, mit denen Entitäten beweisen, dass sie sind, wer sie behaupten zu sein, *Authentifizierung,* und zweitens, das Modell zur Definition und Ausdruck der Menge an Aktionen, die eine gegebene Entität ausführen darf, *Autorisierung*. Schauen wir uns jede dieser Komponenten genauer an.

Authentifizierung

In diesem Abschnitt geben wir eine kurze Einführung in gängige Authentifizierungsprotokolle, -mechanismen, -standards und -trends. Wir tun dies, um ihre Relevanz innerhalb von Zero Trust-Bereitstellungen zu untersuchen. Beginnen wir mit einigen grundlegenden Definitionen, die zur Klarheit beigefügt sind:

- Benutzername/Passwort: Einfache Authentifizierung, die seit Jahrzehnten in Gebrauch ist. Dies ist das Prinzip der Validierung von *etwas, das Sie wissen*.
- Mehr-Faktor-Authentifizierung (MFA): Die Verwendung von mehr als einem Authentifizierungsfaktor als Teil eines Authentifizierungsprozesses. Hierbei wird oft ein physischer Token, eine Smartphone-App oder ein biometrischer Mechanismus verwendet, um *etwas zu validieren, das Sie haben, oder etwas, das Sie sind*.
- Stufenweise Authentifizierung: Der Prozess, bei dem ein Benutzer nach einem zusätzlichen Authentifizierungsformular gefragt wird, nachdem ein Ereignis oder Auslöser stattgefunden hat. Dies kann beispielsweise ausgelöst werden, wenn ein bereits authentifizierter Benutzer versucht, auf eine hochwertige Ressource zuzugreifen.

Hierbei wird oft eine Form von MFA verwendet, da sie auf der bereits erfolgten Authentifizierung des Benutzers basiert.

- Passwortlose Authentifizierung: Dies ist ein allgemeines Prinzip, bei dem Faktoren außer Passwörtern für die anfängliche Authentifizierung verwendet werden. Wir begrüßen und fördern diese Änderung, da sie die bekannten Risiken im Zusammenhang mit schwachen Passwörtern, Passwortdiebstahl und Passwortwiederverwendung beseitigt. Diese Lösungen verwenden oft die zuvor unter MFA aufgeführten Mechanismen.

Jetzt schauen wir uns einige Authentifizierungsprotokolle und -mechanismen an, die derzeit in Gebrauch sind.

LDAP

Wir haben LDAP zuvor eingeführt, da es sich um eine API handelt, die sowohl als Mittel zur Interaktion mit Verzeichnissen als auch zur Authentifizierung von Benutzern verwendet werden kann. Aus Sicht der Authentifizierung beinhaltet die LDAP-API eine native Unterstützung für die Authentifizierung auf Basis von Benutzername und Passwort, die üblicherweise verwendet wird. Die LDAP-API enthält einen Erweiterungsmechanismus, durch den andere Authentifizierungstypen hinzugefügt werden können, über einen Herausforderungs-Antwort-Mechanismus. Diese werden häufig verwendet, sind aber implementierungsabhängig (nicht standardisiert).

RADIUS

RADIUS ist ein weiteres älteres Authentifizierungsprotokoll – sein Alter zeigt sich deutlich in seinem Namen; es ist ein Akronym für *Remote Authentication Dial-In User Service*. Es wurde ursprünglich geschaffen, um Authentifizierung, Autorisierung und Abrechnung (AAA) zu bieten, im Grunde genommen Vorläufer des heutigen Identitätsmanagements. Während der Begriff AAA heute nicht mehr so weit verbreitet ist, sind diese Themen eindeutig Teil der heutigen Mainstream-Identitäts- und Sicherheitsinitiativen.

Trotz seines Alters wird RADIUS heute noch weit verbreitet eingesetzt. Als Teil mehrerer offizieller IETF-Standards (RFCs) wird es von vielen Anbietern unterstützt und bietet eine vernünftige Interoperabilität zwischen Komponenten verschiedener

Anbieter. Wie LDAP hat RADIUS ein einfaches Modell, bei dem ein RADIUS-Client (typischerweise als „Netzzugangsserver“ bezeichnet) direkt mit einem RADIUS-Server interagiert, um die Authentifizierung im Auftrag eines Prinzipals (in der Regel eines Benutzers) durchzuführen. RADIUS gibt nur ein *akzeptieren* oder *ablehnen* zurück (möglicherweise nach einer zusätzlichen *Herausforderung,* die MFA ermöglicht). RADIUS kann verwendet werden, um Identitätskontext über eine Protokollerweiterung bereitzustellen, obwohl wir dies nicht in breitem Einsatz gesehen haben.

RADIUS unterstützt jedoch standardbasierte Authentifizierungsmechanismen über Benutzername und Passwort hinaus, und seine Fähigkeit, dies zu tun, hat sicherlich seine Lebensdauer verlängert. Tatsächlich bieten viele moderne Identitätsanbieter RADIUS-APIs oder Gateways an, die es älteren Anwendungen oder Infrastrukturen ermöglichen, in diese neueren Plattformen integriert zu werden. Mit diesem Ansatz können ältere Systeme die neueren MFA- oder passwortlosen Authentifizierungsansätze verwenden, die auf modernen Identitätsplattformen unterstützt werden, die durch RADIUS aufgerufen werden können.

SAML

Das Security Assertion Markup Language (SAML) entstand aus dem Wunsch und der Notwendigkeit innerhalb der Branche, einen zuverlässigen, vertrauenswürdigen und interoperablen Weg zu haben, um Single Sign On (SSO) für Benutzer in Webanwendungen zu ermöglichen, insbesondere für Web-Apps von verschiedenen Anbietern. Formeller definiert SAML eine XML-Darstellung und ein HTTP-basiertes Protokoll, mit dem Webanwendungen („Dienstanbieter“ in SAML-Sprache) Benutzerauthentifizierungs- und Attributinformationen von einem separaten Identity Provider (IdP) konsumieren können. Das heißt, zusätzlich zur Authentifizierung des Benutzers können die SAML-Antwortdaten (bekannt als *Behauptungen*) zusätzliche Informationen über den Benutzer enthalten, die von der Web-App angefordert und vom Identity Provider bereitgestellt werden.

Als Standard war SAML ein großer Erfolg – mit breiter Akzeptanz sowohl bei Identity Providern als auch bei SaaS und privaten Web-Apps, was einen reichen Marktplatz für SSO von Identity-as-a-Service-Anbietern ermöglicht. Als ein einfacher und zuverlässiger Standard, der eine leicht konfigurierbare Vertrauensbeziehung zwischen Web-Apps und IdPs ermöglicht, ist es ein großartiges Beispiel für einen *Netzwerkeffekt* bei dem der Wert der Unterstützung des Standards mit jedem zusätzlichen unterstützenden Spieler steigt.

Mit einer breiten Palette von Open-Source-Toolkits und Plug-Ins gibt es keine Entschuldigung dafür, dass Web-Apps SAML nicht unterstützen. Ebenso müssen Zero Trust-Lösungen die breite Akzeptanz von SAML-fähigen Identity Providern anerkennen und SAML als Authentifizierungsmechanismus unterstützen.

SAML bietet die Möglichkeit, Attribute, Gruppenmitgliedschaften und Rollen als „Ansprüche“ innerhalb einer SAML-Antwort zu unterstützen. Dies erhöht den Wert seiner Verwendung in Verbindung mit einer Zero Trust-Umgebung, da diese Ansprüche offensichtlich eine primäre Quelle von Identitätskontext für den Verbrauch durch Zero Trust-Richtlinien sind (im Wesentlichen Eingabe in RBAC- und ABAC-Zugriffskontrollmodelle).

OAuth2

OAuth2, ein Standard, der von der IETF definiert wurde,[6] ist als Mechanismus für Entwickler konzipiert, um Autorisierungsprotokolle zu erstellen, damit eine Drittanwendung auf eine begrenzte Menge von Funktionen oder Ressourcen innerhalb einer Webanwendung zugreifen kann, im Auftrag eines Benutzers. Zum Beispiel könnte ein Benutzer einem Fotodruckdienst Zugriff auf seine privaten Fotos auf einer Foto-Sharing-Site gewähren, ohne seinen Benutzernamen und sein Passwort teilen zu müssen. Formeller ist OAuth2 eine Möglichkeit für einen Client, ein Sicherheitstoken von einem vertrauenswürdigen Token-Dienst (typischerweise ein IdP) zu erhalten und dieses Token an eine vertrauende Partei zur Verwendung zu übertragen. Beachten Sie, dass dies grundsätzlich auf der vom Benutzer erteilten Erlaubnis basiert.

Technisch gesehen ist OAuth2 ein Autorisierungsprotokoll und kein Authentifizierungsprotokoll. OpenID Connect, das wir als nächstes besprechen, ist ein Beispiel für ein Authentifizierungsprotokoll, das auf OAuth2 aufbaut.

OpenID Connect (OIDC)

OIDC basiert auf OAuth2 und verwendet ein JSON Web Token (JWT)[7] als sein Token. Es ist darauf ausgelegt, Authentifizierung auf OAuth-Autorisierung hinzuzufügen und wird am häufigsten von Web-Apps verwendet, um Authentifizierung und Autorisierung unter

[6] OAuth2 ist in RFC 6749 und 6750 definiert.

[7] JWT ist ein offenes Standard-Framework, das in RFC 7519 definiert ist, um Ansprüche sicher zwischen zwei Parteien zu definieren.

Verwendung des zugrunde liegenden OAuth-Frameworks zu bieten, basierend auf einem interoperablen REST-Format. Ein OIDC-Token enthält vertrauenswürdige Ansprüche über den Benutzer, zur Verwendung innerhalb der Zielanwendung (vertrauende Partei).

Zertifikatsbasierte Authentifizierung

Aus der Sicht des Unternehmensidentitätsmanagements werden Zertifikate (und ihre unterstützenden Systeme) oft verwendet, um die Identität von Benutzern und Geräten zu validieren – der Besitz eines gültigen Zertifikats kann eine Entität positiv identifizieren. In der Praxis bedeutet dies für Benutzergeräte, dass ein bestimmtes Benutzergerät ein gültiges und aktuelles Zertifikat installiert hat, dass dieses Zertifikat von der eigenen Zertifizierungsstelle des Unternehmens (Teil seiner Public Key Infrastructure) ausgestellt wurde und dass der Benutzer sich in das Desktop- oder mobile Betriebssystem einloggen kann auf eine Weise, dass das Zertifikat – gesichert im lokalen Schlüsselverwaltungssystem des Betriebssystems – für das Konto des Benutzers zugänglich ist. Nicht-Benutzergeräte, wie Server oder IoT-Geräte, haben jeweils ihren eigenen Mechanismus, mit dem das besitzende Unternehmen Zertifikate installieren und sie zur Identifikation und Authentifizierung verwenden kann. Schließlich enthalten einige physische Ausweiskarten unternehmenseigene Zertifikate, die durch Eingabe einer PIN durch einen Benutzer abgerufen und als Form der Mehrfaktorauthentifizierung verwendet werden. Häufige Beispiele dafür sind die CAC (Common Access Card) und die PIV Card (Personal Identity Verification), die in den US-Regierungs- und Verteidigungssektoren verwendet werden.

FIDO2

FIDO2 ist ein aufkommender Standard, der das „passwortlose“ Erlebnis für die Endbenutzergemeinschaft durch FIDO Universal Authentication Framework (UAF) und zwei Varianten der Client-to-Authenticator-Protocols (CTAP1 und CTAP2) bringt. Durch diese Protokolle, die auf PKI basieren, unterstützt FIDO2 Browser, mobile Geräte und Hardware-Fobs als Mittel zur Authentifizierung.

Mobil und Biometrie

Obwohl sie natürlich keine Authentifizierungsstandards sind, nutzen moderne Authentifizierungsmethoden zunehmend benutzerfreundliche und/oder auf mobilen Geräten basierende Technologien zur Benutzerauthentifizierung. Endbenutzer sind mit Technologien wie Fingerabdruckerkennung oder Gesichtserkennung auf ihren mobilen Geräten vertraut, und mobile Apps zur Generierung von Einmalpasswörtern (OTP) haben im Allgemeinen ihre hardwarebasierten Varianten ersetzt.

MFA ist ein großer Teil von Zero Trust, und mobile Geräte sind eine zuverlässige und benutzerfreundliche Möglichkeit, einen zweiten Faktor durchzusetzen. Tatsächlich erwarten Endbenutzer angesichts der unglaublichen Benutzerfreundlichkeit, die Verbraucheranwendungen jetzt bieten (wie kontaktlose Zahlung), das gleiche Maß an Komfort in ihren Unternehmens-IT-Systemen.

Leider ist es nicht immer einfach oder unkompliziert, dies zu erreichen, da die Unternehmens-IT ein komplexeres Problem löst als die Authentifizierung und Autorisierung einer einfachen, einmaligen Kreditkartentransaktion. Unternehmenssicherheitssysteme authentifizieren in der Regel Benutzer und autorisieren den Zugriff auf Geschäfts- oder technische Anwendungen für Minuten oder Stunden. Die Unternehmens-IT ist auch in der Regel durch eine komplexere Netzwerktopologie mit vielen Einschränkungen behindert. Trotzdem funktionieren diese Standards und Technologien gut, und wir beginnen eine breitere Akzeptanz und Priorisierung der Verwendung neuerer Authentifizierungsmittel zu sehen und uns von Passwörtern zu entfernen. Zero Trust-Sicherheitsarchitekturen, mit ihrem inhärent dynamischen und ganzheitlichen Umfang und ihren umfangreichen Integrationsmöglichkeiten, helfen dabei, dies zu beschleunigen.

Autorisierung

Autorisierung ist das Endziel des Zugriffsmanagements, das schließlich dafür verantwortlich ist, von einem bestimmten Richtlinienmodell (technische oder Geschäftsrichtlinie) zu Durchsetzungspunkten zu mappen. Wenn es richtig gemacht wird, bieten Identitätsmanagementsysteme autoritative Merkmale – Rollen und Attribute – die mit Entitäten verbunden sind und haben Governance-Richtlinien und Prozesse, um sicherzustellen, dass diese korrekt sind.

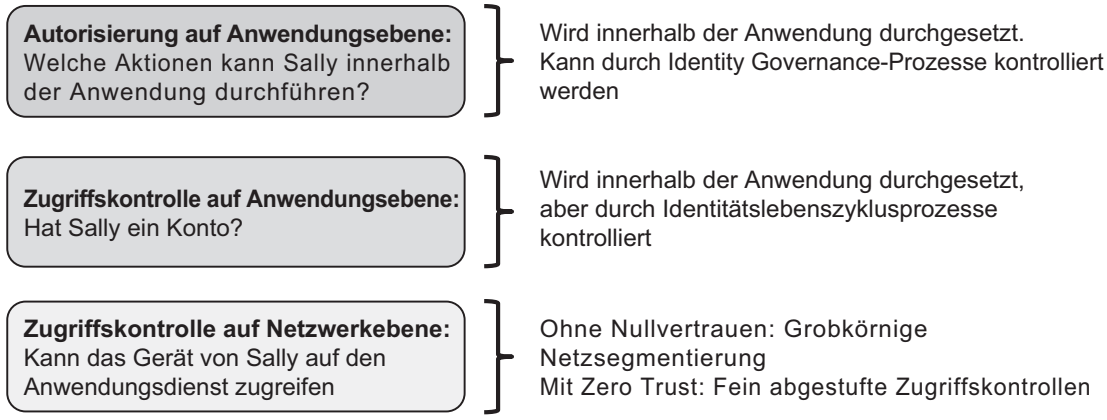

Abb. 5-3. *Zugriffskontrollebenen*

Natürlich sind diese Attribute nur dann sinnvoll, wenn es Laufzeit-IT-Komponenten gibt, die diese Richtlinien tatsächlich korrekt durchsetzen können. Zum Beispiel bedeutet es nicht, dass Sally tatsächlich eine Astronautin ist, nur weil sie in einer Verzeichnisgruppe namens „Astronauten" ist.[8] Ebenso hat Sallys Mitgliedschaft in der Verzeichnisgruppe „ABC123" keine inhärente Bedeutung. In beiden Fällen kommt es darauf an, wie der Rest des IT-, Anwendungs- und Sicherheitssystems diese Informationen interpretiert und wie es Sallys Konten und Zugriff beeinflusst. In der Praxis erfolgt die Autorisierung auf mehreren Ebenen, wie in Abb. 5-3 dargestellt.

Oben steht das Anwendungsebene *Autorisierungs* Modell, das steuert, welche Aktionen unser Benutzer (in diesem Fall Sally) innerhalb der Anwendung ausführen kann. Dies wird in der Regel direkt innerhalb der Anwendung durchgesetzt,[9] basierend auf den Rollen oder Berechtigungen, die mit Sallys Konto verbunden sind. Beachten Sie, dass es vielleicht am einfachsten ist, über die „Anwendung" als eine

[8]Wir ermutigen Sie jedoch, dies selbst in Ihrem Unternehmensverzeichnis auszuprobieren. Bitte lassen Sie uns wissen, ob dies funktioniert, da wir sehr daran interessiert wären, die Ergebnisse zu replizieren.

[9]Es gibt eine relativ kleine Anzahl von Anwendungen, die ihr Autorisierungsmodell externalisieren. Selbst mit Standards wie XACML hat dieser Ansatz bei traditionellen Anwendungsarchitekturen nicht signifikant an Marktanteil gewonnen. Interessanterweise ist eines der Schlüsselelemente, die Zero Trust bietet, effektiv die Externalisierung des **Netzwerk** Autorisierungsmodells. Netzwerkinfrastrukturen haben im Vergleich zu Anwendungen ein sehr armes Autorisierungsmodell, und Zero Trust ist eine Möglichkeit, dieses durch ein viel reichhaltigeres Richtlinienmodell zu ersetzen. Wir werden dies später im Buch ausführlich behandeln.

Geschäftsanwendung nachzudenken, wie ein Finanzmanagementsystem, aber dieses Modell ist genauso anwendbar, wenn die betreffende Anwendung technischer ist, wie ein Quellcode-Repository oder ein Datenbanksystem, oder sogar ein völlig anderer Dienst, wie ein SSH-Login in einen Server. In jedem Fall werden reifere Organisationen einen Satz von Identitätsgovernance-Prozessen haben, mit zugehörigen Tools, um die Autorisierung auf Anwendungsebene zu validieren und durchzusetzen. Weniger reife Organisationen werden dies in der Regel auf eine eher ad-hoc-Art und Weise tun, basierend auf einfachen oder vordefinierten Anwendungsrollen.

Die mittlere Schicht kann als Anwendung *Konto* Ebene betrachtet werden – im Grunde genommen wird der Anwendungszugriff durch das Vorhandensein oder Fehlen eines bestimmten Benutzerkontos in der Anwendung gesteuert. Diese Schicht erfordert, dass der Benutzer gültige Anmeldeinformationen vorlegt, um auf die Anwendung zugreifen zu können. Das heißt, der Zugriff wird über die Authentifizierung durchgesetzt. Beachten Sie, dass viele Zugriffskontrolllösungen auf dieser Ebene arbeiten, einschließlich Single Sign On (SSO) und Privileged Access Management (PAM) Lösungen.

Diese ersten beiden Schichten repräsentieren den traditionellen Umfang und die Grenze des Identitätsmanagements, mit einer im Allgemeinen klaren Trennung von der zugrunde liegenden Schicht der *Netzwerk-Ebene* Zugriffskontrolle. Ohne Zero Trust konnten Sicherheits- oder Netzwerkteams in der Regel nur auf eine statische, grobkörnige Weise Zugriffskontrollen durchsetzen – wie zum Beispiel Benutzer einem gesamten Virtual LAN (VLAN) zuzuweisen, das Hunderte oder Tausende von Hosts umfasst, ganze Netzwerke mit WANs wie MPLS oder Standort-zu-Standort-VPNs remote zu verbinden, oder Remote-Benutzern vollen Netzwerkzugriff über Benutzer-VPNs zu geben. Mit Zero Trust kann die Netzwerkschicht feinkörnige Zugriffskontrollen durchsetzen, basierend auf Rollen und Attributen, die in traditionellen Sicherheitssystemen nur auf der Anwendungsebene verfügbar und wirksam sind.

Während wir unseren *IAM im Rückblick* Abschnitt abschließen und den Übergang zur Diskussion über Zero Trust und IAM beginnen, möchten wir kurz Rollbasierte Zugriffskontrolle (RBAC) und Attributbasierte Zugriffskontrolle (ABAC) diskutieren. Dies sind Begriffe, die den allgemeinen Ansatz beschreiben, die Zugriffskontrolle auf Attribute zu basieren, die mit einer Identität verbunden sind, die typischerweise von einem Identitätsmanagementsystem erhalten werden. (Technisch gesehen kann eine Rolle einfach als eine bestimmte Art von Attribut betrachtet werden, und somit kann

ABAC als umfassend für RBAC betrachtet werden). Der „Kontroll“ Teil von ABAC bezieht sich auf die Fähigkeit einer Organisation, Zugriffsrichtlinien zu definieren, die logische Bedingungen ausdrücken können, unter denen eine Identität berechtigt ist, auf eine bestimmte Ressource zuzugreifen.

Wenn das bekannt vorkommt, sollte es – attributbasierte Richtlinien sind genau das, was Zero Trust durchsetzt. Tatsächlich würden wir argumentieren, dass Zero Trust-Architekturen der effektivste Weg sind, um attributbasierte Zugriffskontrolle zu erreichen. Letztendlich ist ABAC nur ein Konzept, das in einer konkreten Architektur ausgedrückt werden muss, auf einer Plattform, die Organisationen ein reiches Vokabular bietet, um diese Zugriffskontrollrichtlinien auszudrücken. Es ist dieses Richtlinienmodell – sein Umfang, seine Fähigkeit und seine Wirksamkeit – das im Mittelpunkt jeder Zero Trust-Initiative stehen sollte. Wir diskutieren dies mehr nächstes.

Zero Trust und IAM

Jetzt, da wir IAM und seine Komponenten überprüft haben, wollen wir untersuchen, warum und wie IAM für Zero Trust wichtig ist. Denken Sie daran, dass IAM-Systeme vom Zero Trust PDP verwendet werden, um Entitäten zu authentifizieren und als Quelle von Kontext (Rollen und Attribute) für die Entscheidungsfindung in Bezug auf Richtlinien zu dienen. Wie wir bereits diskutiert haben, sind wir glücklich, dass Menschen in unserer Branche eine Vielzahl von standardisierten Authentifizierungs-APIs und -Protokollen erstellt haben. Diese haben eine weit verbreitete Akzeptanz erreicht, so sehr, dass wir uns auf unseren Identitätsanbieter und die Zero Trust-Plattform verlassen können, um zu interagieren. Zero Trust-Plattformen müssen neben der Verwendung der bestehenden IAM-Systeme von Unternehmen für die Benutzerauthentifizierung in der Lage sein, Identitätskontext von ihnen zu erhalten, damit PDPs Zugangsentscheidungen treffen können. Noch einmal, dies unterstreicht, warum die Unterstützung für Standardprotokolle (insbesondere LDAP und SAML) eine Anforderung für Zero Trust-Systeme ist.

Beachten Sie, dass diese Prinzipien unabhängig vom gewählten Zero Trust-Bereitstellungsmodell (oder den Modellen) gelten. In allen Fällen müssen Zero Trust-Systeme mit Identitätssystemen integriert sein – dies ist das Herzstück dessen, was diesen Sicherheitsansatz so viel effektiver macht als traditionelle Ansätze. Lassen Sie uns kurz Zero Trust mit traditionellen Ansätzen vergleichen, was unserer Meinung nach

nicht nur die Identitätsintegration und Zero Trust, sondern auch den Gesamtwert von Zero Trust im Kern verdeutlicht.

Authentifizierung, Autorisierung und Zero Trust-Integration

Abb. 5-4 zeigt drei Szenarien, in denen ein Benutzer auf eine Anwendung zugreift. In allen Fällen hat der Benutzer ein Konto bei der Anwendung, muss sich authentifizieren und hat eine bestimmte Reihe von Privilegien, die er innerhalb der Anwendung

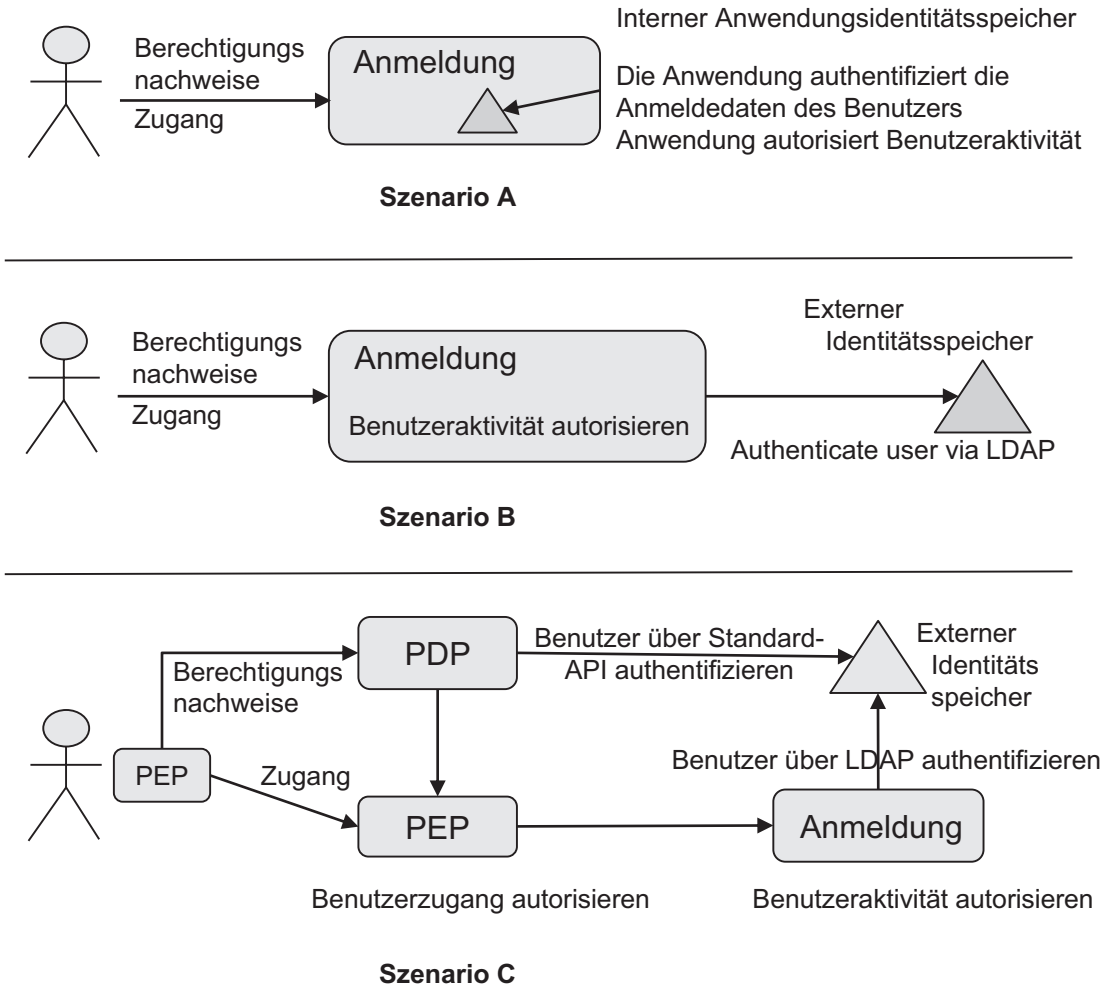

Abb. 5-4. *Authentifizierung, Autorisierung und Zero Trust*

ausführen kann. Wenn es sich beispielsweise um ein Content-Management-System (CMS) für Websites handelt, kann der Benutzer möglicherweise Seiten bearbeiten, aber nicht in der Lage sein, bearbeitete Seiten in die Produktion zu übernehmen. Interessant sind jedoch die Unterschiede zwischen den drei Szenarien aus Sicherheits- und Integrationssicht.

Szenario A zeigt eine klassische, eigenständige Anwendung mit ihrem eigenen internen Identitäts- und Anmeldeinformationsspeicher. Benutzer authentifizieren sich direkt innerhalb der Anwendung, die auch Benutzerberechtigungen durchsetzt. Obwohl dies sicherlich funktioniert und es unzählige auf diese Weise erstellte Anwendungen gibt, hat es eine Reihe von Nachteilen. Als eigenständiges und in sich geschlossenes Identitätssystem ist es die Definition eines „Silo". Nicht nur benutzerdefinierter Code wie dieser weist oft Sicherheitslücken auf, die ausgenutzt werden könnten, es besteht auch das Risiko, dass er von Umzugs- oder Verlasser-Lebenszyklusereignissen ausgelassen wird, was zu Konten führt, die noch aktiv, aber ungenutzt („verwaist") sind. Es verwendet möglicherweise auch kein verschlüsseltes Netzwerkprotokoll und unterstützt möglicherweise kein MFA.

Die Anwendung in Szenario B ist in einigen Punkten definitiv verbessert. Da es ein externes, LDAP-basiertes Identitätssystem verwendet, vermeidet es ein Silo zu sein und wird automatisch auf die zentralisierten Identitätsverwaltungs- und Lebenszyklusprozesse der Organisation aufsetzen. Das LDAP-System kann auch MFA unterstützen, was die Authentifizierungsstärke verbessert. Wie Szenario A kann diese Anwendung jedoch ein unverschlüsseltes Netzwerkprotokoll verwenden. Und, auch wie Szenario A, ist diese Anwendung (und andere Dienste, die auf demselben Host laufen) sehr wahrscheinlich für jeden Benutzer im Netzwerk sichtbar. Als hochwertige Anwendung stellt unser Web-CMS ein attraktives Ziel für einen Gegner dar – stellen Sie sich vor, Sie könnten schädlichen Code in die offizielle Website einer Organisation injizieren!

Szenario C zeigt die Anwendung innerhalb eines Zero Trust-Sicherheitsrahmens. Während die Anwendung Benutzer immer noch gegen LDAP authentifiziert, wird der Netzwerkzugriff auf die Anwendung nun durch einen PEP geschützt. Dies stellt sicher, dass nur autorisierte Benutzer auf diesen Host im Netzwerk zugreifen können, was es für den Gegner viel schwieriger macht, anzugreifen. Darüber hinaus können nicht nur autorisierte Benutzer auf die Anwendung aus der Ferne zugreifen, der Netzwerkverkehr wird auch zwischen dem Gerät des Benutzers und dem PEP, der die Anwendung schützt, verschlüsselt. Es ist wahrscheinlich, dass das Zero Trust-System MFA nach Bedarf

durchsetzen kann, basierend auf Richtlinien und Benutzerkontext. Und, abhängig von den Fähigkeiten der Identitäts- und Zero Trust-Systeme, können Benutzer möglicherweise sogar automatisch in die Anwendung über SSO authentifiziert werden.

Verbesserung der Authentifizierung von Altsystemen

Einer der interessanten und einzigartigen Aspekte eines Zero Trust-Systems ist die Art und Weise, wie es die Reichweite und den Wert von Authentifizierungssystemen erweitern kann, die normalerweise einen begrenzten Umfang haben. Da Zero Trust-Systeme mit Identitätssystemen integriert sind und Richtlinien auf Netzwerkebene durchsetzen können, ermöglichen sie neue Wege, wie Authentifizierungssysteme angewendet werden können. Betrachten Sie zum Beispiel die „Legacy"-Anwendung, die in Abb. 5-5 dargestellt ist.

Im „vorherigen" Zustand greifen Benutzer über einen Thick Client auf diese Kerngeschäftsanwendung zu, der ein unverschlüsseltes anwendungsspezifisches Protokoll verwendet. Obwohl dieser Verkehr über ein Standard-TCP/IP-Netzwerk läuft

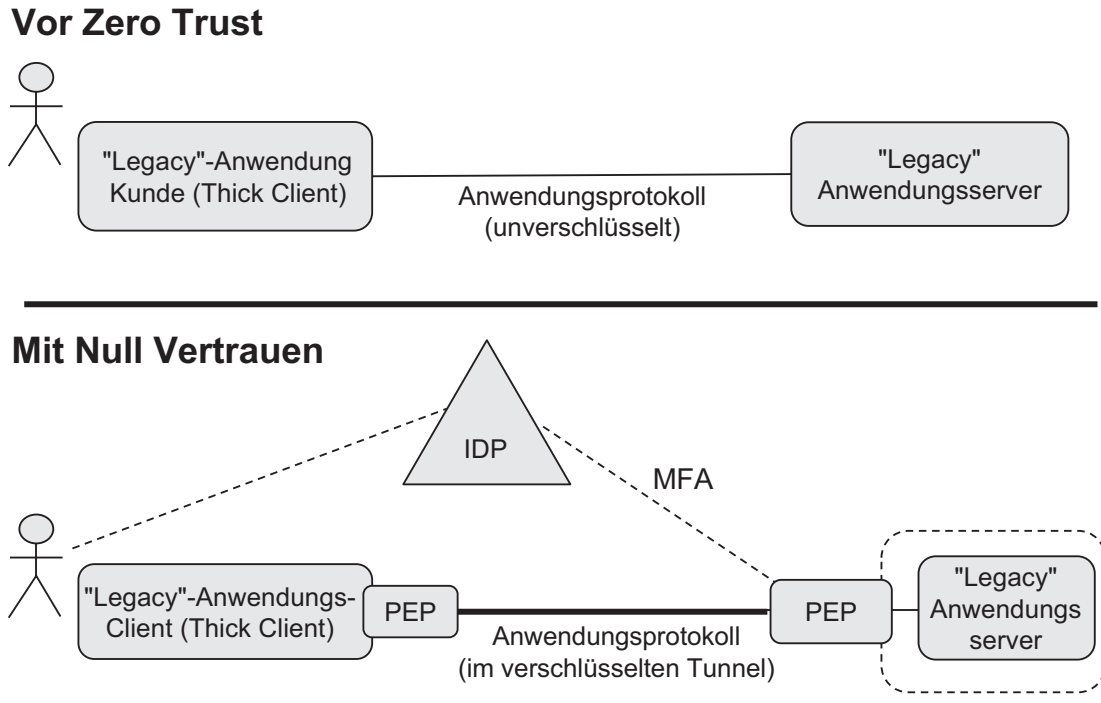

Abb. 5-5. *Vorher und Nachher – Authentifizierung von Legacy-Anwendungen*

und von einem Standard-Unternehmensgerät ausgeht, verwendet dieser Anwendungsverkehr keine modernen Anwendungsprotokolle (wie HTTPS) und ist daher für moderne Tools und Sicherheitssysteme, wie solche, die auf HTTP-Headern basieren, unzugänglich. Und doch sendet die Anwendung trotz ihrer „Verschlossenheit" gegenüber Sicherheitstools sensible Geschäftsdaten unverschlüsselt. Darüber hinaus ist diese Organisation nicht in der Lage, diese Anwendung zu modifizieren, um sie web- oder SAML-freundlich zu machen.[10] All diese Faktoren erschweren es ihnen, ihre Sicherheits- und Compliance-Anforderungen zu erfüllen, wie die Durchsetzung von MFA und die Verschlüsselung des Netzwerkverkehrs.

Im „mit Zero Trust"-Zustand hat die Organisation ein modernes Authentifizierungssystem eingerichtet. Dieses System fungiert als autoritative Identitätsquelle sowohl für die ersten Benutzeranmeldungen als auch für die Durchsetzung von MFA. Während diese Legacy-Anwendung nicht aus einer Identitäts- oder primären Authentifizierungsperspektive verbunden ist, kann das Zero Trust PEP den Zugriff des Benutzers auf die Anwendung abfangen und den IDP aufrufen, um MFA durchzusetzen, bevor der Zugriff des Benutzers fortgesetzt wird. Dieser Ansatz hat mehrere bedeutende Vorteile für die Organisationen: Erstens erfüllen sie ihre MFA- und Verschlüsselungsanforderungen. Zweitens verwenden sie den gleichen IDP konsistent im gesamten Unternehmen, wodurch sie eine einfachere Benutzererfahrung bieten und die betriebliche Komplexität reduzieren. Und die Zero Trust-Lösung ermöglicht es ihnen, all diese Ziele zu erreichen, ohne Änderungen am Anwendungsserver oder Client vornehmen zu müssen.

Das vorhergehende Beispiel, obwohl einfach, veranschaulicht eine Möglichkeit, wie die Prinzipien und Vorteile von Zero Trust erreicht werden können, auch mit vorhandenen Elementen einer IT-Infrastruktur, die nicht geändert werden können. Insbesondere als Overlay auf bestehende Netzwerke sind Zero Trust-Architekturen einzigartig positioniert, um diesen Wert zu bringen, während sie disruptive Änderungen minimieren. Während wir beim Thema Veränderung sind, diskutieren wir, wie Zero Trust-Systeme Organisationen dabei helfen können, ihre IAM-Programme voranzutreiben.

[10]Es kann eine Reihe von vernünftigen Gründen dafür geben, wie zum Beispiel, dass es sich um eine Closed-Source-Anwendung handelt, die nicht unter der Kontrolle der Organisation steht, eine intern entwickelte Anwendung, die ältere Technologien nutzt, oder eine Anwendung, für die die Organisation nicht mehr das Fachwissen zur Modifikation hat.

Zero Trust als Katalysator zur Verbesserung von IAM

Zero Trust-Projekte sind eine hervorragende Gelegenheit für Organisationen, ihre Identitätssysteme schrittweise zu verbessern oder signifikant zu transformieren. Wenn sie richtig angegangen werden, ermöglichen Zero Trust-Projekte es Organisationen, ihre vorhandenen Identitätssysteme zu vereinfachen und zu glätten, oder zu moderneren und effektiveren Systemen zu migrieren.

Zum Beispiel haben viele größere Organisationen mehrere inkompatible Verzeichnisse für Authentifizierung und Benutzerattribute im Einsatz. Diese Systeme könnten im Laufe der Zeit unabhängig voneinander gewachsen sein, vielleicht initiiert durch separate Abteilungen mit einzigartigen Anforderungen für verschiedene Projekte, oder vielleicht geerbt als Ergebnis einer Akquisition. Diese könnten sich nicht nur auf Verzeichnisse innerhalb einer einzigen Infrastruktur beschränken, sondern könnten auch Verzeichnisse in der Cloud, Kundenidentitätssysteme oder sogar Geschäftspartneridentitäten umfassen. Ein Identitätspraktiker könnte alle diese Verzeichnisse in ein „ein Verzeichnis, um sie alle zu beherrschen“ konsolidieren wollen; dies könnte ein Projekt sein, das man in Angriff nehmen sollte, sollte aber kein ausschlaggebender Faktor sein, bevor man ein Zero Trust-Projekt beginnt, aus zwei Gründen.

Erstens haben in vielen Fällen diese unterschiedlichen Identitätssysteme unterschiedliche und in einigen Fällen widersprüchliche Anforderungssätze, so dass es oft unmöglich ist, dass ein einziges Identitätssystem sie alle erfüllt. Diese Unterschiede können sich als technische Plattform- oder Integrationsanforderungen, Unterstützung für spezifische regulatorische oder Compliance-Richtlinien (wie Datenresidenz) oder sogar etwas so einfaches (aber wichtiges) wie lokale Sprachunterstützung darstellen.

Zweitens müssen Organisationen das Zero Trust-Projekt nicht nur als Katalysator für den Ersatz bestimmter veralteter Technologien betrachten (die wir in späteren Kapiteln ausführlich untersuchen werden), sondern auch als Mechanismus zur Normalisierung disparater Systeme. Wenn es richtig gemacht wird, kann Zero Trust die Sicherheit und den Betrieb vereinfachen, indem es als homogenisierende Schicht fungiert, die die zugrunde liegende Komplexität maskiert – fast wie eine Schneedecke, die eine komplexe Landschaft glättet.

Das bedeutet jedoch nicht, dass Zero Trust-Programme für Identitätssysteme, die grundlegend defekt sind, kompensieren können (oder sie magisch reparieren). Allerdings werden die meisten Identitätsteams von Organisationen von klugen und

fokussierten Menschen geleitet, die mit einer komplexen Mischung von Tools und einer großen Menge an Arbeit zu kämpfen haben. Wenn es richtig gemacht wird, kann Zero Trust dazu beitragen, die Identitätsoperationen zu vereinfachen und zu rationalisieren und die Komplexität des gesamten Identitäts-Programms zu reduzieren, ohne dass umfassende oder disruptive Änderungen erforderlich sind.

Zusammenfassung

Identitätsmanagement-Systeme haben einen breiten Anwendungsbereich, den wir in diesem Kapitel vorgestellt haben. Sie neigen dazu, komplex zu sein – von Natur aus dynamisch und oft unordentlich, sie handhaben täglich Joiner-, Mover- und Leaver-Prozesse, Ausnahmen und alles. Realistisch gesehen ist diese Komplexität unvermeidlich – Identitätssysteme dienen im Wesentlichen als Software- und Prozessmodell der Organisation, ihrer Menschen und ihrer Rollen. Aus dieser Perspektive betrachtet, sollte es nicht überraschend sein, dass Unternehmen spezialisierte Teams zur Bedienung dieser Systeme einrichten und dass es ein Anbieter- und Beratungsökosystem um sie herum gibt.

Der Identitätslebenszyklus (einschließlich der Identitätsgovernance) ist letztendlich dafür verantwortlich, zu bestimmen „wer Zugang zu was haben sollte“ (d. h., Autorisierung), ist aber in der Regel auf manuelle oder automatisierte IT-Systeme für die Bereitstellung von Konten angewiesen,[11] das ist, wie die Zugriffskontrolle auf Anwendungsebene durchgesetzt wird. Zero Trust-Systeme fügen eine Netzwerkebene zur Durchsetzung der Zugriffskontrolle hinzu, und um dies zu erreichen, muss das Zero Trust-System in der Lage sein, Identitätsattribute zur Eingabe in sein Richtlinienmodell abzurufen, zum Zeitpunkt der Identitätsauthentifizierung sowie danach periodisch.

Zero Trust-Teams müssen absichtlich – und damit meinen wir durch *organisatorisches Design* – eng mit den Identitätsmanagement-Teams abgestimmt sein. Zero Trust-Systeme setzen Zugriffsregeln durch (einige davon werden vom Identitätsteam stammen), basierend auf Daten aus den Identitätssystemen. Wie bei jeder Systemintegration wird dies auf dokumentierten und stabilen APIs,

[11] Der Automatisierungsprozess ist ein inhärent „unordentlicher“ Teil von IAM – er erfordert in der Regel Adapter oder benutzerdefinierte Datenbankarbeit, um Anwendungen mit einem Bereitstellungsmotor zu integrieren. Die Branche hat in den letzten Jahren einige Fortschritte in diesem Bereich gemacht, mit dem IETF-Standard SCIM – dem System für Cross-Domain-Identitätsmanagement. Siehe https://tools.ietf.org/wg/scim/ und http://www.simplecloud.info/.

Datenbankschemas, Versionierung und Änderungsmanagement angewiesen sein. Ja, das ist Arbeit, aber es sollte nicht als eine entmutigende Aufgabe angesehen werden. IAM-Prozesse *müssen* in Organisationen existieren – jeden Tag treten Menschen bei, bewegen sich und verlassen – und es liegt in der Verantwortung der Sicherheitsteams, diese Prozesse effizient zu unterstützen, die Benutzerproduktivität zu ermöglichen und gleichzeitig die Sicherheit zu maximieren.

Identität steht im Mittelpunkt von Zero Trust, und es gibt eine breite Palette von reifen und aufkommenden Standards, die sehr effektiv zur Integration dieser Elemente genutzt werden können. Ein Verständnis dafür, wie die IAM-Systeme Ihrer Organisation funktionieren, wird ein natürlicher Teil jeder Zero Trust-Initiative sein, da Sie sie für die Authentifizierung und Identitätsattribute verwenden werden. Überraschenderweise können Identitätsmanagementprogramme (Technologie, Menschen und Prozesse) für Ihre Zero Trust-Initiative wertvoll sein, auch wenn sie relativ unreif sind – Ihre IAM-Umgebung muss nicht perfekt sein (aber sie kann auch nicht „kaputt“ sein). Letztendlich können und sollten Organisationen Zero Trust unabhängig von ihrem Ausgangspunkt der IAM-Plattformen annehmen.

KAPITEL 6

Netzwerkinfrastruktur

Netzwerke und die Hardware- und Softwareinfrastrukturen, die sie bilden, werden eindeutig von der Umstellung einer Organisation auf Zero Trust betroffen sein. Tatsächlich macht ein großer Teil der Stärke und des Wertes, den Zero Trust bringt, seine Fähigkeit aus, Identitäts- und kontextbewusste Richtlinien auf Netzwerkebene durchzusetzen und diese normalerweise getrennten Welten zu verbinden. Infolgedessen werden die Unternehmensnetzwerkinfrastruktur, die Betriebsabläufe und möglicherweise die Netzwerk-Topologie von einer Umstellung auf Zero Trust betroffen sein. Sicherheits- und Netzwerkarchitekten müssen sich dessen bewusst sein und in der Lage sein, diese Änderungen zu planen. Nur wenige Unternehmen werden von einem völlig leeren Blatt Papier ausgehen, und Sicherheitsarchitekten, die für Zero Trust planen, müssen mit ihren IT-Kollegen zusammenarbeiten, um ihre aktuelle Umgebung zu verstehen. Bestehende Infrastrukturkomponenten müssen die Zero Trust-Architektur und -Anforderungen eines Unternehmens informieren und beeinflussen, ohne dabei zu viele Einschränkungen aufzuerlegen. Das heißt, Netzwerke und ihre Teams, Betriebsabläufe und Prozesse *werden* sich als Folge der Einführung von Zero Trust ändern müssen. Diese Änderungen müssen akzeptiert und nicht bekämpft werden. Wir wissen, das ist leichter gesagt als getan, und manchmal sind Änderungen kulturell schwieriger als technisch.

Selbst Änderungen, die recht einfach sein können und als „gleich für gleich“ eingesetzt werden können, wie zum Beispiel der Ersatz eines VPN durch eine Zero Trust-Fernzugriffslösung, können organisatorisch oder politisch herausfordernd sein. Wir werden einige der nichttechnischen Aspekte von Zero Trust-Implementierungen später in Kap. 19 untersuchen, während wir in diesem Kapitel den Einfluss von Zero Trust auf primäre Netzwerkinfrastrukturkomponenten: Firewalls, DNS und Wide Area Networks fokussieren. Wir berühren auch kurz einige sekundäre Bereiche – Web Application Firewalls, API Gateways und Load Balancer/Application Delivery Controller. Wir haben noch viel mehr zu sagen über andere Netzwerkelemente, wie NAC und VPN, und wir

J. Garbis und J. W. Chapman, *Zero Trust Sicherheit*, https://doi.org/10.1007/979-8-8688-0105-1_6

werden diese in speziellen Kapiteln behandeln. Schließlich sei darauf hingewiesen, dass wir mit Ausnahme unserer Diskussion über NAC in Kap. 7 weitgehend die Diskussion über Netzwerkhardware und Switching oder Routing weglassen.

Netzwerk-Firewalls

Netzwerk-Firewalls haben natürlich historisch die Grundlage der Netzwerksicherheitsinfrastruktur gebildet und dienten als ursprüngliche Netzwerk-„Policy Enforcement Points". Firewalls werden definitiv in einem Zero Trust-Netzwerk weiter existieren, obwohl ihre Rolle sich ändern wird. Wir glauben, dass es eine von zwei Ergebnissen geben wird, wie in Abb. 6-1 dargestellt.

Szenario A in Abb. 6-1 zeigt eine vereinfachte Ansicht einer traditionellen Firewall, die IP-zentrierte Zugriffsregeln durchsetzt. Traditionelle Firewalls haben nur ein sehr begrenztes Vokabular, um ihre Regeln auszudrücken, sie verwenden das klassische Firewall-5-Tupel: Quell-IP, Quell-Port, Ziel-IP, Ziel-Port und Protokoll. Dieses begrenzte (wir sollten sagen, *verarmte*) Vokabular erlaubt nur die Definition von Zugriffsregeln auf der Grundlage von (lokalen) IP-Adressen, nicht auf Identitäten oder Kontext, und führt typischerweise zu übermäßigen Netzwerkzugriffsrechten. Dies liegt natürlich daran, dass IP-Adressen keine Identitäten sind und nicht eindeutig sind. Es sei denn, das ursprüngliche Gerät und die Firewall befinden sich im selben Netzwerk, ist es wahrscheinlich, dass die eingehende IP-Adresse nicht eindeutig ist. Am häufigsten werden IP-Adressen über Netzwerk- oder Subnetzgrenzen hinweg übersetzt (neu zugeordnet und geteilt), was es der Firewall unmöglich macht, irgendwelche Identitäts- oder kontextbewussten Entscheidungen über Zugriffskontrollen zu treffen.

Zero Trust ist natürlich darauf ausgelegt, dieses Problem zu lösen, indem es Identitäts- und kontextbewusste Policy Enforcement Points im Netzwerk ermöglicht. Dies wird zu einem von zwei Ergebnissen führen. Der erste Fall, wie in Szenario B dargestellt, ist, dass die Regeln der Firewall viel einfacher werden, da sie effektiv alle Kontrolle an den PEP abgibt. Da der PEP in der Regel einen verschlüsselten Tunnel beendet, hat er Kenntnis von der Entität am Ursprungspunkt des Tunnels und kann identitätszentrierte Regeln durchsetzen.

Die Alternative wird in Szenario C gezeigt, wo der PEP mit der traditionellen Firewall verschmolzen ist. Dieses Szenario ist wahrscheinlich, wenn der Zero Trust-Anbieter auch Ihr (Next-Gen) Firewall-Anbieter ist. Oberflächlich gesehen werden Szenarien B

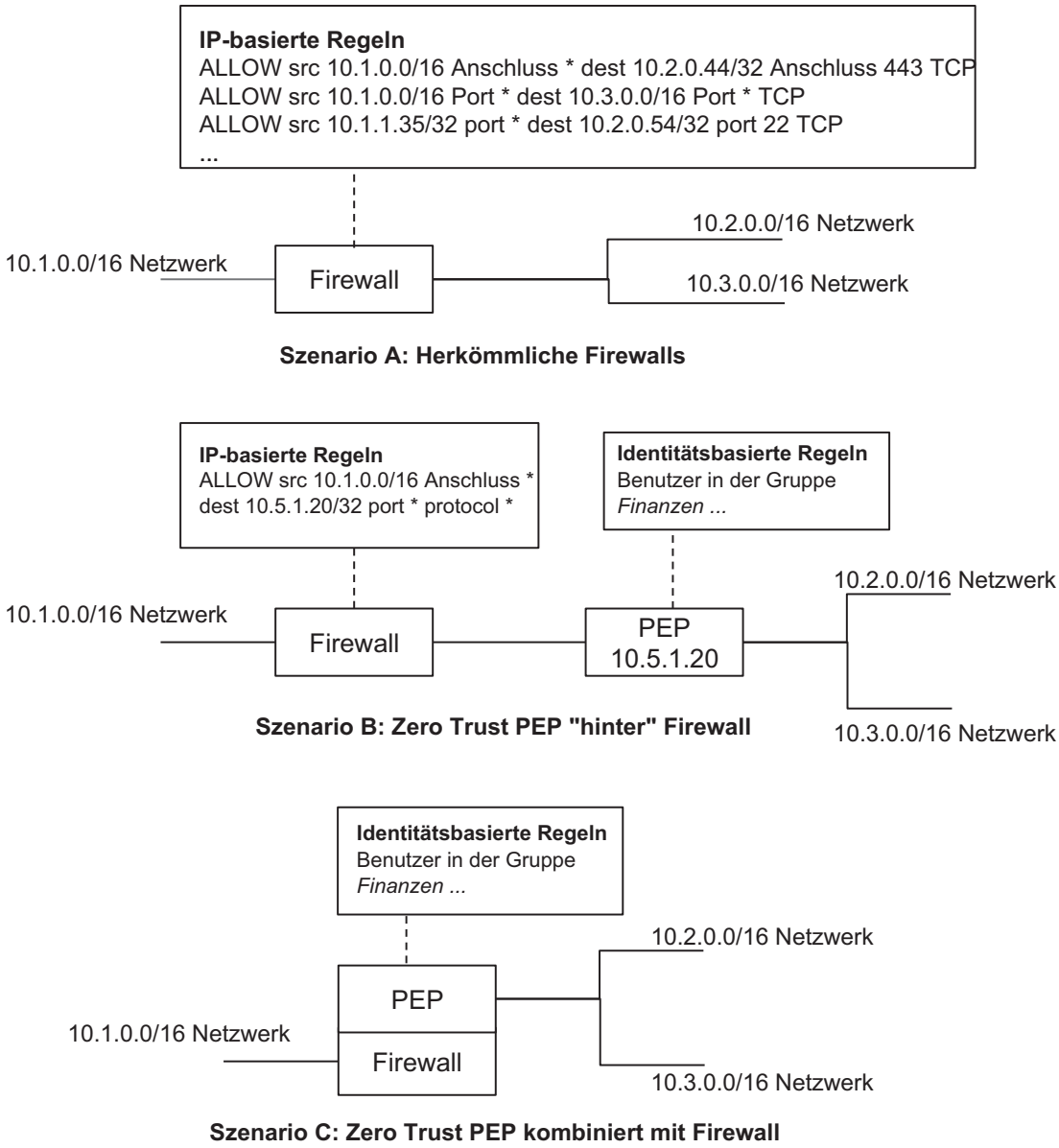

Abb. 6-1. *Firewalls und Zero Trust*

und C im Wesentlichen die gleichen funktionalen Ergebnisse liefern. Die Unterschiede werden sich ergeben, wenn Sie die Fähigkeiten spezifischer Anbieter in Bezug auf Richtlinienmodelle, Betriebsabläufe und Verwaltbarkeit bewerten. Szenario C ist oft der Ansatz, den Next-Generation Firewall (NGFW) Anbieter wählen, die in einigen Fällen

Zero Trust PEP-Fähigkeiten zu ihren Firewall-Stacks hinzugefügt haben (wir werden NGFWs in einem kommenden Kapitel behandeln).

Letztendlich müssen Zero Trust PEPs als Firewalls agieren – schließlich sind sie Netzwerk-Durchsetzungspunkte. Ein Zero Trust-System wird zu vereinfachten Firewall-Konfigurationen mit weniger Regeln und zu einer reduzierten laufenden Arbeitslast für deren Verwaltung und Wartung führen. In einigen Fällen können Organisationen die Größe, Komplexität und Kosten ihrer Firewalls reduzieren, da sie die Durchsetzungsarbeit von der Firewall auf den PEP verlagert haben. Das heißt, die Zugriffskontrollen, die Organisationen traditionell mit Firewalls zu erreichen versucht haben, können einfacher und effektiver über Zero Trust-Richtlinien erreicht werden, die in PEPs durchgesetzt werden.

Das Domain Name System

Das Domain Name System (DNS) ist ein unglaublich wichtiger Teil unserer Netzwerkinfrastruktur und gleichzeitig ein häufiges Kopfzerbrechen (und ein weit verbreitetes Meme[1]). DNS ist natürlich das System, das Domainnamen und Hostnamen in IP-Adressen übersetzt, was letztendlich die Art und Weise ist, wie Computer miteinander kommunizieren. Standard-DNS bietet keine Verschlüsselung oder Privatsphäre und hat einige interessante Komplexitäten, wenn Benutzer remote sind.

Öffentliche DNS Server

Öffentliches DNS funktioniert in einer einfachen hierarchischen Weise, wobei die Standard-Netzwerkeinstellungen der Geräte in der Regel so konfiguriert sind, dass sie einen DNS-Server in ihrem lokalen Netzwerk abfragen. Dieser fungiert in der Regel als rekursiver Server, der nicht gecachte Abfragen an einen Satz externer rekursiver, Root-, Top-Level-Domain- und autoritativer Server weiterleitet.[2] Öffentliche DNS-Server haben einige Sicherheitsprobleme, einschließlich Vertraulichkeitsproblemen (später in diesem Kapitel diskutiert), und Problemen mit der Sicherheit der DNS-Infrastruktur (nicht im

[1]Suchen Sie einfach nach „es ist immer DNS“, wenn Sie ein Schmunzeln brauchen.
[2]Für technische Einführungen siehe www.digitalocean.com/community/tutorials/an-introduction-to-dns-terminology-components-and-concepts oder https://aws.amazon.com/route53/what-is-dns/.

Rahmen unserer Diskussion, aber es gibt einige vielversprechende Standards in Arbeit bei der IETF). Schließlich ist zu beachten, dass öffentliche DNS-Einträge (per Definition) dazu bestimmt sind, öffentlich im Internet verfügbar zu sein, für jeden nicht authentifizierten Benutzer.

Private DNS Server

Private DNS hingegen ist eine ganz andere Angelegenheit und ist die Quelle vieler Frustrationen und Memes, wie bereits erwähnt. Der grundlegende Grund ist, dass diese DNS-Server und ihre Inhalte privat sein sollen – nur für ein begrenztes Publikum zugänglich. Ein Teil dieser Privatsphäre wird implizit dadurch erreicht, dass der private DNS-Server nur von einem lokalen Netzwerk aus verfügbar ist, wodurch der Zugang auf die physisch anwesenden Benutzer beschränkt wird. Ein weiterer Aspekt dieser Privatsphäre ist, dass private DNS-Abfragen in der Regel private (nicht im Internet routbare) IP-Adressen zurückgeben, die nur von diesem privaten Netzwerk aus zugänglich sind.

Lokale Geräte erhalten in der Regel einen lokalen (privaten) DNS-Server als ihren ersten Ausgangspunkt für Hostnamenauflösungsanfragen. Um öffentliche DNS-Einträge aufzulösen, gibt der Server entweder eine zwischengespeicherte Antwort zurück oder fragt rekursiv seinen konfigurierten externen öffentlichen DNS-Server ab, der die öffentlich routbare IP-Adresse zurückgibt. Um private DNS-Einträge (z. B. server1234.internal.company.com) aufzulösen, verweist er einfach auf seine lokale Datenbank und gibt die private IP-Adresse für den Server zurück.

Die meisten Organisationen haben komplexe Domänen und Netzwerke, und die DNS-Komplexität steigt schnell an. Zum Beispiel muss eine Organisation mit drei internen Domänen, die über LAN verbunden sind, sicherstellen, dass entweder die DNS-Server ihre Inhalte replizieren oder dass alle DNS-Server für Geräte erreichbar sind, um DNS-Anfragen zu stellen. Offensichtlich müssen die von den privaten DNS-Servern zurückgegebenen internen IP-Adressen auch im Netzwerk zugänglich sein.

Bis jetzt haben wir nur über lokale Benutzer gesprochen, und die Dinge werden noch komplizierter, wenn die Benutzer von den Zielservern entfernt sind. Dies ist natürlich ein häufiges Vorkommnis, mit der Kombination von IaaS-basierten privaten Ressourcen und vielen Benutzern, die von zu Hause aus arbeiten. In diesen Situationen stehen IT- und Sicherheitsteams vor der Herausforderung, dass Benutzer Zugang zu

privaten Servern benötigen, die in unterschiedlichen und isolierten Domänen liegen, wie geografisch verteilten Standorten oder über IaaS-Umgebungen verteilt sind.

Traditionelle Remote-Zugangslösungen (lesen: VPNs) haben begrenzte Fähigkeiten, oft unterstützen sie entweder das vollständige Tunneln aller DNS-Verkehrs zu einem internen Server oder das Split-Tunneln basierend auf Domain-Namen (Suchdomänen). Im ersteren Fall werden alle DNS-Abfragen an den Remote-DNS-Server gesendet; im letzteren Fall wird ein Teil des DNS-Verkehrs an den lokalen (LAN) DNS-Server gerichtet. Zero Trust-Lösungen müssen natürlich auch dieses Problem lösen, und verschiedene Plattformen gehen es auf unterschiedliche Weise an. Einige Zero Trust-Plattformen erfordern, dass interne Server Datensätze in das öffentliche DNS veröffentlichen, die externe Benutzer zu externen (oder extern zugänglichen) Proxies für die Anwendungen leiten. Dies ist oft ein Ansatz, der von Cloud-gerouteten Zero Trust Systemen gewählt wird und tendiert dazu, statischer zu sein. Andere Zero Trust-Modelle können einen ausgefeilteren Ansatz wählen und beispielsweise Client-DNS-Anfragen auf der Grundlage von Suchdomänen über einen PEP an private DNS-Server übertragen. Dies beseitigt die Notwendigkeit, öffentliche DNS-Einträge für private Server zu haben, und ermöglicht die dynamische Auflösung von Hosts, was für virtuelle oder Cloud-Umgebungen unerlässlich sein kann.

Dies ist ein sehr komplexes Thema, und es gibt keinen standardisierten Weg, wie Zero Trust-Lösungen dies angehen – es hängt stark von der Plattformarchitektur ab. Aber es ist eine wichtige Frage, die Sie Ihren potenziellen Anbietern stellen sollten, um sicherzustellen, dass sie mit Ihrer Netzwerkarchitektur übereinstimmt. Aus unserer Sicht sollten Zero Trust-Sicherheitsplattformen die Fähigkeit bieten, Dienste, die auf privaten Hosts laufen, automatisch aufzulösen (und verfügbar zu machen), basierend auf der Richtlinie. Da heutzutage so viele Umgebungen dynamisch sind, mit Diensten, die ständig erstellt, aktualisiert und zerstört werden, muss eine Zero Trust-Lösung diese agilen, DevOps-artigen Initiativen unterstützen und darf sie nicht behindern.

Überwachung von DNS für die Sicherheit

Die Überwachung des DNS-Verkehrs ist eine weit verbreitete Sicherheitsfunktion und sollte ebenso Teil Ihres Zero Trust-Systems sein. DNS-Anfragen zur Auflösung bekannter schlechter Domänen sind ein klares Zeichen für bösartige Aktivitäten und sollten schnell von einem geeigneten Durchsetzungspunkt erkannt und darauf reagiert werden – dies ist ein hochwertiger und risikoarmer Bestandteil einer Zero Trust-Plattform. Die

einfache Schlussfolgerung ist, dass Ihre Zero Trust-Architektur die DNS-Überwachung einschließen muss, ebenso die DNS-Filterung oder -Blockierung, und idealerweise in der Lage sein sollte, schnell auf bekannte schlechte DNS-Anfragen zu reagieren, indem sie den Benutzerzugriff anpasst. Wenn Ihre Zero Trust-Lösung DNS-Verkehr durch einen verschlüsselten Tunnel sendet, seien Sie sich bewusst, wie und wo Ihr Unternehmen diesen Verkehr überwacht und wie er davon betroffen sein könnte.

Bevor wir unsere Diskussion über DNS abschließen, möchten wir kurz auf die Verwendung von Verschlüsselung eingehen. Standard-DNS ist ein unverschlüsseltes Protokoll, das UDP verwendet – sowohl Anfragen als auch Antworten werden im Klartext übertragen und sind daher für Beobachter (sowohl bösartige als auch gutartige) auf lokalen oder Zwischennetzwerken sichtbar. Die Infrastruktursicherheit entwickelt sich jedoch weiter – es gibt laufende Spezifikationen (sowie einige Open-Source-Ansätze), die Verschlüsselung in DNS auf verschiedene Weisen einführen. Die IETF führt diese Bemühungen mit mehreren RFCs an, die verschiedene Aspekte der DNS-Sicherheit behandeln, einschließlich vorgeschlagener Standards, die DNS über TLS/DTLS (DoT) und DNS über HTTPS[3] (DoH) spezifizieren, die beide DNS-Verkehr verschlüsseln. Diese Ansätze variieren in der Art und Weise, wie sie funktionieren, obwohl letzterer (DNS über HTTPS) in der Branche etwas umstritten ist, und das aus gutem Grund.[4]

Was für Sicherheitsarchitekten wichtig zu verstehen ist, ist, wie ihre Sicherheitssysteme DNS-Abfrageüberwachung oder -Filterung verwenden und die Wege zu verstehen, auf denen eine Umstellung auf verschlüsseltes DNS ihre Sichtbarkeit und Kontrolle beeinflussen kann. Organisationen sollten in Erwägung ziehen, DoT zu adoptieren, da es Sicherheitsvorteile bietet und innerhalb bestehender Unternehmens-DNS-Setups störungsfrei arbeiten kann (obwohl es die DNS-Überwachung beeinflussen kann, wie gerade besprochen).

Einige Zero Trust-Systeme werden durch ihr Design die Sicherheit von DNS verbessern – zum Beispiel kann es unterstützen, DNS-Anfragen durch einen verschlüsselten Tunnel zu senden, wie zuvor besprochen, angetrieben durch eine Zero Trust-Richtlinie. Dies würde die Vorteile von verschlüsseltem DNS kombinieren mit der

[3]DNS über TLS ist in RFC 8310 und DNS über HTTPs ist in RFC 8484. Beide sind verfügbar unter www.ietf.org/.

[4]Wir empfehlen Ihnen, sich über einige der Wege zu informieren, auf denen DNS über HTTPS die Unternehmenssicherheit negativ beeinflusst und seine Ziele zur Verbesserung der Sicherheit möglicherweise nicht erreicht. Siehe Anhang A für Links zu relevanten Artikeln.

Fähigkeit, DNS-Überwachung und -Filterung durchzuführen. Basierend auf den heutigen Standards sollten Sicherheit und IT vermeiden, dass Benutzer DNS über HTTPS nutzen, da es Unternehmens-DNS-Kontrollen auf Weisen umgeht, die schädlich sein können.

Weitverkehrsnetze

Weitverkehrsnetze (WANs) sind seit den 1980er Jahren ein fester Bestandteil von Unternehmensnetzwerken und verbinden geografisch verteilte Unternehmensstandorte und -netzwerke lange bevor das Internet weit verbreitet und zuverlässig genug für den Einsatz war. Die zugrunde liegenden Technologien haben sich allmählich von leitungsvermittelten zu paketvermittelten Netzwerken verschoben. WANs konzentrieren sich hauptsächlich auf die Bereitstellung zuverlässiger und effizienter Netzwerkkonnektivität, nicht auf Sicherheit. Was das in der Praxis bedeutet, ist, dass WAN-Verkehr in der Regel privat über Carrier oder Netzwerkanbieter geroutet wird, jedoch ohne zusätzliche Verschlüsselung. Das heißt, der Verkehr ist während der Übertragung nicht öffentlich sichtbar, aber er ist für die Netzwerkdienstanbieter sowie für jeden anderen Zwischenakteur mit legalem (oder illegalem) Zugang zum Netzwerk zugänglich.[5] Die Schlussfolgerung ist, dass die Netzwerkverkehrsverschlüsselung in der Regel nicht vom WAN selbst bereitgestellt wird.

Ebenso ist die Zugriffskontrolle einfach nicht im Rahmen des WANs – sie sind darauf ausgelegt, verteilte Unternehmensnetzwerke zu verbinden, und nicht ein Modell für die Zugriffskontrolle auf der Grundlage von Firewall-Regeln oder -Richtlinien bereitzustellen. Unternehmen, die WANs nutzen, müssen natürlich Netzwerkfirewalls an den Rändern einsetzen und konfigurieren, unmittelbar hinter ihrem Service Provider WAN-Router. Sie müssen auch entscheiden, ob und wie sie den Verkehr, der das WAN durchquert, verschlüsseln, entweder über ein verschlüsseltes Anwendungsprotokoll oder auf andere Weise.

In den letzten zehn Jahren oder so sind Software-Defined Wide Area Networks (SD-WANs) aufgetaucht, basierend auf der Annahme, dass die grundlegende Internet Service Provider (ISP) Konnektivität ausreichend Bandbreite, Zuverlässigkeit und geringe Latenz hat, um als Grundlage für Unternehmens-WANs verwendet zu werden. SD-WANs

[5]Natürlich gilt dies auch für den Verkehr, der heute das Internet durchquert.

können definitiv reduzierte Kosten liefern, da traditionelle WANs ziemlich teuer sein können (sowie langsam von ISPs bereitgestellt werden). SD-WANs nutzen typischerweise einen verschlüsselten Tunnel-Overlay wie IPSec zwischen entfernten Knoten, um Datenschutz und -integrität zu gewährleisten. Sie bieten auch oft mehrere Routen (Netzwerkpfade) zwischen ihren Knoten, um die Netzwerkqualität zu gewährleisten, was einige Auswirkungen hat, wenn es mit Zero Trust kombiniert wird, was wir später diskutieren. Wie traditionelle WANs bieten SD-WANs Netzwerkkonnektivität zwischen verteilten Standorten und bieten kein eingebautes Sicherheitsmodell oder erzwingen Zugriffsrichtlinien.

Wenn Unternehmen Zero Trust-Systeme entwerfen und implementieren, werden sie sich wahrscheinlich weniger auf WANs verlassen (und mehr auf verschlüsselte Verbindungen, die von Benutzergeräten initiiert werden). Das bedeutet nicht, dass WANs verschwinden werden, es ist nur so, dass es zwei Faktoren gibt, die beide zu einer Verringerung ihrer Bedeutung beitragen. Erstens, Zero Trust-Systeme „kümmern sich nicht“ um das zugrunde liegende Netzwerk – sie gehen davon aus, dass es unsicher ist und verschlüsseln den gesamten Verkehr. Und zweitens ist in der heutigen Welt die Internetkonnektivität meist allgegenwärtig, kostengünstig und im Allgemeinen schnell und zuverlässig genug, um für geschäftskritische Unternehmenskommunikation verwendet zu werden.[6]

Obwohl die meisten Zero Trust-Implementierungen wahrscheinlich nicht sofort zu Änderungen an der WAN-Infrastruktur führen werden, wird zumindest die Möglichkeit eröffnet, sie zu reduzieren oder zu ersetzen, was ein Gespräch ist, das die Netzwerk-, IT- und Sicherheitsteams definitiv führen sollten. Natürlich bringt Veränderung oft Komplexität mit sich, und Zero Trust ist keine Ausnahme. Insbesondere erinnern Sie sich daran, dass Zero Trust-Systeme typischerweise einen verschlüsselten Overlay-Tunnel über Zwischennetzwerke einrichten, meistens zwischen dem Benutzeragenten PEP und dem PEP vor den geschützten Ressourcen. Dieser Tunnel ist, nach Design, undurchsichtig für Netzwerkzwischenstellen. Während dies die Vorteile von Datenschutz und -integrität mit sich bringt, kann es auch die Fähigkeit legitimer Netzwerkzwischenstellen, ihre Aufgaben zu erfüllen, negativ beeinflussen (dies wird ein häufiges Thema in diesem Buch sein). SD-WANs verlassen sich oft auf Netzwerkverkehrsmetadaten wie Port und Protokoll, um Netzwerkrouting- und

[6]Die wachsende Bereitstellung und Nutzung von drahtlosen Mobilfunkkommunikationen, einschließlich 5G, wird diesen Trend nur beschleunigen.

Priorisierungsentscheidungen (Traffic Shaping) zu treffen, um Qualitätsziele zu erreichen. Dies kann normalerweise teilweise kompensiert werden, erfordert aber eine Koordination zwischen den Zero Trust- und Netzwerkteams.

Zusammenfassend wird die Einführung von Zero Trust sehr wahrscheinlich die Nutzung von WANs durch Unternehmen beeinflussen, oft vorteilhaft durch Reduzierung der Kosten oder Bandbreitennutzung, und in einigen Fällen können sie sogar eliminiert werden. Da der Zero Trust-Netzwerkverkehr jedoch typischerweise auf bestehenden WANs überlagert wird, müssen Sie darauf achten, wie Ihr WAN möglicherweise Netzwerkverkehrsmetadaten verwendet und wie dies beeinträchtigt werden könnte.

Lastverteiler, Application Delivery Controller und API-Gateways

Lastverteiler, Application Delivery Controller (ADCs) und API-Gateways sind weit verbreitete Komponenten der Netzwerk- und IT-Infrastruktur. Gemeinsam werden sie verwendet, um eine bessere Leistung und höhere Skalierbarkeit und Resilienz für Anwendungen zu bieten und gleichzeitig eine Abstraktionsschicht zwischen Anbietern eines Dienstes und dessen Nutzern zu ermöglichen. Sie können komplex sein und ihre Ziele oft durch verschiedene technische Ansätze erreichen. Zum Beispiel können selbst einfache Lastverteiler eine oder mehrere Techniken (wie Round-Robin, Zufall oder lastbasiert) verwenden, um Arbeitslasten auf Server zu verteilen. ADCs und API-Gateways reduzieren die Serverlast, indem sie bestimmte Netzwerk-, Inhaltsoptimierungs- und API-Konsolidierungsfunktionen vor ihren Back-End-Servern ausführen. Dies kann Funktionen wie SSL-Terminierung, Inhalts-Caching, Verbindungsmultiplexing, Traffic-Shaping und Mikroservice-Abstraktion oder -Konsolidierung umfassen. Im Allgemeinen ist zu beachten, dass diese Systeme Netzwerk- und Anwendungsfunktionen bereitstellen und, abgesehen von der Unterstützung der *Verfügbarkeit,* normalerweise nicht als Sicherheitsgeräte betrachtet werden.

Die von diesen Systemen bereitgestellten Funktionen sind wertvoll und werden in Zero Trust-Systemen weitgehend unverändert bestehen bleiben. Ein Punkt, auf den man jedoch achten sollte (wie bereits bei SD-WANs diskutiert), ist die mögliche Auswirkung von Änderungen der Netzwerk-Topologie und der neuen Verwendung von getunneltem verschlüsseltem Verkehr innerhalb des Zero Trust-Systems. Dieser Verkehr wird

wahrscheinlich für Zwischenkomponenten wie diese undurchsichtig werden – es hängt alles davon ab, wo die PEPs sind und wie die PEPs Richtlinien durchsetzen. Im Allgemeinen sollten Lastverteiler, ADCs oder API-Gateways gut mit den auf Enklaven basierenden und Cloud-gerouteten Bereitstellungsmodellen funktionieren, wenn sie hinter einem PEP liegen. Ressourcenbasierte und Mikrosegmentierungsmodelle könnten möglicherweise mit diesen Komponenten interferieren, da sie mit der Notwendigkeit eines aktiven Netzwerkvermittlers in Konflikt geraten könnten.

Der Schlüssel hier ist, sich bewusst zu sein, wie Ihre Organisation diese Systeme nutzt, und sich mit Ihren Kollegen aus den Bereichen Netzwerk, Anwendung, IT und Sicherheit auszutauschen. Bedenken Sie, dass nicht alle Anwendungen und Dienste unbedingt in ein Zero Trust-System aufgenommen werden müssen. Es kann durchaus sein, dass ein Webanwendungsserver (einschließlich Last Verteiler und ADC) vorhanden ist, um eine öffentlich verfügbare Anwendung bereitzustellen, die per Design für nicht authentifizierte und anonyme Benutzer sichtbar und zugänglich sein soll. Beispielsweise könnten die Website eines Unternehmens oder eine SaaS-Anwendung in diese Kategorie fallen. Im Gegensatz dazu könnte ein API-Dienst möglicherweise von überall im Internet zugänglich sein, könnte jedoch von einem durch Zero Trust geschützten PEP profitieren. Es hängt vom Zugriffsmodell und der Art der Client-Systeme ab, die zur Nutzung der API berechtigt sind.

Abschließend möchten wir noch einen weiteren wichtigen Punkt hervorheben. Obwohl es durchaus Dienste geben kann, die für die Nutzung durch öffentliche und nicht authentifizierte Benutzer bestimmt sind (wie das Beispiel der Website), wird es wahrscheinlich *andere Dienste auf demselben Host geben,* die eine Authentifizierung und Autorisierung erfordern und in Ihren Zero Trust-Bereich aufgenommen werden sollten. Beispielsweise wird ein öffentlich zugänglicher Webserver (oder Last Verteiler-Hardware) eine Verwaltungsschnittstelle haben, wie SSH. Der Zugriff auf diese Schnittstelle *muss* auf autorisierte Benutzer beschränkt und vor nicht autorisierten Benutzern verborgen werden – ein Problem, für das Zero Trust eine perfekte Lösung ist.

Webanwendungs-Firewalls

Webanwendungs-Firewalls (WAFs) sind Sicherheitskomponenten, die vor Webservern sitzen und sie schützen, indem sie HTTP-Verkehr parsen, überwachen und sichern. Der Begriff WAF ist vielleicht etwas irreführend, da sie weniger eine *Netzwerk-Firewall* und

mehr ein *Sicherheits-Proxy* sind. Tatsächlich handelt es sich bei diesen Systemen technisch gesehen um Reverse Proxies, die eingehenden HTTP-Verkehr untersuchen, um Angriffe wie SQL-Injection und Cross-Site-Scripting zu erkennen und zu verhindern.

WAFs werden häufig eingesetzt, um öffentlich zugängliche Webserver zu schützen, die natürlich fast sicher regelmäßig abgetastet, gescannt und angegriffen werden. Offensichtlich rechtfertigen solche Ressourcen Investitionen in Sicherheitslösungen wie WAFs. Interessanterweise werden WAFs jedoch auch eingesetzt, um *interne* Anwendungen zu schützen, die nur für interne Benutzer zugänglich sind. In diesem Fall schützen sie vor böswilligen Insidern und kompromittierten Geräten im internen Netzwerk. Aus einer Zero Trust-Perspektive begrüßen wir die zusätzliche Sicherheit auch für interne Anwendungen und die Annahme eines Kompromisses, die sie wahrscheinlich motiviert hat.

Zero Trust-Systeme können Angriffe natürlich nicht verhindern, aber sie können die Angriffsfläche, die eine kompromittierte Maschine angreifen kann, reduzieren. So wird ein richtiges Zero Trust-System für eine hypothetische interne Webanwendung den Zugriff nur auf die Benutzer beschränken, die legitime geschäftliche Bedürfnisse haben und ein Konto in der Webanwendung haben. Wenn 10 % der Benutzerpopulation diese Anwendung nutzt, wird das Zero Trust-System die Fähigkeit der verbleibenden 90 % der Geräte, überhaupt einen Angriff zu versuchen, eliminieren. In Bezug auf WAFs gibt es definitiv noch einen Platz für sie intern mit Zero Trust, da die 10 % der Benutzer durchaus bösartige Software hosten können, die versuchen kann, die Anwendung anzugreifen.

Zusammenfassung

Es sollte klar sein, dass einige Elemente Ihrer Netzwerkinfrastruktur sicherlich von der Einführung von Zero Trust betroffen sein werden. Auch wenn Ihre Reise nicht alles im Netzwerk beeinflussen wird, werden zumindest alle Netzwerkelemente eine sorgfältige Analyse und Diskussion erfordern. Das heißt, als Zero Trust-Architekt und -Leiter müssen Sie proaktiv ein Verständnis für Ihr Unternehmensnetzwerk erlangen und verstehen, wie verschiedene Sicherheits-, Konnektivitäts-, Verfügbarkeits- und Zuverlässigkeitskomponenten eingesetzt werden.

Zero Trust-Systeme, da sie als verschlüsseltes Overlay auf den zugrunde liegenden Netzwerken agieren, werden diese Art von Koordination, Zusammenarbeit und

Verständnis erfordern. Das bedeutet nicht, dass Zero Trust-Projekte zwangsläufig störend sein werden, und wir möchten Sie nicht davon abhalten, diese Reise zu beginnen. Tatsächlich gibt es definitiv Anwendungsfälle und Szenarien, in denen Zero Trust schrittweise und einfach eingesetzt werden kann. Aber eine unternehmensweite Zero Trust-Architektur wird einen Großteil des Netzwerks und der vernetzten Anwendungen beeinflussen und eine breite Analyse der Infrastrukturelemente erfordern. Dieses Kapitel und die folgenden in Teil II werden Ihnen den Kontext und das Verständnis liefern, um dies erfolgreich zu tun.

KAPITEL 7

Netzwerkzugriffskontrolle

Wir behandeln Network Access Control (NAC) Lösungen getrennt von den Firewall-, DNS- und Load Balancer-Lösungen, die wir in Kap. 6 aus zwei Gründen abgedeckt haben: Erstens, um den Anbietern Anerkennung zu zollen – NAC-Lösungen stellen frühe (und andauernde) Versuche dar, einige der Prinzipien von Zero Trust zu erreichen – insbesondere die Fähigkeit, identitätszentrierte Zugriffsrichtlinien auf Netzwerkebene durchzusetzen. Zweitens, NAC-Implementierungen werden generell beeinflusst werden, wenn Organisationen eine moderne Zero Trust-Architektur einsetzen – der Wert und die Bedeutung von NAC (als etablierte Kategorie) werden abnehmen, ersetzt durch die effektivere Fähigkeit von Zero Trust, als eine umfassendere und leistungsfähigere Netzwerkzugriffskontrolllösung zu dienen.

Einführung in die Netzwerkzugriffskontrolle

Was die Branche heute als NAC bezeichnet, ist eine Kategorie, die aus mehreren Funktionen und Netzwerkprotokollen besteht, die sich auf die Identifizierung und Validierung von Benutzergeräten, die Authentifizierung von Benutzern und die Durchsetzung von Richtlinien beziehen, die festlegen, auf welche Netzwerkressourcen Benutzer zugreifen dürfen. Kommerzielle NAC-Lösungen führen oft eine Geräteerkennung durch und können Geräteposture-Checks wie Antivirenschutzstufe, System-Patch-Level und Gerätekonfiguration validieren. Dies ermöglicht es diesen Systemen, Richtlinien wie das Quarantänisieren von fehlgeschlagenen Geräten in nur zur Behebung bestimmte Netzwerksegmente durchzusetzen. Sobald die Richtlinie erfüllt ist, kann der Computer auf Netzwerkressourcen und das Internet zugreifen, innerhalb der vom NAC-System definierten Richtlinien.

Die Ziele von NAC sind lobenswert und die beschriebenen Funktionen stellen tatsächlich einen Teil unserer Zero Trust-Prinzipien dar. Warum sind wir also kritisch gegenüber NAC und glauben, dass seine Zukunft begrenzt ist? Das Problem mit NAC

J. Garbis und J. W. Chapman, *Zero Trust Sicherheit*, https://doi.org/10.1007/979-8-8688-0105-1_7

sind nicht seine Ziele, sondern die Art und Weise, wie NAC-Systeme konzipiert sind. Insbesondere erfordert ihr Ansatz (und das Netzwerkprotokoll, das sie verwenden, 802.1x) in der Regel, dass eine einzige Organisation die Netzwerkhardwareinfrastruktur besitzt und betreibt, die für alle Benutzer und alle Server vorhanden ist. Daher sind NAC-Lösungen für Remote-Benutzer, deren Geräte mit einem persönlichen oder Drittanbieter-Netzwerk verbunden sind oder die auf Ressourcen in der Cloud zugreifen, nutzlos. Da NAC-Systeme auf Netzwerkebene 2 arbeiten, sind sie hardwarebasiert und funktionieren einfach nicht in Cloud-Umgebungen oder für Remote-Benutzer.

Wenn sie für geeignete Szenarien verwendet werden – Benutzer vor Ort greifen auf Ressourcen vor Ort zu – kann NAC nützlich sein, obwohl sie in der Praxis dazu neigen, Benutzern nur grobkörnige Zuweisungen zu virtuellen LANs (VLANs) zu bieten, die in der Regel viele Dutzend (wenn nicht Hunderte) von verfügbaren Diensten haben. Dies ist nicht gut mit den Zielen von Zero Trust abgestimmt. Und es ist wichtig zu beachten – NAC-Lösungen bieten keine Netzwerkverkehrsverschlüsselung oder Remote-Zugriff.[1] Es gibt einen weiteren Aspekt, der für NAC-Lösungen typisch ist und eine eigene Diskussion verdient – den Zugang zum Gastnetzwerk. Wir werden das später in diesem Kapitel besprechen, aber zuerst wollen wir uns 802.1x (mündlich als “acht-null-zwei-eins-ex” bezeichnet), das Protokoll, das alle traditionellen NAC Lösungen verwenden, genauer ansehen.

802.1x, ein offenes Protokoll, das durch eine Kombination von IEEE- und IETF-Papieren definiert ist, legt einen Netzwerkauthentifizierungsmechanismus für die Authentifizierung und Autorisierung von Geräten für die Verbindung zu einem LAN fest. Kurz gesagt, ein NAC-System ist dafür verantwortlich, den Zugriff eines Geräts auf ein Netzwerk zu autorisieren und ihm zu erlauben (oder zu verhindern), dass es eine IP-Adresse in diesem LAN erhält. Dies funktioniert in Verbindung mit Netzwerkhardware (Switches), wie in Abb. 7-1 gezeigt.

Wie das Diagramm zeigt, verwendet das Gerät des Benutzers (der *Supplicant*) das Extensible Authentication Protocol (EAP) on LAN (EAPOL) um Anmeldeinformationen oder Zertifikatsinformationen an den Authenticator zu übermitteln. Wenn der Supplicant zum ersten Mal mit dem Netzwerk-Switch verbunden wird, wird er als “nicht autorisiert” eingestuft und lässt nur EAP-Verkehr zu – UDP, TCP und ICMP sind nicht

[1]Um fair zu sein, viele NAC-Anbieter haben auch Produkte mit diesen Fähigkeiten in ihrem Portfolio, mit unterschiedlichen Integrationsgraden.

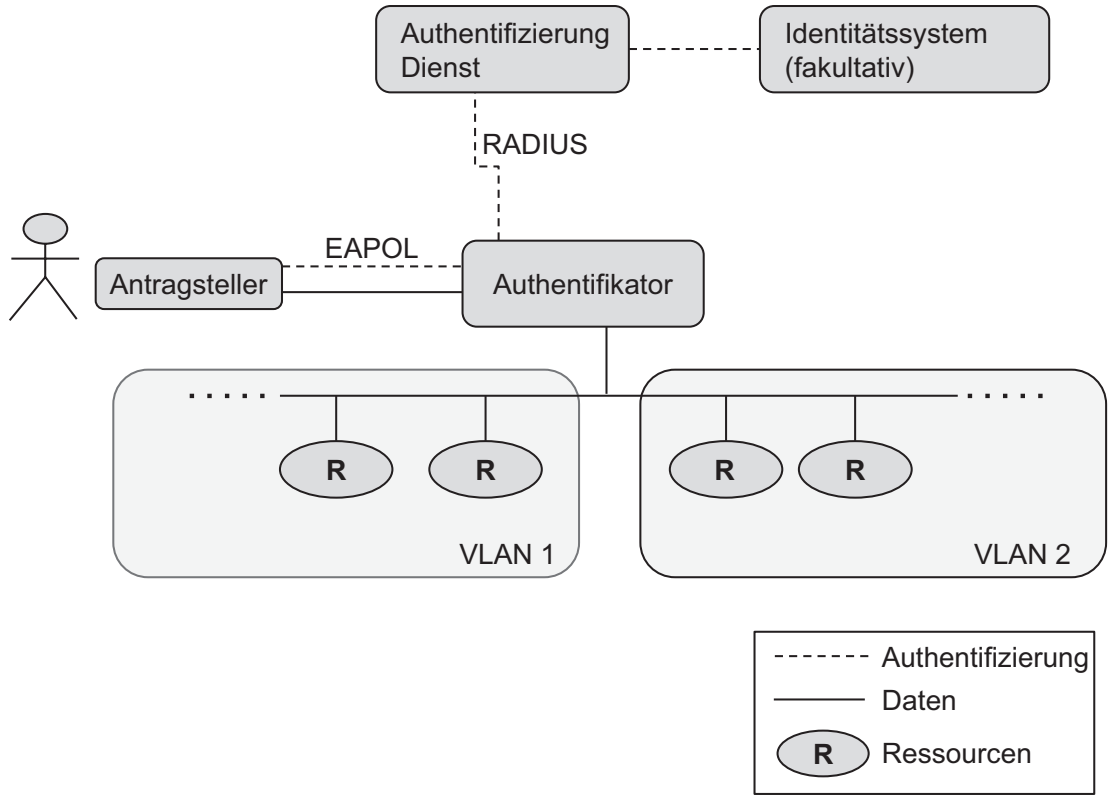

Abb. 7-1. *802.1x Authentifizierung*

erlaubt.[2] EAP ist, nach Design,[3] ein sehr einfaches Protokoll, das auf Schicht 2, nach der IP-Schicht, arbeitet. Als solches ist es buchstäblich ein *lokales Netzwerk*-Protokoll, das nur im lokalen Subnetz (Broadcast-Domain) zugänglich ist und nicht geroutet werden kann.[4] Der Authenticator validiert die Anmeldeinformationen des Benutzers mit dem Authentication Service, in der Regel unter Verwendung des RADIUS-Protokolls. Produkte, die auf 802.1x basieren, können entweder Benutzeranmeldeinformationen unterstützen, die gegen ein Identitätssystem validiert werden, oder eine zertifikatbasierte Authentifizierung.

[2]Tatsächlich hat der Supplicant zu diesem Zeitpunkt in der Autorisierungssequenz, wenn DHCP verwendet wird, noch keine IP-Adresse zugewiesen.

[3]Siehe https://tools.ietf.org/html/rfc3748, Abschnitt 1.3, Anwendbarkeit.

[4]Einige NAC-as-a-Service-Anbieter leiten diesen Verkehr effektiv um, indem sie ihn über einen lokalen Agenten erfassen, der wiederum mit einem cloudbasierten Authenticator kommuniziert.

Wenn die Anmeldeinformationen des Benutzers gültig sind, setzt der Authenticator den Netzwerk-Switch des Supplicants auf den „autorisierten“ Zustand, und das Gerät kann eine IP-Adresse erhalten und UDP-, ICMP- und TCP-Verkehr senden. Am wichtigsten ist, dass der Authenticator das Gerät einem Netzwerksegment (einem virtuellen LAN oder VLAN) zuweist, indem er eine Konfigurationseinstellung am Netzwerk-Switch vornimmt.

Die Implikation dieses Protokolls ist, dass der Supplicant und der Authenticator sich im selben Netzwerk-Broadcast-Domain befinden müssen – das heißt, beide verwenden das gleiche physische Netzwerkmedium (Ethernet oder Wi-Fi). Darüber hinaus müssen sie Netzwerkhardware verwenden, die vom Unternehmen besessen und betrieben wird, und diese Hardware muss ubiquitär über die Infrastruktur verteilt sein. Das Ergebnis ist, dass NAC für Remote-Benutzer einfach nicht nützlich ist, oder für Benutzer, die auf Cloud-Ressourcen zugreifen. In beiden Szenarien läuft entweder der Benutzer oder der Dienst, auf den sie zugreifen (oder beide), auf einer Netzwerkinfrastruktur, die von jemand anderem als dem Unternehmen betrieben wird. Diese Situationen, die zunehmend häufig sind, stellen daher eine erhebliche Einschränkung der Wirksamkeit von NAC dar.

Sobald das Gerät eines Benutzers einem VLAN zugewiesen ist, haben viele NAC-Lösungen keine weitere Beteiligung in Bezug auf Zugriffskontrolle (außer einer periodischen erneuten Authentifizierung). Die Kontrolle des Benutzer- oder Gerätezugriffs innerhalb des VLAN liegt dann in der Verantwortung der Firewalls des Unternehmens (oder Next-Gen-Firewalls), die natürlich ihr eigenes Zugriffsrichtlinienmodell haben. Beachten Sie, dass einige fortschrittliche NAC-Anbieter zusätzliche Fähigkeiten haben (außerhalb des Geltungsbereichs von 802.1x) und die Integration mit anderen Sicherheitskomponenten unterstützen.

Schließlich unterstützt 802.1x nur die grobkörnige Zuweisung von Benutzern zu virtuellen LAN-Segmenten (VLANs), üblicherweise mit Dutzenden, wenn nicht Hunderten oder mehr Diensten oder Peer-Geräten, die im Netzwerk sichtbar sind. Und weil jedes Gerät zu einem bestimmten Zeitpunkt nur einem einzigen VLAN zugewiesen werden kann, perpetuieren NACs die Probleme des übermäßig breiten Netzwerkzugriffs. Während es wahr ist, dass NACs durch die Verwendung von Firewall-ACLs ergänzt werden können, sind diese in der Regel statisch und IP-zentriert und daher schlecht auf unsere Zero Trust-Ziele abgestimmt.

Zero Trust und Netzwerkzugriffskontrolle

Die grobe Zuweisung von Geräten zu Netzwerken, die in der Praxis Benutzern einen umfassenden Netzwerkzugriff auf alle Ports und Protokolle über ein gesamtes VLAN gewährt, ist einfach nicht kompatibel mit dem Prinzip der minimalsten Berechtigung von Zero Trust. Das bedeutet nicht, dass eine NAC-Lösung nicht *Teil* eines Zero Trust-Unternehmens sein kann – tatsächlich werden wir später einige solche Szenarien untersuchen und wir haben zuvor die Rolle von NAC in der BeyondCorp-Infrastruktur erklärt. Wir möchten Sie jedoch darauf hinweisen, dass Sie die Lösungen von NAC-Anbietern und deren Übereinstimmung mit Ihren Zero Trust-Anforderungen sorgfältig prüfen, bevor Sie entscheiden, wie Sie sie in Ihre Zero Trust-Architektur einbeziehen. NAC-Anbieter sind sich sicherlich der Einschränkungen von 802.1x bewusst, und einige NAC-Anbieter haben über das 802.1x-Protokoll hinausgehende Fähigkeiten zu ihren Produktportfolios hinzugefügt, um diese Grenzen zu überwinden. Zum Beispiel haben einige NAC-Anbieter auch Endpunktinspektionsfähigkeiten und Remote-Zugriffsfunktionen oder liefern NAC sogar als cloudbasierten Service.

Beachten Sie auch, dass Unternehmensnetzwerke in der Regel einen nicht unerheblichen Prozentsatz an Geräten haben, die 802.1x nicht unterstützen, wie zum Beispiel Drucker, VOIP-Telefone oder IoT-Geräte. NAC-Lösungen bieten in der Regel eine VLAN-Zuweisung für diese, typischerweise basierend auf MAC-Adressen, aber diese Ansätze sind auf lokale Netzwerkzugriffskontrollen beschränkt und oft schwierig zu verwalten. Wir werden später diskutieren, wie diese Geräte in Zero Trust-Umgebungen angegangen werden, in Kap. 16.

In jedem Fall gibt es NAC-Fähigkeiten, die auch in einer Zero Trust-Architektur sinnvoll sein können, insbesondere wenn sie bereits vorhanden sind – insbesondere der Zugang zum Gastnetzwerk und die Geräteerkennung. Lassen Sie uns diese genauer betrachten.

Unverwalteter Gastnetzwerkzugang

Gastnetzwerkzugang ist ein Bereich, der in gewisser Weise in einem Zero Trust-Netzwerk weniger problematisch werden kann. Lassen Sie uns dies zunächst definieren, damit wir ein gemeinsames Verständnis für unsere Analyse haben:

Gastnetzwerkbetrieb ist der Prozess und die Kontrolle der Bereitstellung von Internetzugang für Nicht-Mitarbeiter mit unverwalteten Geräten.

Das Gastnetzwerk bietet Internetzugang und kann einige zusätzliche Geräte umfassen, die Gästen zugänglich sind, wie drahtlose Konferenzraum-A/V-Systeme oder einen Gastdrucker, aber diese Benutzer und Geräte müssen vom Netzwerk der Mitarbeiter des Unternehmens isoliert sein.

Beachten Sie, dass Gastnetzwerke heutzutage fast ausschließlich auf drahtloser (Wi-Fi) Basis statt auf verkabelter Basis betrieben werden – und unsere Diskussion richtet sich daher nur an diese Art von Netzwerken. Viele (vielleicht sogar die meisten) Gastnetzwerke sind durch ein statisches Wi-Fi-Passwort geschützt und bestehen typischerweise aus einem einzigen flachen Netzwerksegment, so dass alle Geräte im Netzwerk Peer-Zugriff auf alle anderen Geräte haben. In einigen Umgebungen ist dies ausreichende Sicherheit – es ist ein vernünftiger Ansatz, wenn zum Beispiel der Wireless Access Point (WAP) des Gastnetzwerks vom Unternehmensnetzwerk isoliert ist und es keine große Sorge um den Zugang zu sensiblen Assets oder bösartiges Verhalten von Gästen gibt.

Unternehmen können sich dafür entscheiden, dieses Gastnetzwerk mit wenig oder keiner Überwachung oder Verwaltung zu betreiben, oder können sich dafür entscheiden, in diese Fähigkeiten zu investieren. Der entscheidende Punkt hier ist, dass es bei diesem Ansatz per Definition keine Benutzer- oder Geräteauthentifizierung gibt – alle Benutzer werden gleich behandelt und es wird kein Versuch unternommen, zwischen Benutzern oder Gerätetypen zu unterscheiden. Wir untersuchen die Auswirkungen dieses Ansatzes später, im Abschnitt „Verwaltete vs. unverwaltete Gastnetzwerke: Eine Debatte“. Schließlich ist zu beachten, dass der zuvor beschriebene unverwaltete Gastnetzwerkzugang früher, eine gängige Funktion von WAP-Hardware, das 802.1x Protokoll nicht verwendet.

Verwalteter Gastnetzwerkzugang

Verwalteter Gastnetzwerkzugang ist eine Fähigkeit, die vielen kommerziellen NAC-Lösungen gemeinsam ist und besteht in der Regel aus den folgenden Arten von Funktionen:

- Zugangsregistrierungsportal, typischerweise mit E-Mail- oder SMS-Verifizierung

- Grundlegender Workflow der Mitarbeiteranforderung (Sponsor) für Gastzugang, mit vorübergehender Netzwerkzugangsprovisionierung

Der Hauptunterschied zwischen unverwaltetem und verwaltetem Gastnetzwerkzugang besteht darin, dass der letztere Ansatz eine Benutzerselbstidentifikation mit Authentifizierung erfordert und in der Regel nur für eine begrenzte Zeit Zugang gewährt. In der Regel erfordern diese Systeme eine Registrierung – entweder durch Selbstbedienung des Gastes oder durch einen Sponsor-Mitarbeiter – über ein einfaches Portal und gewähren nur für eine begrenzte Zeit Zugang (typischerweise 24 Stunden oder weniger). Zeitlich begrenzter Zugang bietet eine zusätzliche Sicherheitsebene, über die inhärent auf kurze Reichweiten basierende Natur von Wi-Fi hinaus. Dieses verwaltete Gastnetzwerkportal und Workflow ist eine gängige Funktion von kommerziellen NAC Lösungen.

Verwaltete vs. Unverwaltete Gastnetzwerke: Eine Debatte

Obwohl nicht ganz im Bereich der Lincoln-Douglas-Debatten, gibt es unterschiedliche Perspektiven und Ansätze zur Sicherheit für Gastnetzwerke, ohne klare richtige oder falsche Antwort – Organisationen müssen ihre eigenen Entscheidungen treffen, basierend auf dem, was für ihre Umgebung und ihr Risikoprofil richtig ist. Es gibt mehrere Fähigkeiten, die mit einem Netzwerk verbunden sein können, die Organisationen berücksichtigen müssen, die grob auf einem Spektrum von weniger sicher bis sicherer eingestuft werden können, wie in Tab. 7-1 gezeigt. Dies sind interessante Kompromisse und bleiben auch bei Zero Trust-Netzwerken relevant. Beachten Sie, dass unter allen Umständen ein Gastnetzwerk vom Mitarbeiter- oder Unternehmens-LAN getrennt sein muss.

Jede Organisation und jedes Sicherheitsteam muss seine eigenen Entscheidungen darüber treffen, aber aus unserer Sicht ist ein passwortgeschütztes WLAN-Gastnetzwerk wahrscheinlich ausreichend für die meisten Unternehmensumgebungen, solange es vom Unternehmensnetzwerk getrennt ist. WPA3 wird WPA2 vorgezogen, wenn verfügbar, und Geräteisolierung ist ein netter Vorteil, kann aber als optional betrachtet werden.

Unternehmen mit Zero Trust-Netzwerken sollten natürlich weiterhin Gast-WLAN anbieten, mit der Kombination von Netzwerksicherheitsattributen, die für ihre

Tab. 7-1. *Netzwerksicherheitsattribute*

Netzwerksicherheit	Attribute
Offenes WLAN: Kein Passwort	Keine Netzwerkverkehrsverschlüsselung Keine Benutzerauthentifizierung oder -identifikation
Passwortgeschütztes WLAN	Netzwerkverkehrsverschlüsselung[5] Keine Benutzerauthentifizierung oder -identifikation Captive Portal zur Annahme der Nutzungsbedingungen (optional)
Benutzerregistrierung	Zeitlich begrenzter Netzwerkzugang. Benutzerselbstidentifikation und -authentifizierung (typischerweise auf E-Mail-Basis, nicht gegen ein Verzeichnis validiert) Formular zur Annahme der Nutzungsbedingungen
Mitarbeiter-Sponsoring	Zeitlich begrenzter Netzwerkzugang Validierter Mitarbeiter-Workflow erforderlich, um Zugang zu ermöglichen Benutzeridentifikation und -authentifizierung Formular zur Annahme der Nutzungsbedingungen
Geräteisolierung	Einige WLAN-Netzwerke unterstützen die Möglichkeit, Geräte über Router-Firewall-Regeln voneinander zu isolieren, obwohl diese Geräte mit demselben Wireless Access Point verbunden sind. Dies ist eine gute Praxis, um neugierige Benutzer (oder Malware) daran zu hindern, Netzwerk- und Port-Scans im lokalen Netzwerk durchzuführen[6]
Netzwerk Überwachung	Dazu können Dienste gehören, die häufig in Unternehmensnetzwerken verwendet werden, einschließlich DNS-Filterung oder IDS/IPS

[5]Beachten Sie, dass die typischen WLAN-Standards, die in Gebrauch sind - WPA und WPA2 mit vorgeschalteten Schlüsseln - den Verkehr so verschlüsseln, dass Benutzer ohne das Passwort ihn nicht einsehen können, die Verschlüsselung bietet jedoch **keinen** Schutz vor anderen autorisierten Benutzern im Netzwerk. Dies wurde in WPA3 behoben, aber - wie immer - erfordert Zero Trust die Verwendung von verschlüsselten Anwendungsprotokollen zusätzlich zu jeder L1- oder L2-Netzwerkverschlüsselung.

[6]Gelegentlich kann diese Neugierde zu verbesserter Sicherheit führen, wie Jason bemerkt: Einmal, während ich beim Zahnarzt auf meine Tochter wartete, verband ich mich mit ihrem Gast-WLAN und führte einen Netzwerkscan durch. Leider entdeckte ich, dass alle ihre Bürocomputer und Drucker im Netzwerk sichtbar waren, mit offenen Ports. Glücklicherweise war die Zahnärztin eine Nachbarin von uns, also kontaktierte ich sie und drängte sie nachdrücklich, ihren IT-Service dazu zu bringen, dies zu beheben. Bei meinem nächsten Besuch, etwa sechs Monate später, waren die Bürogeräte ordnungsgemäß unzugänglich. White-Hat-Erfolg freigeschaltet!

Umgebung geeignet sind. Ein Zero Trust-Netzwerk beeinflusst nicht die Notwendigkeit eines Gastnetzwerks und ändert nicht die zuvor diskutierten Überlegungen.

Eine interessante Randbemerkung: Ihr Unternehmens-Gastnetzwerk wird wahrscheinlich mindestens so sicher sein wie öffentliche WLAN-Netzwerke, wie Flughäfen und Cafés. Und – wie wir in diesem Buch diskutiert haben – muss Ihr Zero Trust-System Ihren Benutzern den Zugriff auf Unternehmensressourcen von diesen Netzwerken aus ermöglichen. Daher gibt es keinen Grund, warum Ihre allgemeine Mitarbeiterpopulation nicht auch das Gastnetzwerk nutzen kann, genau wie wenn sie remote wären. Natürlich haben Unternehmen oft zusätzliche Sicherheits- oder Compliance-Kontrollen oder mehr Bandbreite für ihre Mitarbeiter-Netzwerke. Daher bevorzugen sie möglicherweise, dass die Mitarbeiter das Mitarbeiter-Netzwerk anstelle des Gastnetzwerks regelmäßig nutzen.

Mitarbeiter BYOD

Viele Organisationen erlauben es ihren Mitarbeitern, persönliche Geräte zu verwenden, um auf Unternehmensnetzwerke und unternehmensverwaltete Ressourcen zuzugreifen. Dies kann die Verwendung eines persönlichen Smartphones oder Tablets beinhalten, oder die Vorliebe eines Benutzers für eine bestimmte Art von Laptop-Gerät oder spezifisches Betriebssystem. Organisationen können einen laissez-faire-Ansatz verfolgen – den Benutzerzugriff von jedem Gerät aus erlauben – oder können ein gewisses Maß an Unternehmenspräsenz auf dem Gerät verlangen, wie die Installation von unternehmensausgestellten Zertifikaten oder Gerätemanagement-Software.[7]

Sicherheitsteams müssen entscheiden, ob und wie sie Mitarbeitern erlauben, BYODs zur Nutzung von Unternehmensressourcen zu verwenden. Mit traditionellen NACs kann dies je nachdem, wie streng der Netzwerkzugang kontrolliert wird und inwieweit das Sicherheitsteam die Installation von Zertifikaten oder Management-Software auf Benutzergeräten verlangt, möglich oder nicht möglich sein. Wir haben verschiedene Ansätze in Tab. 7-2 zusammengefasst. Beachten Sie, dass dies im Allgemeinen für

[7]Letzteres kann umstritten sein, da es genau an der Schnittstelle von Benutzerproduktivität, Datenschutz und Sicherheit liegt. Viele Mitarbeiter lehnen es ab, dem Sicherheitsteam ihres Arbeitgebers die Möglichkeit zu geben, ihr persönliches Smartphone zu manipulieren – mit (berechtigten) Bedenken hinsichtlich des Unternehmenszugangs zu privaten Informationen wie Fotos oder Browserverlauf. Dies führt dazu, dass sich einige Menschen für eine gefürchtete „Zwei-Telefon"-Existenz entscheiden.

Tab. 7-2. *BYOD-Konfiguration Vergleich*

Gerätekonfiguration	Mit NAC	Mit Zero Trust
„Reines“ BYOD – nichts installiert oder konfiguriert	Gastnetzwerk mit Internetzugang. Grobgranulare (vollständige Netzwerk-) Zugriffskontrollen über WLAN-Passwortsicherheit Gilt nur für Benutzer vor Ort	Gastnetzwerk mit Internetzugang Zugriff auf sichere Ressourcen mit „clientloser“ Zero Trust-Zugriff möglich. Gilt gleichermaßen für Benutzer vor Ort und Remote-Benutzer
BYOD mit Installation von Unternehmenszertifikaten	Mitarbeiternetzwerk (VLAN) Zugang über eingebauten 802.1x Supplicant. Bietet grobgranulare Zugriffskontrollen. Gilt nur für Benutzer vor Ort	Gleich wie „reines BYOD“. Im Allgemeinen erfordert der Zugriff auf den Gerätezertifikatspeicher die Installation von Client-Software
BYOD mit installierter und konfigurierter Software (Unternehmenszertifikat optional)	Mitarbeiternetzwerk (VLAN) Zugang über 802.1x (entweder eingebaut oder installiert). Kann Geräteposture-Checks über installierte Management Software beinhalten	Granulare Netzwerkzugriffskontrolle mit Zero Trust Client-Installation. Kann Zertifikat und Geräteposture-Checks für bedingten Zugriff verwenden. Gilt gleichermaßen für Benutzer vor Ort und Remote-Benutzer

Laptop- und Mobilgeräte gleich ist, obwohl es natürlich geringfügige Unterschiede zwischen den Betriebssystemen und Sicherheitsplattformen geben kann.

Gerätehaltungsprüfungen

Letztendlich ist diese Reihe von Anforderungen – den Zugang aller nicht autorisierten Benutzer und/oder Geräte zu blockieren, den Zugang von autorisierten, aber nicht konformen Geräten zu quarantänieren/beschränken und den eingeschränkten Zugang von autorisierten Benutzern auf validierten Geräten zu erlauben – sowohl für NAC als auch für Zero Trust-Lösungen üblich und tatsächlich wichtige Ziele für die Sicherheit, unabhängig von der zugrunde liegenden Implementierung. In diesem Kapitel haben wir versucht, die Funktionsweise von 802.1x-basierten NAC-Lösungen zu erklären und ihre

Mängel hinsichtlich ihrer Übereinstimmung mit Zero Trust-Prinzipien hervorzuheben. Als nächstes untersuchen wir das Thema der Gerätekonfigurationsanalyse. Beachten Sie, dass diese Fähigkeit außerhalb des Geltungsbereichs des 802.1x-Standards liegt, aber häufig in NAC-Produkten enthalten ist.

NAC-Lösungen bieten oft die Möglichkeit, Benutzergerätekonfigurationsprüfungen durchzuführen – gemeinhin als Haltungsprüfungen bezeichnet. Dies kombiniert die Abfrage von Geräteinformationen – wie das OS-Patchlevel oder das Vorhandensein einer aktuellen Antiviruslösung – mit der Fähigkeit, eine Richtlinie zu definieren und durchzusetzen, die bestimmt, auf welche Netzwerkressourcen (falls vorhanden) ein Gerät aufgrund seines Geräteprofils zugreifen können sollte. Ein gängiges Beispiel ist: Wenn ein Gerät nicht „auf dem neuesten Stand“ mit Sicherheits- oder A/V-Patches ist, quarantänieren Sie es auf ein “IT-Remediation” VLAN, das nur auf das IT-Helpdesk-Portal/Self-Service-Portal zugreifen kann.

Dies ist ein erstrebenswertes Ziel – tatsächlich müssen Geräteeigenschaften als Teil eines jeden Zero Trust-Richtlinien- und Durchsetzungsmodells enthalten sein. Natürlich erfordert dies die Fähigkeit, Geräteinformationen für die Verwendung innerhalb der Richtlinie zu erhalten – die verschiedenen Ansätze dazu sind in Tab. 7-3 dargestellt.

Letztendlich ist die Fähigkeit, Geräteeigenschaften zu erlangen, nur ein Teil der Gleichung – und, würden wir argumentieren, ein weniger wichtiger Teil. Die Fähigkeit, ein dynamisches Richtlinienmodell zu erstellen und durchzusetzen, um den Netzwerkzugang Zugang auf der Grundlage dieser Eigenschaften zu steuern, ist das Wichtigste. Wir werden später, in Kap. 17, ausführlich über ein Zero Trust-Richtlinienmodell sprechen.

Tab. 7-3. *Ansätze zur Gerätehaltung mit NAC*

Ansatz	Auswirkungen
Native 802.1x Supplicant	Geräteeigenschaften sind nicht Teil des 802.1x-Standards und werden möglicherweise nicht von eingebauten OS-Funktionen bereitgestellt
Produktspezifischer 802.1x Supplicant	Viele NAC-Produkte enthalten einen Client-Agenten (802.1x. supplicant) mit zusätzlichen Fähigkeiten zur Abfrage von Client-Geräteeigenschaften
Zusätzlicher Geräteagent (z. B., MDM)	Unternehmensgerätemanagementlösungen beinhalten die Fähigkeit, Gerätehaltungsinformationen abzurufen, die von einem Netzwerkzugriffspolicy-Durchsetzungspunkt verwendet werden können. Dieser Ansatz erfordert in der Regel eine Integration zwischen dem NAC-Authentifizierungsserver und einem EDM-Server über einen API-Aufruf

Geräteerkennung und Zugriffskontrollen

Wenn wir unseren Fokus wieder auf das Netzwerk richten, gibt es eine letzte Fähigkeit, die NACs typischerweise bieten, nämlich die Geräteerkennung und -sichtbarkeit. Offensichtlich ist die Fähigkeit, zu entdecken und zu berichten, welche Geräte in einem Unternehmensnetzwerk betrieben werden, eine Kernanforderung für Netzwerk- und Sicherheitsteams, und es gibt viele verschiedene Arten von Produkten, die dabei helfen können, nicht nur NACs. NACs bieten dies, weil sie Teil der Netzwerkinfrastruktur sind und neue Geräte auf der Infrastrukturebene erkennen, wenn sie sich mit dem Netzwerk verbinden. Diese Entdeckung ist ein direktes Nebenprodukt ihrer Arbeitsweise und ist notwendig, um jegliche Authentifizierung und VLAN-Zuweisung durchzuführen.

Zu verstehen, was in einem Netzwerk vorhanden ist (einschließlich Benutzer, Geräte und Arbeitslasten), ist natürlich eine Voraussetzung für die Anwendung eines Richtlinienmodells und die Durchsetzung von Zugriffskontrollen. Ein Schlüsselteil jedes Zero Trust-Modells ist, dass Entitäten authentifiziert werden müssen und dass das System eine Vielzahl von Attributen verwendet, um kontextbezogene Zugriffsentscheidungen zu treffen. NAC-Lösungen können *Teil* einer Zero Trust-Lösung sein (sowohl für grobkörnige Netzwerkzuweisungen wie in BeyondCorp als auch für Geräteerkennungsinformationen), können jedoch keine dynamischen, feinkörnigen und universellen Zugriffskontrollen für alle Benutzer und alle Ressourcen bereitstellen.

In Bezug auf das, was Sicherheits- und Netzwerkteams in Unternehmensnetzwerken (nicht Gastnetzwerken) erreichen müssen, haben wir dies zusammengefasst und NAC mit Zero Trust-Ansätzen in Tab. 7-4 verglichen.

Ein zusätzlicher Kommentar – die Verwendung von Geräte-MAC-Adressen für Zugriffskontrollen ist natürlich ein „nicht großartig, aber besser als nichts“-Ansatz, und jede Verwendung davon muss mit einem klaren Verständnis der damit verbundenen Risiken und des Bedrohungsmodells erfolgen. Es ist trivial für einen bösartigen Akteur mit physischem Zugang zu einem Netzwerk, seine MAC-Adresse zu ändern und sich als autorisiertes Gerät auszugeben, um Zugang zu erhalten. In Anbetracht dessen ist es wichtig, das Gedankenexperiment durchzuführen und sicherzustellen, dass, wenn dies passieren würde, das Gerät nur sehr begrenzten Zugang hätte (z. B. zu einem Drucker oder VOIP VLAN).

Tab. 7-4. *Gerätesicherheitsansätze in Unternehmensnetzwerken*

Gerätetyp	Mit NAC	Mit Zero Trust
Unautorisierte Geräte	Blockieren von jeglichem Netzwerkzugriff: kein VLAN, keine IP-Adresse zugewiesen	Blockieren des Zugriffs auf jegliche geschützte Ressourcen Kann den Internetzugriff blockieren Gerät ist im Netzwerk, kann aber nichts zugreifen
Autorisierte, aber nicht verwaltete oder nicht-802.1x-Geräte	VLAN-Zuweisung (typischerweise nach MAC-Adressgruppierung)	Zugriffskontrollen basierend auf Gerätetyp (z.B. MAC-Adressgruppierung) Feinkörniger als VLAN
Autorisierte und verwaltete oder 802.1x-fähige Geräte	Geräte authentifizieren und VLAN zuweisen (kann auf Identitätsgruppen basieren)	Authentifizieren und feinkörnige und identitätsspezifische Zugriffskontrollen anwenden

Zusammenfassung

In diesem Kapitel haben wir den Funktionsbereich der Netzwerkzugriffskontrolle vorgestellt und erklärt, wie das 802.1x-Protokoll funktioniert. Dann haben wir NAC-Lösungen aus der Perspektive von Zero Trust betrachtet und untersucht, wie NAC-Lösungen den Zugang zu Gastnetzwerken handhaben, was auch in Zero Trust-Netzwerken noch ein erforderlicher Anwendungsfall ist. Schließlich haben wir einige andere Aspekte von NAC in Betracht gezogen, einschließlich BYOD, Geräteprofile und Geräteerkennung.

NAC-Lösungen können Teil einer Zero Trust-Umgebung sein, insbesondere wenn sie benötigte Fähigkeiten rund um die Kontrolle des Gastnetzwerkzugangs bieten, aber 802.1x-basierte NAC-Funktionen sind nicht geeignet, um als zentraler Teil einer Zero Trust-Umgebung verwendet zu werden. Einige NAC-Anbieter haben über 802.1x hinaus innoviert und Zero Trust-Fähigkeiten hinzugefügt, obwohl Unternehmen, die sie in Betracht ziehen, sie sorgfältig gegen ihre Netzwerk- und Architekturanforderungen bewerten müssen.

KAPITEL 8

Intrusion-Detection- und -Prevention-Systeme

Unternehmenssicherheitsplattformen benötigen eindeutig die Fähigkeit, Eindringversuche zu verhindern und zu erkennen – was wir hier kurz als *unerwünschte Softwareausführung oder unerwünschte menschliche Aktivität auf einem Unternehmensgerät oder Netzwerk* definieren. Intrusion Detection Systems (IDS) bieten die Fähigkeit, *verdächtige Aktivitäten zu erkennen, protokollieren* und *zu melden,* und Intrusion Prevention Systems (IPS) fügen die Fähigkeit hinzu, *zu reagieren,* indem sie die Aktivität auf irgendeine Weise blockieren oder beenden. Intrusion Detection und Prevention Systems (IDPS[1]) verlassen sich typischerweise auf Signaturen (Mustererkennung) und/oder Anomalie-Erkennungsmechanismen (oft unter Verwendung statistischer Analysen oder maschinellem Lernen), um unerwünschte Aktivitäten zu identifizieren. Sie integrieren auch oft mit Bedrohungsintelligenzsystemen, um aktualisierte Daten zur Informierung ihrer Algorithmen zu erhalten. Diese Lösungen sind sowohl als eigenständige Lösungen als auch innerhalb vieler Next-Generation Firewalls (NGFWs[2]) verfügbar.

Traditionell waren IDPS am effektivsten in Umgebungen, in denen sie an gut definierten Netzwerk-„Engpässen" platziert werden können, Sichtbarkeit in den Verkehr erhalten und idealerweise eine tiefe Paketinspektion durchführen können. In einer Zero Trust-Architektur sind PEPs ein natürlicher Ort für diese Funktionen. Tatsächlich glauben wir, dass moderne IDPS, wenn sie in ein Zero Trust-System integriert sind,

[1]In diesem Kapitel beziehen wir uns auf die Gesamtkategorie als IDPS. Wenn wir einen der Bereiche im Besonderen diskutieren, verwenden wir entweder das IDS oder IPS Akronym.
[2]Tatsächlich, wie wir in Kap. 10 anmerken werden, war die Integration von IDPS in traditionelle Firewalls eine der Schlüsselfähigkeiten, die es diesen Anbietern ermöglichte, ihre Produkte glaubwürdig als „Next Generation" zu positionieren.

J. Garbis und J. W. Chapman, *Zero Trust Sicherheit*, https://doi.org/10.1007/979-8-8688-0105-1_8

effektiv zu einem PEP werden können. Wie andere Elemente in unserem Sicherheitsökosystem werden IDPS ihren Wert und ihre Effektivität steigern, wenn sie Zero Trust-Richtlinien konsumieren und durchsetzen können und als Quelle von Ereignissen für das PDP dienen, das wiederum andere PEPs dazu veranlasst, Maßnahmen zu ergreifen und beispielsweise Änderungen in den Benutzerrisikostufen oder Zugriffsrechten zu initiieren.

Eine abschließende einleitende Anmerkung zum Kontext – bisher haben wir nur netzwerkbasierte IDPS besprochen; es gibt eine weitere Kategorie von *hostbasierten* IDPS. Wir werden sie als nächstes vergleichen, um zu sehen, was sie tun und wie sie von der Umstellung auf Zero Trust betroffen sind.

Arten von IDPS

Es gibt zwei allgemeine Ansätze für kommerzielle IDPS, *hostbasierte* und *netzwerkbasierte,* die sich in ihrem Einsatzort und ihrer Einsatzweise unterscheiden, wie in Tab. 8-1 dargestellt. Beachten Sie, dass *Präventionssysteme* mindestens einige der *Erkennungsfunktionen* enthalten müssen; damit sie Maßnahmen ergreifen können, müssen sie natürlich zuerst unerwünschte (oder zumindest unerwartete) Aktivitäten erkennen.

Es sollte aus Tab. 8-1 klar sein, dass es eine sehr große Vielfalt an potenziellen Funktionen und Mechanismen gibt, mit denen Sicherheitslösungen unerwartete Aktivitäten erkennen und darauf reagieren können. Dieser Grad an Komplexität ist einer der Gründe, warum moderne IT und Informationssicherheit so herausfordernd sein können – es gibt viele Möglichkeiten, wie bösartige Aktivitäten ausgedrückt werden können, und es gibt viele potenzielle Ansätze zur Abwehr derselben. Einige dieser Aktionen, wie die Beendigung der Netzwerkverbindung, liegen eindeutig im Rahmen eines Zero Trust-Systems. Andere, wie die hostbasierte Prozessbeendigung oder die „Detonation“ von Sandbox-Inhalten, liegen wahrscheinlich außerhalb des Geltungsbereichs eines Zero Trust-Systems. Dennoch können diese Systeme einen Mehrwert schaffen, indem sie als Daten- oder Ereignisquelle für eine Zero Trust-Plattform dienen.

Jetzt, da wir etwas Kontext haben, betrachten wir die beiden IDPS-Bereitstellungsmodelle und diskutieren die Auswirkungen jeder Organisation, die zu einer Zero Trust-Architektur wechselt.

Tab. 8-1. *Typische Intrusion Detection und Prevention Funktionen, nach Einsatzmodell*

Funktionstyp	Erkennung	Prävention
Hostbasiert	Überwachung der Dateiintegrität Prozessverhaltensanalyse Netzwerk-Metadatenanalyse Lokale Protokoll- und Ereignisanalyse Protokoll- und Ereignisweiterleitung Überwachung des Verhaltens von Geräten oder Benutzern Überwachung der Softwareinstallation oder des Downloads Erkennung von Rechteerhöhung oder Rootkits	Prozess-Whitelisting Prozessbeendigung Verhinderung von Software-Download oder -Installation Beendigung der Netzwerkverbindung
Netzwerkbasiert	DNS-Überwachung Netzwerk-Metadatenanalyse Netzwerkverkehrsinspektion (Deep Packet Inspection)	DNS-Filterung Netzwerkinhaltsblockierung Beendigung der Netzwerkverbindung „Detonation“ verdächtiger Inhalte in einer Sandbox

Host-basierte Systeme

Host-basierte Intrusionserkennungs- und -verhinderungssysteme nutzen einen Software-Agenten, der entweder auf Benutzergeräten oder Servern (Ressourcen) läuft. Host-basierte Systeme haben den Vorteil, dass sie alles, was im Betriebssystem geschieht, einschließlich Prozess- und Netzwerkaktivität, tiefgehend untersuchen und lokale Aktionen durchführen können. Die lokale Präsenz auf dem Host ist in vielen Zero Trust-Implementierungen vorteilhaft, die typischerweise verschlüsselte Verkehrstunnel über Netzwerke nutzen (wir werden dies später in diesem Kapitel weiter untersuchen).

Ein Nachteil ist, dass diese Arten von Systemen die Installation und Verwaltung von Software auf potenziell großen Mengen von Geräten erfordern und in der Regel erhöhte Berechtigungen zum Ausführen benötigen. Diese Agenten haben auch das Potenzial, die

Akkulaufzeit von mobilen Geräten zu reduzieren, legitime Benutzeraktivitäten zu stören und die Geräteleistung auf allen Plattformen zu reduzieren. Dieser letzte Faktor könnte möglicherweise ein Problem sein, in Bezug darauf, wie er das Benutzererlebnis beeinflussen könnte.

Trotzdem empfehlen wir generell, dass Organisationen irgendeine Art von Agenten auf Geräten einsetzen, die auf geschützte Ressourcen zugreifen, aus verschiedenen Gründen, wie bereits in Kap. 3 diskutiert. Eine Herausforderung, mit der IT-Teams jedoch oft konfrontiert sind, ist die der Agentenproliferation (und funktionale Überschneidung zwischen Agenten), insbesondere auf Endbenutzergeräten. Dies ist ein ungelöstes Problem, da diese Agenten typischerweise als Binärdateien mit ihrem eigenen einzigartigen Bereitstellungs-Fußabdruck, Abhängigkeiten und Konfiguration verteilt werden. Eine Konsolidierung von Agenten und eine Koordination der Freigabe unter den Anbietern sind unwahrscheinlich und Unternehmen sollten realistischerweise nicht darauf zählen. Stattdessen müssen Sicherheitsteams die Realität akzeptieren und einen durchdachten Ansatz zur Agentenbereitstellung wählen. Glücklicherweise bieten moderne Geräte und Betriebssysteme in der Regel genügend Speicher und Verarbeitungskapazität zur Unterstützung des Betriebs mehrerer Agenten ohne signifikante Probleme.[3]

Netzwerkbasierte Systeme

Netzwerkbasierte IDS und IPS werden in das Netzwerk einer Organisation eingebunden, wo sie die Möglichkeit haben, den Netzwerkverkehr zu überwachen (und möglicherweise zu modifizieren). Moderne Netzwerke sind natürlich verteilt und segmentiert, und der Umfang und die Fähigkeiten eines netzwerkbasierten IDS/IPS-Systems hängen vollständig davon ab, wo die Systemknoten eingesetzt sind und auf welche Art von Netzwerkverkehr sie Zugriff haben. Zum Beispiel kann ein IDS, das innerhalb eines Mitarbeiter-LAN-Subnetzes eingesetzt wird, potenziell den Verkehr zwischen den Geräten auf diesem einen Subnetz oder den Verkehr zwischen diesen Geräten und entfernten Ressourcen untersuchen. Ein IDS auf einer WAN-Verbindung,

[3]Beachten Sie, dass Internet der Dinge (IoT) und einige Arten von nicht verwalteten Geräten im Allgemeinen die Installation von Software-Agenten nicht unterstützen. Netzwerkbasierte IDPS können natürlich mit diesen Geräten verwendet werden. Wir werden IoT-Geräte und „Dinge“ aus einer Zero Trust-Perspektive später in Kap. 16 untersuchen.

die verteilte Rechenzentren verbindet, kann möglicherweise den Verkehr zwischen den Rechenzentren untersuchen, aber keinen lokalen LAN-Verkehr innerhalb eines bestimmten Rechenzentrums oder Netzwerks sehen.

Netzwerk-IDPS können über einen Netzwerk-Tap oder Span-Port (passive Beobachtung des Verkehrs) oder in-line (Beobachtung des Verkehrs, während er durch den Knoten transitiert) eingesetzt werden. Der letztere Ansatz hat den Vorteil, dass er Verbindungen zuverlässiger beenden kann, wenn eine Bedrohung erkannt wird. Dieser in-line Ansatz ist einer der Gründe, warum NGFWs, die Intrusionserkennung und -verhinderung als Funktion beinhalten, ein beliebter und immer noch wachsender Markt sind.

Man könnte argumentieren, dass eine Organisation idealerweise netzwerkbasierte IDPS mit Knoten „überall“ einsetzen sollte, so dass das System in der Gesamtheit „allen“ Netzwerkverkehr überwachen kann. Unser Gegenargument ist jedoch, dass

- Organisationen könnten durch Kapital- und Betriebsbudgets eingeschränkt sein und nicht in der Lage sein, netzwerkbasierte IDPS im gesamten Netzwerk einzusetzen.
- In der heutigen Umgebung arbeiten viele Benutzer und Ressourcen auf Drittanbieternetzwerken, außerhalb der Kontrolle des Unternehmens – mit Benutzern, die von zu Hause aus oder in Hotelnetzwerken arbeiten, auf Ressourcen zugreifen, die möglicherweise in einer Cloud-Umgebung laufen (insbesondere IaaS). Traditionelle IDPS können möglicherweise nicht in diesen Umgebungen arbeiten.
- Schließlich macht die weit verbreitete Verwendung von verschlüsselten Netzwerkprotokollen es für netzwerkbasierte IDPS schwieriger, so effektiv zu sein, wie sie es in der Vergangenheit waren.

Zero Trust-Umgebungen machen diesen letzten Punkt noch relevanter und machen oft die Bereitstellung von netzwerkbasierten IDS schwieriger, da die von Zero Trust-Systemen häufig verwendeten verschlüsselten Tunnel den Verkehr für Netzwerkintermediäre weitgehend undurchsichtig machen. Die Auswirkungen, die verschlüsselte Netzwerkprotokolle auf netzwerkbasierte Sicherheitssysteme haben, sind ein interessantes Thema, das wir als nächstes betrachten werden.

Netzwerkverkehrsanalyse und Verschlüsselung

Offensichtlich verändert ein Zero Trust-System die Sicherheitsarchitektur und das Netzwerk eines Unternehmens. Es wird die Art und Weise ändern, wie verschiedene IT- und Sicherheitskomponenten miteinander interagieren, und auch das Netzwerk ändern – möglicherweise aus topologischer Sicht, aber definitiv durch Änderung der Netzwerksegmentierung und Auflegung zusätzlicher Verschlüsselungsebenen. Diese letzte Änderung ist besonders wichtig zu verstehen, insbesondere für Organisationen mit netzwerkbasierten IDS-Systemen.

Moderne Anwendungsprotokolle nutzen Verschlüsselung (am häufigsten TLS), wie sie sollten, da sie die Nachrichtenintegrität und Vertraulichkeit vor Netzwerkpeers oder Vermittlern gewährleistet. Dies impliziert natürlich, dass der Inhalt verschlüsselter Datenverkehr auch für autorisierte Netzwerkvermittler, die Sicherheitsfunktionen ausführen möchten, undurchsichtig ist. Die Lösung dafür ist die etablierte Praxis, dass der Vermittler ein aktiver Teilnehmer im Gespräch ist, einen verschlüsselten Link beendet und den anderen initiiert, um die Verkehrsinspektion durchzuführen.[4]

Dies wird in der Regel durch die Verteilung eines von der Unternehmens-PKI generierten Zertifikats ermöglicht, das auf einer Vertrauenswurzel basiert, die beiden Enden der verschlüsselten TLS-Verbindung gemeinsam ist – im Grunde ein legitimer Man-In-The-Middle (MITM) Angriff.

Wir haben erwähnt, dass dieser Ansatz gut etabliert ist und tatsächlich wird er von vielen Sicherheitsprodukten als Möglichkeit zur Untersuchung verschlüsselten Datenverkehrs verwendet. Es basiert jedoch auf einem einfachen Nutzungsmodell – der Einweg-Authentifizierung mit einem statischen Satz von Zertifikaten, bei dem der Client das Zertifikat des Servers als Teil des Aufbaus der TLS-Verbindung authentifiziert, der Server jedoch keine Validierung des Clients auf Netzwerkebene durchführt. Dies ist sehr nützlich für Modelle, bei denen der Server *sollte* legitim eine Verbindung von jedem Client akzeptieren und die Client-Authentifizierung später im Prozess auf Anwendungsebene durchführt. Die Einfachheit dieses Modells ist auch das, was es einem Zwischennetzwerksicherheitskomponenten ermöglicht, die TLS-Beendigung

[4]Obwohl technisch unkompliziert, ist dies dennoch ein komplexer Bereich, der Sicherheit mit Datenschutz und Regulierung ausbalanciert. Zum Beispiel sind Arbeitgeber in vielen Ländern oft gesetzlich verpflichtet, bestimmte Arten von Datenverkehr, wie den Zugang von Mitarbeitern zu persönlichen Gesundheitsseiten, **nicht** zu entschlüsseln.

durchzuführen, da es nur das Teilen eines einzigen, statischen Serverzertifikats erfordert.

Dieses Modell ist jedoch möglicherweise nicht in Zero Trust-Umgebungen anwendbar. Viele Zero Trust-Implementierungen verwenden gegenseitiges TLS (*mTLS,* auch bekannt als *Zwei-Wege-TLS*) für die Kommunikation zwischen dem Benutzeragenten PEP und dem Netzwerk PEP. Mit dieser Methode validieren beide PEPs das Zertifikat des anderen. Dies führt zu erhöhter Sicherheit, da ein bösartiger Akteur keinen MITM-Angriff mit nur einem einzigen gestohlenen Zertifikat durchführen kann – es erfordert den Besitz der Zertifikate beider Komponenten, ein viel unwahrscheinlicheres Szenario. Einige Zero Trust-Systeme gehen noch weiter und verwenden kurzlebige Zertifikate für diese Kommunikationen. Die Konsequenz dieser verbesserten Sicherheit ist, dass ein Standard-Netzwerk-IDPS, das „zwischen" PEPs läuft, nicht auf verschlüsselte Teile des Netzwerkverkehrs zugreifen kann. Das heißt, selbst wenn das IDPS Zugriff auf die Zertifikate hat, die zum Verschlüsseln des *Anwendungsprotokolls* verwendet werden, hat es keinen Zugriff auf die Zertifikate, die zum Verschlüsseln des *Zero Trust-Tunnels* verwendet werden.

Wir diskutieren dies im nächsten Abschnitt ausführlich, aber zuerst noch eine zusätzliche Anmerkung zu TLS. Die Branche befindet sich im Übergang zu TLS v1.3 (finalisiert im August 2018), das bestimmte Sicherheitsaspekte der TLS-Verbindung ändert und die Dinge für Netzwerksicherheitslösungen schwieriger macht. Insbesondere sind zusätzliche Teile des TLS-Handshakes jetzt verschlüsselt, was die Fähigkeit eines passiven Netzwerkbeobachters, bösartige Aktivitäten zu erkennen, verringert. Wenn Sie an einer tieferen Analyse interessiert sind, empfehlen wir dieses durchdachte und gut geschriebene IETF-Dokument, *Auswirkungen von TLS 1.3 auf operative Netzwerksicherheitspraktiken*.[5] Die Quintessenz ist, dass die Bewegung zu TLS 1.3 im Gange ist und eher angenommen als bekämpft werden muss.[6]

[5]Dieses Whitepaper ist hier verfügbar: https://datatracker.ietf.org/doc/draft-ietf-opsec-ns-impact/.

[6]Dies wird eine Abkehr von der passiven Netzwerkverkehrsüberwachung (sogar durch Inline-Geräte) und eine Hinwendung zur aktiven Man-in-the-Middle-TLS-Entschlüsselung oder hostbasierten IDPS erfordern. Die Auswirkungen davon könnten eine Reduzierung der Netzwerkleistung und die Notwendigkeit einer erhöhten Investition in Netzwerkinfrastrukturhardware und/oder hostbasierte IDPS-Lösung sein.

Zero Trust und IDPS

Moderne Sicherheitsinfrastruktur erfordert IDPS – im weitesten Sinne definiert – als allgemeines Set von Funktionen über die Plattformen einer Organisation hinweg. Dies wird weiterhin wichtig sein, auch wenn Organisationen sich in Richtung einer Zero Trust Sicherheitsarchitektur bewegen. Aber das *Wie* von IDS/IPS wird sich wahrscheinlich mit der Implementierung eines Zero Trust Ansatzes ändern. Organisationen müssen sich dessen bewusst sein und bereit sein, Änderungen vorzunehmen. Zum Beispiel wird Zero Trust Änderungen in der Netzwerksegmentierung und den Verschlüsselungsmustern des Netzwerkverkehrs mit sich bringen. Dies könnte Organisationen dazu veranlassen, ihre Nutzung von hostbasierten IDS/IPS zu erhöhen, oder mehr in netzwerkbasierte IDPS zu investieren, die Teil eines Zero Trust Systems sind. Dies ist in Abb. 8-1 dargestellt.

Abb. 8-1 zeigt die vier verschiedenen Zero Trust Deployment Modelle, mit netzwerkbasiertem IDPS (NIDPS) und hostbasiertem IDPS (HIDPS) dargestellt, zusammen mit dem verschlüsselten (getunnelten) Netzwerkverkehr und den impliziten Vertrauenszonen. Abhängig vom Zero Trust Deployment Modell kann der NIDPS durch den getunnelten Verkehr geblendet werden. Sie können dies in allen Szenarien in Abb. 8-1 sehen, wo ein NIDPS „Zero Trust-aware“ sein muss, wenn es zwischen PEPs betrieben werden soll – das bedeutet, dass es Teil des Zero Trust Systems ist und die Fähigkeit hat, den getunnelten Verkehr zu entschlüsseln. Standard NIDPS *kann* weiterhin betrieben werden, aber nur in den Szenarien B und C, wo es ein Netzwerksegment innerhalb der impliziten Vertrauenszone gibt, auf das das NIDPS eingesetzt werden kann.

Host-basierte IDPS werden weitgehend unbeeinflusst vom verschlüsselten Netzwerkverkehr weiterhin betrieben, da sie auf Hosts laufen und daher Zugang zum Netzwerkverkehr „hinter“ den PEPs haben. Während sie unverändert in einer Zero Trust Umgebung betrieben werden können, können hostbasierte Systeme tatsächlich mehr Wert liefern, indem sie sogar nur lose in die Zero Trust Umgebung integriert sind. Zum Beispiel könnte ein hostbasiertes System auf einem Server sein Maß an Prüfung und Alarmierung anpassen, wenn das Zero Trust System einen höheren Risikoscore für das Netzwerk des Hosts anzeigt.

Im Allgemeinen werden IDPS-Fähigkeiten wahrscheinlich eher in die Zero Trust Plattform eines Unternehmens „eingebaut“, anstatt ein eigenständiges Tool zu sein. In gewissem Maße – und abhängig von seinen Fähigkeiten – könnte man argumentieren,

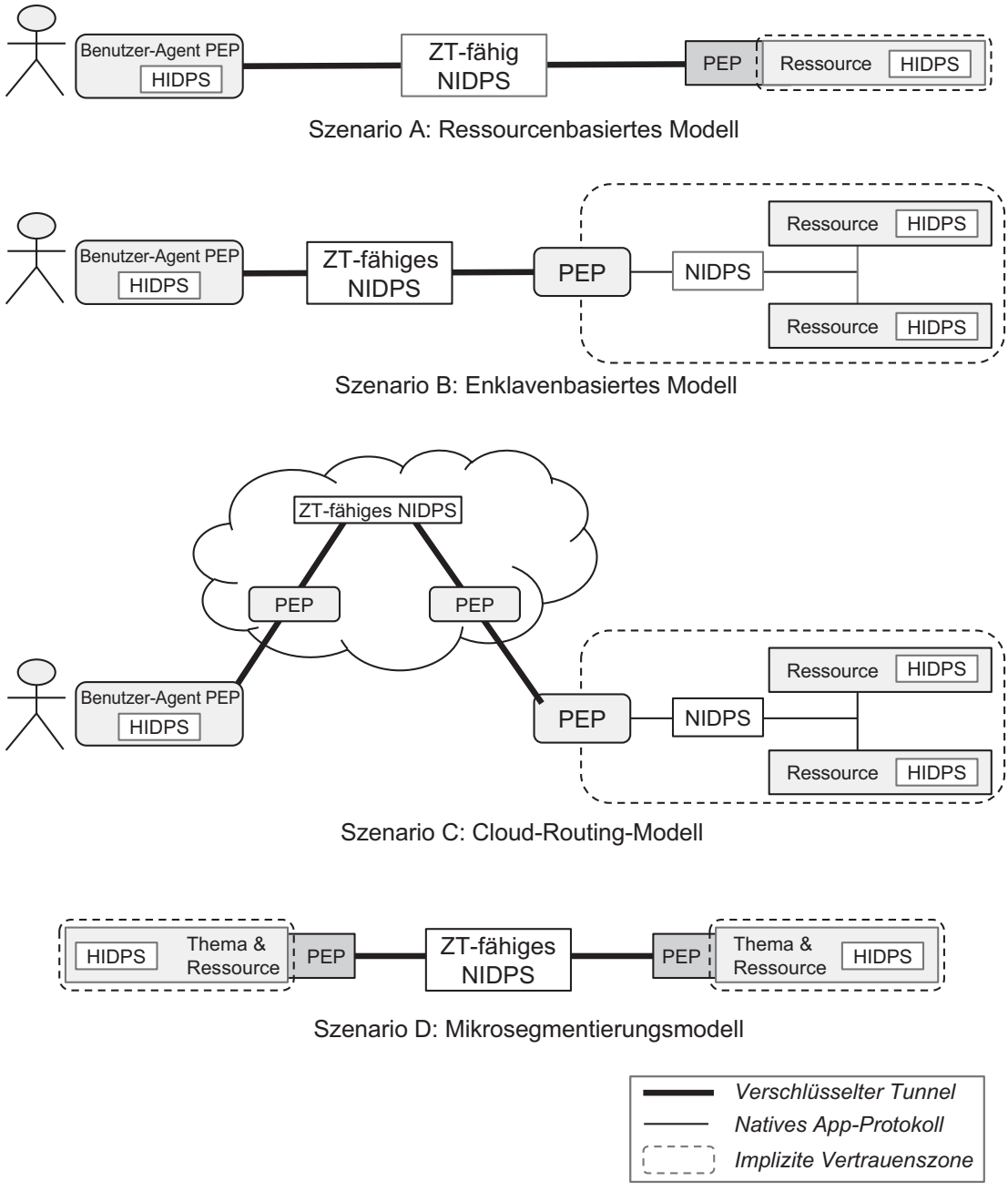

Abb. 8-1. *IDPS und Zero Trust Deployment Modelle*

dass das Zero Trust System tatsächlich das IDPS *wird*. Das heißt, IDPS wird nicht zu einer separaten Funktion, sondern zu einem inhärenten Teil des gesamten Sicherheitsgewebes. Sie können durch PEPs erreicht werden, die IDPS-Fähigkeiten enthalten, oder durch separate IDPS, die „hinter" den PEPs sitzen, mit einem gewissen Grad an Integration in die Zero Trust Umgebung. Sie sollten in der Lage sein, Richtlinien, Ressourcen-Metadaten oder Identitätskontext zu konsumieren, um das Maß an Inspektion und Durchsetzung anzupassen.

Zum Beispiel könnte der Netzwerkverkehr, der ein IDPS durchläuft und auf eine Ressource mit geringem Wert zugreift, nicht so strenge (lesen: ressourcenintensive) Analyse benötigen wie der Verkehr für eine Ressource mit hohem Wert. Oder der Zugriff von einem lokalen Benutzer auf ein unternehmenseigenes Gerät könnte weniger Prüfung erfordern als ein entfernter Benutzer, der von einem BYOD-Gerät aus zugreift. Diese Arten von Integrationen können die Infrastruktur reduzieren, die zur Unterstützung des IDPS benötigt wird, und können auch die Menge an Alarmen (Falschpositiven) reduzieren, zu denen IDPS neigen.

Die Integration mit Zero Trust ermöglicht es dem IDPS auch, eine breitere Palette von Maßnahmen in Reaktion auf erkannte Eindringversuche zu ergreifen. Während IDS nur benachrichtigen kann und IPS den versuchten Netzwerkzugriff blockieren kann, haben Zero Trust Systeme eine größere Reichweite und können global Maßnahmen ergreifen. Zum Beispiel können sie Benutzer zur stärkeren Authentifizierung auffordern oder Benutzergeräte in allen Netzwerken in Quarantäne stellen.

Betrachten wir einen weiteren Bereich – Client-seitige Sicherheitsprodukte (oftmals bestehend aus Antivirus und IDPS in einem einzigen Programm) sind ein wertvoller Bestandteil einer Zero Trust Sicherheitsarchitektur. Aber diese Lösungen können eine bessere Sicherheit (und mehr Wert) liefern, wenn sie mit einem Zero Trust Richtlinienmodell integriert sind, das als Netzwerk-Durchsetzungspunkt agieren kann. Zum Beispiel könnten Organisationen eine Zugriffsrichtlinie definieren wollen, die aktuelle Antivirus-Signaturen auf Client-Geräten erfordert, bevor der Zugriff auf unternehmensverwaltete Ressourcen erlaubt wird. Die Client-Profil-Daten können entweder vom Client bereitgestellt oder von einem zentralen Antivirus-Management-System bereitgestellt werden. In jedem Fall kann das Zero Trust System – als netzwerkbasierter Policy Enforcement Point – sicherstellen, dass nicht konforme Geräte keinen Zugriff auf Ressourcen haben und zum Beispiel nur den Zugriff auf einen IT-Helpdesk oder ein Selbstbedienungssystem zur Aktualisierung von Antivirus-Signaturen erlauben. Da Zero Trust den gesamten Netzwerkzugriff auf alle

Unternehmensressourcen kontrolliert, kann diese Richtlinie unabhängig vom Standort des Benutzers oder der Art und dem Standort der Ressourcen, auf die sie zugreifen, durchgesetzt werden.

Dies sind Beispiele dafür, wie wir glauben, dass diese Arten von Fähigkeiten richtig betrachtet werden sollten – nicht nur als IDS oder IPS Funktionen, sondern als Quellen von Daten (Input) in Zero Trust Systeme, als potenzielle Katalysatoren für Maßnahmen durch ein Zero Trust System und als Mechanismen zur Durchsetzung von Richtlinien. Wenn man die Dinge auf diese Weise angeht, kann sowohl die Sicherheit als auch die Effizienz verbessert werden, zum Beispiel durch die Ausrichtung der Richtliniendurchsetzung im gesamten Netzwerk und die Entfernung unnötiger oder redundanter Durchsetzungspunkte.

Es gibt keinen einzigen Weg oder eine einzige richtige Antwort darauf, wie diese Fähigkeiten eingesetzt werden können – es hängt ganz von der Sicherheitsinfrastruktur, dem Ökosystem und dem Ansatz zur Zero Trust einer jeden Organisation ab. Und das ist ein schwieriges Problem, mit vielen divergierenden Produkten und wenigen standardisierten Möglichkeiten, sie zusammenzubinden. Die gute Nachricht ist, dass die Branche in diesem Bereich Fortschritte macht. Zum Beispiel hat die Threat Intelligence Community standardisierte und strukturierte Wege zur Darstellung und Übertragung von Threat Intelligence Informationen entwickelt und gefördert, durch die STIX und TAXII Spezifikationen.[7]

Stellen Sie sich einen standardbasierten Threat Intelligence Feed vor, der ein Zero Trust System über neu entdeckte Malware informiert, die eine Schwachstelle in einer bestimmten Desktop-Client-OS-Version ausnutzt und spezifische Anwendungstypen ins Visier nimmt. Diese Informationen können verwendet werden, um die Prüfung, die ein IDPS auf die ins Visier genommenen Anwendungen legt, zu erhöhen und das Zero Trust PEP dazu zu bringen, die Installation eines Client-OS-Patches zu erzwingen, bevor irgendein Zugriff gewährt wird.

Wir sind optimistisch hinsichtlich der Arten von Integrationen, die diese Arten von Spezifikationen ermöglichen werden, und helfen Organisationen, mehr Wert aus ihrer bestehenden IT- und Sicherheitsinfrastruktur zu ziehen und ihren Weg zu Zero Trust besser voranzutreiben.

[7]STIX steht für Structured Threat Intelligence eXchange und TAXII für Trusted Automated eXchange of Intelligence Information. Siehe https://oasis-open.github.io/cti-documentation/ für weitere Informationen.

Zusammenfassung

In diesem Kapitel haben wir die Konzepte hinter Intrusion Detection und Prevention Systemen vorgestellt, einschließlich der Funktionen, die diese Systeme typischerweise ausführen. Wir haben auch die beiden Haupttypen, hostbasierte und netzwerkbasierte IDPS, verglichen und die Auswirkungen von verschlüsselten Netzwerkprotokollen auf IDPS diskutiert. Schließlich haben wir IDPS aus der Perspektive der Zero Trust Deployment Modelle betrachtet und das Potenzial für ihre Rolle als Zero Trust Policy Enforcement Point diskutiert.

KAPITEL 9

Virtuelle private Netzwerke

Virtuelle private Netzwerke (VPNs) wurden erstmals in den 1990er Jahren erstellt und eingesetzt, als Reaktion auf die zunehmende Verbreitung von Unternehmensnetzwerken, kombiniert mit einem zunehmend breiten Heimgebrauch von PCs (entweder „tragbare“ oder Desktop-PCs, die in den Häusern der Menschen eingesetzt wurden). Die zugrunde liegenden Netzwerkprotokolle haben sich natürlich im Laufe der Zeit weiterentwickelt und sind standardisierter (und sicherer) geworden, aber das Kernkonzept ist unverändert geblieben: Ein verschlüsselter Netzwerktunnel wird zwischen entfernten Knoten hergestellt, der es ermöglicht, Anwendungsdatenverkehr sicher durch diesen Tunnel zu übertragen, über ein nicht vertrauenswürdiges Zwischennetzwerk.

Heute ist der Begriff „VPN“ tatsächlich überladen und bezieht sich auf drei allgemeine Arten von Lösungen, wie in Abb. 9-1 dargestellt.

- Verbraucher-VPN: Schützt den Internetverkehr des Endbenutzers vor Vermittlern, für Datenschutz und Sicherheit. Häufig verwendet, um Datenschutz zu gewährleisten oder Beschränkungen zu umgehen, die von ISPs oder Regierungen auferlegt werden.
- Unternehmens-VPN: Verbindet entfernte Benutzer mit einem Unternehmensnetzwerk. Dies ist unser Fokus und die Art von VPN, die am stärksten von Zero Trust betroffen ist.
- Standort-zu-Standort-VPN: Dies ist eine der Möglichkeiten, wie Unternehmen WANs erstellen können.

J. Garbis und J. W. Chapman, *Zero Trust Sicherheit*, https://doi.org/10.1007/979-8-8688-0105-1_9

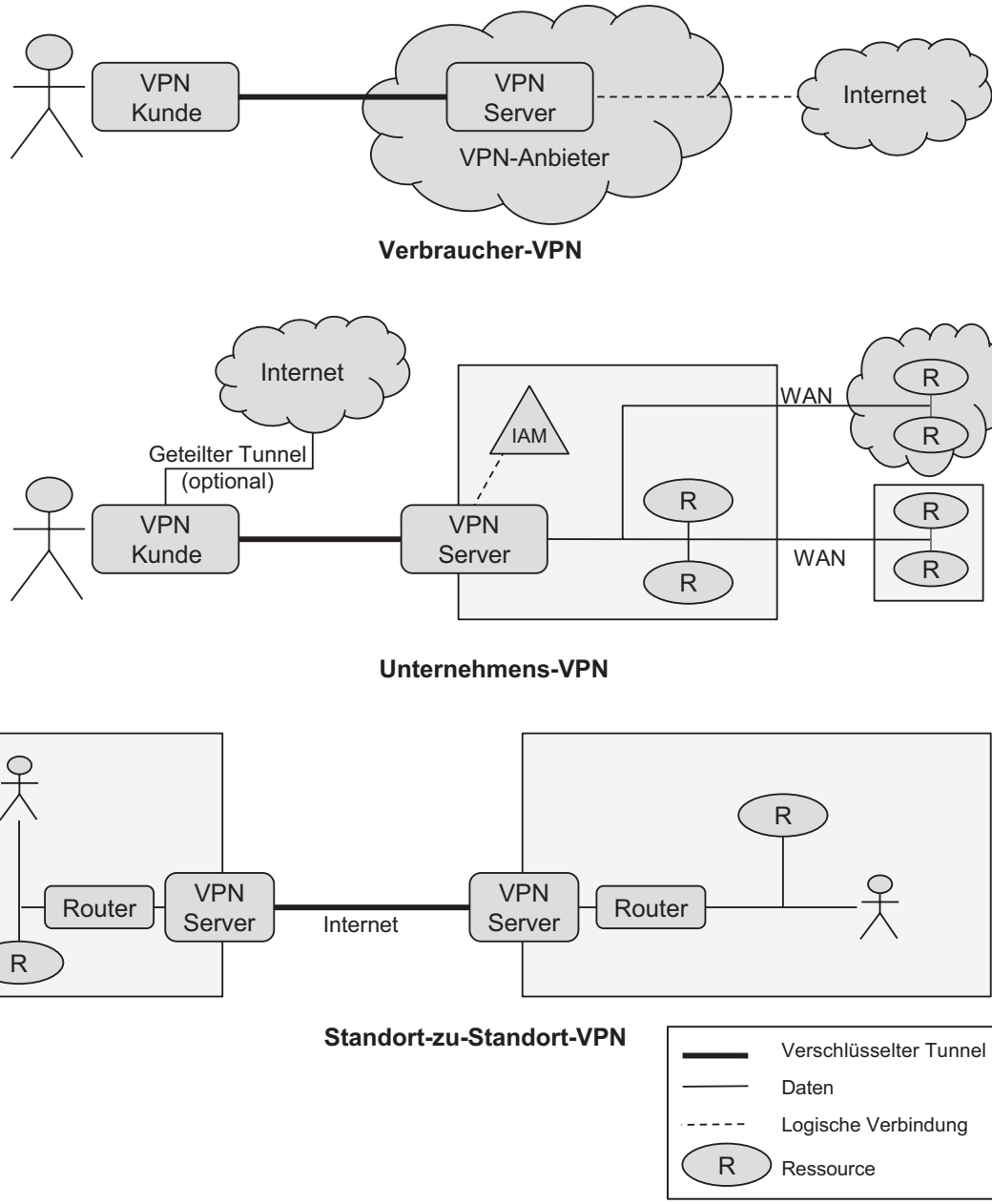

Abb. 9-1. *VPN-Arten*

VPNs erfordern zwei zusammenarbeitende Komponenten, die auf ein gemeinsames Geheimnis und/oder eine gemeinsame Vertrauenswurzel[1] angewiesen sind, um einen sicheren verschlüsselten Tunnel zu etablieren. Benutzerzentrierte und Unternehmens-VPNs stellen diesen Tunnel zwischen einem Benutzerdienst, der einen VPN Client ausführt, und dem VPN-Server (manchmal auch als *VPNKonzentrator* oder *VPNGateway* bezeichnet) her. Beachten Sie, dass der VPN-Client in diesem Fall separat installierte Software sein kann, im Betriebssystem des Benutzers enthalten ist oder sogar innerhalb eines Browsers ausgeführt wird.

In beiden dieser ersten beiden Szenarien wird ein Teil oder der gesamte Benutzerverkehr durch den verschlüsselten Tunnel gesendet, um die Privatsphäre und Integrität über die nicht vertrauenswürdigen Zwischennetzwerke zu wahren. Sobald der Verkehr den VPN-Server erreicht, wird er aus dem umschließenden Tunnel entfernt und an sein vorgesehenes Ziel weitergeleitet. Bei Verbraucher-VPNs wird der Verkehr zu einem Ziel im Internet gesendet, während bei Unternehmens-VPNs er zu einem Ziel irgendwo im internen Unternehmensnetzwerk geleitet wird. Beachten Sie, dass viele Unternehmens-VPNs „Split Tunneling“ unterstützen, bei dem nur der für das Unternehmensnetzwerk bestimmte Verkehr über den Tunnel gesendet wird; anderer Verkehr geht direkt vom Gerät des Benutzers aus. Die Alternative (voller Tunnel) leitet den gesamten Verkehr des Benutzers in das Unternehmen. Dies fügt Latenz (und Bandbreitenkosten) hinzu, ermöglicht es dem Unternehmen jedoch, Sicherheitsfunktionen auf dem gesamten Verkehr des Benutzers durchzuführen.

Standort-zu-Standort-VPNs funktionieren etwas anders und stellen einen sicheren verschlüsselten WAN-Tunnel zwischen zwei festen Standorten her, wodurch sie effektiv zu einem einzigen logischen LAN werden. In diesem Fall wird ein Teil des Verkehrs von Benutzern und Geräten auf diesen LANs über den VPN-Link geleitet, um das entfernte Ziel zu erreichen. Dies ist für die Benutzer transparent; sie führen keine VPN-Software aus, und ihr Verkehr erreicht einfach sein Ziel.

[1]Verschiedene Arten von VPNs gehen dies unterschiedlich an, z. B. TLS vs. IPSec. Der Unterschied ist für unsere Diskussion nicht relevant.

Unternehmens-VPNs und Sicherheit

Untersuchen wir nun das Unternehmen VPN-Szenario, beginnend mit den positiven Aspekten dessen, was sie bieten. Zunächst bieten sie natürlich einen verschlüsselten Tunnel für den Benutzerverkehr, zwischen dem Gerät des Benutzers und dem Unternehmensnetzwerk. Und sie sind in der Regel so konfiguriert, dass sie das Identitätsverwaltungssystem (IAM) des Unternehmens für die Benutzerauthentifizierung verwenden, oft über die LDAP- oder RADIUS-Protokolle.

Sie können auch grundlegende IAM-Attribute (wie Gruppenmitgliedschaften) verwenden, um Benutzer in VPN-Zugriffskontrollgruppen zu mappen. Einige VPNs können MFA zum Zeitpunkt der ersten Verbindung erzwingen, und einige bieten Host-Posture-Checks als zusätzlichen Kontext, um eine dynamische Zugriffskontrolle zu erreichen.

All diese Funktionen klingen positiv und sind in der Tat Fähigkeiten, die auch in einer Zero Trust-Lösung vorhanden sein müssen. Warum sind wir also negativ gegenüber Unternehmens-VPNs und bestehen darauf, dass sie ersetzt werden müssen?

Wir werden VPNs im nächsten Abschnitt aus einer Zero Trust-Perspektive untersuchen, aber selbst aus traditioneller Sicht haben Unternehmens-VPNs eine Reihe von Mängeln. Zum Beispiel können ihre Regeln zwar so eingerichtet werden, dass sie den Zugriff für einzelne IP-Adressen und Ports verwalten, in der Praxis tun sie dies jedoch nicht. Es ist viel einfacher für Netzwerk- und Sicherheitsteams, den Zugriff auf ein VLAN oder ein vollständiges Subnetz zuzuweisen – was in der Praxis wahrscheinlich der gleiche breite Zugriff ist, den Benutzer erhalten, wenn sie vor Ort sind.[2]

Nun, um fair zu sein, ist es durchaus möglich, VPNs zu verwenden, um einen begrenzten und fokussierten Zugriff auf eine minimale Menge von Unternehmensressourcen zu gewähren. Dies funktioniert am besten für Benutzer oder Benutzergruppen, die gut definiert sind und nur Zugriff auf eine bekannte, feste Menge von Anwendungen benötigen. Betrachten Sie zum Beispiel eine Gruppe von Remote-Mitarbeitern, die eine interne Anwendung zur Analyse von Versicherungsansprüchen verwenden. Diese Benutzer benötigen möglicherweise nur Zugriff auf diese eine Anwendung, um ihre Arbeit zu erledigen. Oder betrachten Sie einen Drittanbieter, der

[2]Wir finden es bitter ironisch, dass der zu permissive Netzwerkzugriff, der Benutzern vor Ort gewährt wird, als Rechtfertigung, wenn auch fehlgeleitet, verwendet werden kann, um entfernten Benutzern den gleichen breiten Zugriff zu gewähren.

nur Zugriff auf eine einzige Anwendung benötigt. In beiden Fällen kann, wenn die benötigten Anwendungen statische IP-Adressen haben, ein VPN verwendet werden, um einen begrenzten Netzwerkzugriff zu gewähren. Allerdings, selbst wenn dies der Fall ist (was normalerweise nicht für die meisten Benutzer zutrifft), weisen VPNs immer noch fünf weitere Mängel auf.

Erstens, obwohl VPNs das Unternehmens-IAM für Authentifizierung und Gruppenmitgliedschaft verwenden können und dies auch tun, sind die Zugriffskontrollrichtlinien in der Regel sehr einfach aus einer Identitätsperspektive. Zum Beispiel wird der Zugriff sehr oft für einen gegebenen Satz von Benutzerdaten gleich sein, unabhängig vom Gerät, von dem aus der Benutzer sich verbindet. Dies macht es für Sicherheitsteams schwieriger, den Zugriff von persönlichen Geräten einzuschränken oder den Missbrauch gestohlener Anmeldeinformationen zu verhindern.

Zweitens sind die Zugriffskontrollmodelle von VPNs sehr statisch aus einer *Ressourcen*-Perspektive – sie sind konfiguriert, um Zugriff auf ein festes Subnetz oder eine Reihe von IP-Adressen oder Hostnamen zu gewähren. Sie sind einfach nicht dafür ausgelegt, Zielressourcen dynamisch aufzulösen und den Benutzerzugriff anzupassen. Die heutigen IT-Umgebungen neigen dazu, dynamisch zu sein, insbesondere für Organisationen, die virtualisierte Ressourcen verwenden oder ein DevOps-Modell verwenden. Dies führt dazu, dass Organisationen zu breiten Netzwerkzugriff gewähren, um die Produktivität der Benutzer aufrechtzuerhalten.

Drittens, wie in Abb. 9-1 dargestellt, zwingen VPNs den Organisationen ein bestimmtes Netzwerk Modell auf – sie unterstützen nur einen einzigen Zugangspunkt zum Unternehmensnetzwerk. Dies perpetuiert ein perimeterbasiertes Netzwerkmodell, in dem alle Unternehmensressourcen über ein internes Netzwerk (LAN oder WAN) verbunden sein müssen. Wie wir im gesamten Buch diskutiert haben, stellt dies ein Sicherheitsrisiko dar und ist oft technisch schwierig oder unmöglich in der heutigen verteilten und cloudbasierten Welt zu erreichen. Die Auswirkungen davon sind, dass entweder das Netzwerk der Organisation unnötig offen ist, oder Benutzer gezwungen sind, sich ständig von einem anderen VPN-Server zu trennen und wieder zu verbinden, um auf spezifische Ressourcen zuzugreifen. Letzteres wird definitiv Endbenutzer frustrieren und behindern.[3]

[3]Die Split-Tunneling-Fähigkeiten von Unternehmens-VPNs helfen hier nicht – sie trennen nur unternehmensgebundenen Verkehr (der durch den einzelnen Tunnel gesendet wird) von Internet-gebundenem Verkehr (nicht getunnelt).

Viertens, damit Benutzer sich verbinden können, *müssen* VPN-Server einen offenen Port im Internet freigeben. Dies macht sie zu einem einladenden Ziel für Angreifer weltweit. Leider gab es in der jüngsten Vergangenheit viele, viele öffentlich bekannt gewordene VPN-Schwachstellen, bei denen unbefugte Remote-Benutzer einen VPN-Server kompromittieren und Zugang zum Unternehmensnetzwerk erhalten können. Aus unserer Sicht ist es in der heutigen Bedrohungslandschaft unverantwortlich, die „Haustür" Ihres Unternehmensnetzwerks auf diese Weise freizugeben.

Und fünftens sind VPNs letztendlich nur ein Remote-Zugriffstool – und als solches sind sie ein Silo. Sie können nicht verwendet werden, um Zugriffskontrollen für Benutzer vor Ort durchzusetzen. Organisationen sind gezwungen, ein separates Set von Netzwerk- und Sicherheitstools für Benutzer vor Ort bereitzustellen und zu verwalten. Dies führt zu doppelten Ausgaben, doppelter Arbeit und inkonsistenten Zugriffskontrollen über die Toolsets hinweg (was wiederum wahrscheinlich zu einem zu breiten Netzwerkzugriff führen wird, um die Produktivität der Benutzer nicht zu beeinträchtigen).

VPNs weisen offensichtlich viele Sicherheitsmängel auf, zusätzlich zu einer allgemein schlechten Benutzererfahrung, begrenzter Bandbreite, abgebrochenen Verbindungen und Anwendungskonflikten. Das sind die Gründe, warum wir so vehement auf ihre Beseitigung bestehen. Lassen Sie uns sie nun mit einem Zero Trust-Ansatz kontrastieren.

Zero Trust und VPNs

Aus einer Zero Trust-Perspektive sollten VPNs wirklich als *Fernzugriff*-Tools und nicht als *Sicherheits*-Tools betrachtet werden. Wir erkennen an, dass dies eine kontroverse Haltung ist und dass Organisationen mit ihren VPNs ein gewisses Maß an Erfolg erzielt haben können, aber wir glauben, dass VPNs zu viele Mängel aufweisen, um ihre fortgesetzte Nutzung zu rechtfertigen. Das heißt, selbst ein gut konfiguriertes VPN wird unter Einschränkungen leiden, die eine ordnungsgemäße Zero Trust-Lösung nicht aufweisen sollte. Lassen Sie uns untersuchen, wie und warum dies der Fall ist.

Eine Zero Trust-Lösung sollte den Benutzerzugriff dynamisch anpassen, basierend auf kontextbezogenen Informationen über den Benutzer, das Gerät, das Netzwerk, das System und die Zielressourcen. All dies sollte vom zentralisierten PDP gesteuert werden. Die Lösung sollte auch eine stufenweise Authentifizierung unterstützen, basierend auf Kontext und Benutzeraktivität. Die Zero Trust-Lösung sollte auch die Möglichkeit

unterstützen, dass entfernte Identitäten mehrere gleichzeitige Zugangspunkte zum Unternehmensnetzwerk haben. Dies beseitigt die Anforderung, dass alle verteilten Ressourcen von diesem einzigen Zugangspunkt aus zugänglich sein müssen (das traditionelle, auf dem Perimeter basierende Sicherheitsmodell). Das Zero Trust-Modell unterstützt von Natur aus verteilte PEPs, die jeweils eine logisch oder physisch zusammenhängende Ressourcengruppe schützen, wie in Abb. 9-2 dargestellt. Da die Benutzer diese PEPs direkt nutzen, besteht für das Unternehmen keine Notwendigkeit, WAN-Verbindungen zwischen jedem der verteilten Standorte aufrechtzuerhalten.

Lassen Sie uns nun die beiden letzten Wege betonen, in denen Zero Trust-Systeme VPNs überlegen sind. Erstens sollten Zero Trust-Systeme den Netzwerkeinstiegspunkt des Unternehmens vor unbefugten Benutzern verbergen. Das heißt, nach dem Prinzip der geringsten Berechtigung sollten entfernte Einheiten, die keine Berechtigung zum Zugriff auf Unternehmensressourcen haben, den Netzwerkeinstiegspunkt nicht sehen

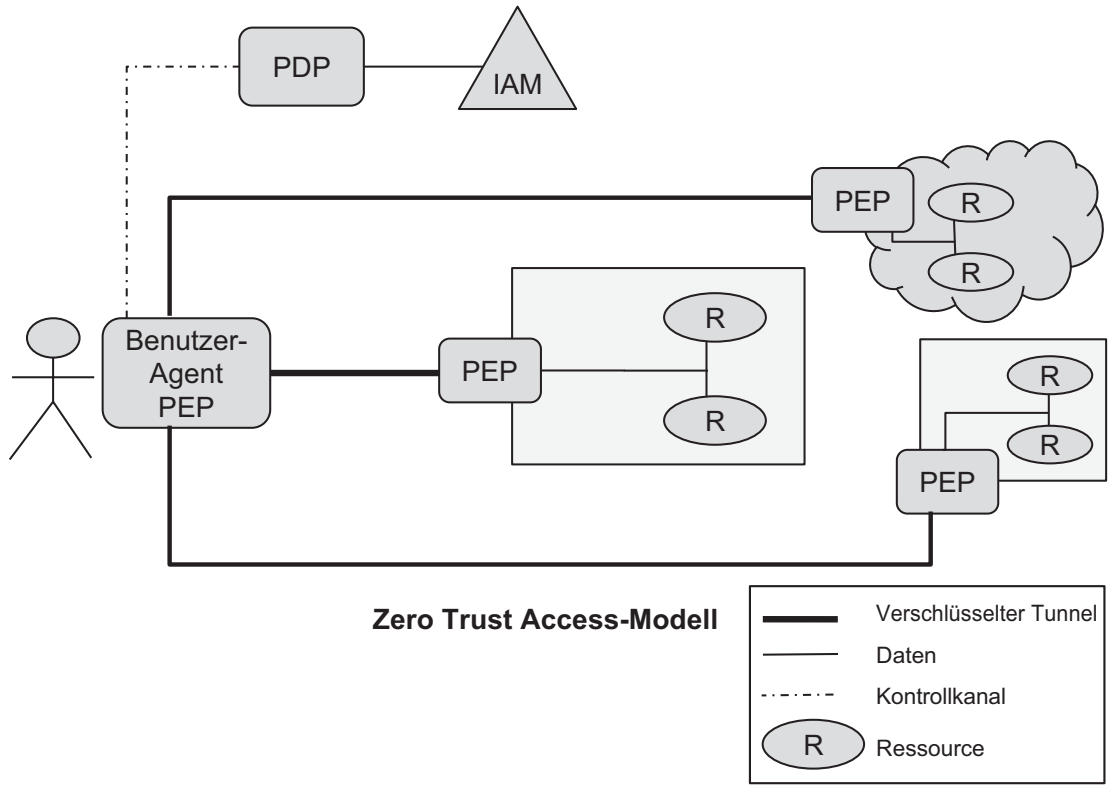

Abb. 9-2. *Zero Trust Zugangsmodell*

oder sich damit verbinden können. Dies ist an sich ein großer Fortschritt in Bezug auf die Sicherheit. Beachten Sie, dass dies auf zwei Arten erreicht werden kann – entweder durch Tarnung des Netzwerkeinstiegspunkts, so wie es der Software-Defined Perimeter macht[4] oder durch Verlagerung des Einstiegspunkts vom Unternehmensnetzwerk zu einer Cloud-gehosteten Plattform eines Anbieters (wie im Cloud-Routed-Modell).

Schließlich und vielleicht am wichtigsten bietet Zero Trust (nach Design) ein einheitliches Zugriffskontrollmodell für Benutzer vor Ort und Remote-Benutzer. VPNs sind *nur* Fernzugriffssilos und verlängern als solche nur die Kopfschmerzen und Ineffizienzen, die mit einer eigenständigen Lösung verbunden sind. Das einheitliche Zugriffskontrollmodell von Zero Trust vereinfacht die Abläufe und bietet Organisationen eine zentrale Plattform, innerhalb derer sie Zugriffskontrollrichtlinien in allen Umgebungen definieren und durchsetzen können.

Bevor wir dieses Kapitel abschließen, möchten wir kurz diskutieren, wie die verschiedenen Zero Trust-Bereitstellungsmodelle den Fernzugriff angehen, da sie unterschiedlich sein können. Die Enklaven-basierten und Cloud-gerouteten Modelle bieten beide von Natur aus Fernzugriffsfähigkeiten als Teil ihrer Architekturen und werden daher VPNs vollständig ersetzen. Die beiden anderen Zero Trust-Bereitstellungsmodelle, ressourcenbasiert und Mikrosegmentierung, bieten jedoch möglicherweise keine eingebauten Fernzugriffsfähigkeiten. Bei der Bewertung potenzieller Anbieter und Architekturen ist es wichtig, ein klares Verständnis dieser Anforderungen und potenziellen Unterschiede zu haben und mit einem geeigneten Fragenkatalog ausgestattet zu sein, um die verschiedenen Angebote zu unterscheiden und zu bewerten.

Zusammenfassung

VPNs bieten einen veralteten und ehrlich gesagt unsicheren Ansatz für den Fernzugriff und müssen ausgemustert oder ersetzt werden, wenn Organisationen zu Zero Trust wechseln. Wie wir in diesem Kapitel erläutert haben, sind VPNs fehlerhafte Lösungen, so sehr, dass selbst gut eingesetzte und gut verwaltete VPN-Implementierungen unter einigen erheblichen Mängeln leiden. Es ist an der Zeit, dass Organisationen

[4]Mit Single-Packet Authorization, wie in Kap. 4 diskutiert.

vorankommen und ein reichhaltigeres und effektiveres Set von Tools nutzen, um ihre Zugriffskontrollmodelle zu erstellen.

Mit der Einführung von Zero Trust sollte Ihre Unternehmensnetzwerk- und Sicherheitsinfrastruktur keine Fernzugriffslösung (Unternehmens-VPN) enthalten. Sie sollte einfach eine *Zugriffslösung* sein, die so eingesetzt wird, dass sie den Zugriffskontrollen sowohl für Remote- als auch für On-Premises-Benutzer durchsetzt, basierend auf einer einheitlichen Plattform und einem Richtlinienmodell. Und im Gegensatz zu VPNs umarmt es eher die verteilte Natur der Ressourcen, auf die die Benutzer zugreifen.

KAPITEL 10

Next-Generation-Firewalls

In diesem Kapitel werden wir uns hauptsächlich mit der Stellung von Next-Generation Firewalls (NGFWs) in einer Zero Trust-Landschaft befassen. Wir haben tatsächlich bereits die meisten der Hauptfunktionen besprochen, die Teil von NGFW-Produkten sind, einschließlich Kern-Firewalling, IDS/IPS und VPN, in vorherigen Kapiteln. Daher wird dieses Kapitel die Rolle diskutieren, die NGFW-Fähigkeiten und -Plattformen in einer Zero Trust-Welt spielen sollten, anstatt eine direkte Analyse ihrer Funktionalität.

Unser Ziel ist es, Ihnen zu helfen zu verstehen, wo und wie NGFW-Lösungen Teil Ihrer Zero Trust-Architektur sein sollten und wie Sie sicherstellen können, dass sie gut in den Rest Ihrer Unternehmenskomponenten integriert werden können. Um das zu tun, werden wir zunächst die Marktkategorie untersuchen.

Geschichte und Entwicklung

Unternehmensnetzwerk-Firewalls begannen mit einem sehr fokussierten Satz von grundlegenden Netzwerkfunktionen – der klassischen 5-Tupel-Firewall-Regel, die in Kap. 6 eingeführt wurde. Diese traditionellen Firewalls – insbesondere aus heutiger Sicht – waren eindeutig stärker auf *Netzwerk* (Erlauben oder Nicht-Erlauben von Netzwerkpaketen) ausgerichtet, ohne Konzept von *Identität*. Im Laufe der Zeit haben erfolgreiche Firewall-Anbieter Innovationen hervorgebracht und schließlich hat sich der Markt auf den Begriff „Next-Generation“ geeinigt.

Heute sind im Grunde alle Unternehmensfirewalls „Next Generation“ und beinhalten typischerweise IDS/IPS, Verkehrsanalyse und Malware-Erkennung zur Bedrohungserkennung, URL-Filterung und ein gewisses Maß an Anwendungsbewusstsein/Kontrolle. Wie das NAC-Marktsegment begannen Anbieter in diesem Bereich eine Reise zur identitätszentrierten Sicherheit etwa zur gleichen Zeit, als

J. Garbis und J. W. Chapman, *Zero Trust Sicherheit*, https://doi.org/10.1007/979-8-8688-0105-1_10

Zero Trust-Ideen in der Branche aufkamen. Heute bieten viele NGFW-Anbieter Zero Trust-Fähigkeiten an, mit unterschiedlichem Erfolg bei der Erfüllung der von uns zuvor skizzierten Prinzipien. Lassen Sie uns sie aus dieser Perspektive betrachten.

Zero Trust und NGFWs

Wir glauben, dass es fair und angemessen ist, einigen NGFW-Anbietern Anerkennung dafür zu geben, dass sie Pioniere bei der Ermöglichung und Durchsetzung einiger Zero Trust-Prinzipien für Unternehmensnetzwerke vor Ort waren. Ihre NGFW-Produkte bieten ein Maß an Identitätszentrierung und feinkörnigen Richtlinien, erfüllen aber nicht unsere Zero Trust-Prinzipien. Am bemerkenswertesten ist, dass NGFWs immer noch Firewalls sind, in dem Sinne, dass ihr Kontrollbereich begrenzt ist. Am bemerkenswertesten ist, dass sie keine Plattformen sind, die Sicherheit für „alle Benutzer für alle Ressourcen unabhängig vom Standort“ bieten können – das ist einfach kein Designziel. Sie bieten keinen feinkörnigen Remote-Zugriff, haben in der Regel keine Benutzerauthentifizierung, Verschlüsselung oder Geräteisolierung (kein Benutzeragent PEP) und sind typischerweise hardwarebasiert.

Natürlich haben NGFW-Anbieter ihre Plattformen weiterentwickelt und erweitert, durch Akquisitionen und organische Feature-Entwicklung, und haben Remote-Zugriff und andere Fähigkeiten hinzugefügt, wie wir in früheren Kapiteln behandelt haben. Obwohl dies ein erfolgreicher Markt war, und es NGFW-Anbieter mit glaubwürdigen Zero Trust-Angeboten gibt, glauben wir nicht, dass es ganz genau wäre zu sagen, dass der NGFW-Bereich sich in Zero Trust verwandelt hat. Es gibt viele glaubwürdige Zero Trust-Anbieter, die nicht aus einer NGFW-Perspektive begonnen haben und deren Plattformen unterschiedliche Architekturen haben.

Es ist wichtig zu verstehen, dass wir nicht versuchen, spezifische Angebote oder Architekturen von Anbietern zu analysieren – wie wir in unserer Einleitung besprochen haben, ist das ein sich schnell bewegendes Ziel und eine solche Bewertung wäre weder genau noch fair. Was wir versuchen zu tun, ist eine Erklärung und ein Rahmen zu liefern, damit Sie die funktionalen Komponenten verstehen können, die typischerweise einen NGFW ausmachen, und sie aus der Perspektive einer Zero Trust-Architektur bewerten können.

Eine Zero Trust-Architektur kann Produkte enthalten, die als NGFWs kategorisiert sind, oder auch nicht. Aber sie wird sicherlich diese Fähigkeiten enthalten, die historisch

Teil von NGFWs waren – wie IDS/IPS und ein identitäts- und anwendungsbewusstes Richtliniendurchsetzungsmodell. Daher ist es wichtig, über die Rolle von NGFWs in einer Zero Trust-Architektur zu sprechen. Es gibt zwei Aspekte davon, die wir behandeln möchten: erstens die Auswirkungen der Verschlüsselung des Netzwerkverkehrs zwischen den Komponenten im Netzwerk und zweitens die allgemeine Netzwerk-Topologie, die NGFW-basierte Lösungen möglicherweise auferlegen.

Netzwerkverkehr-Verschlüsselung: Implikationen

Eine wichtige Implikation der Zero Trust-Prinzipien ist, dass der Netzwerkverkehr verschlüsselt sein muss, entweder innerhalb seines nativen Anwendungsprotokolls (z. B. HTTPS) oder als Ergebnis der Weiterleitung durch einen verschlüsselten Tunnel. Während ersteres für einige Szenarien geeignet ist (z. B. SaaS-Anwendungen), stützen sich die meisten Zero Trust-Implementierungen auf einen verschlüsselten Tunnel in eine PEP, aus verschiedenen Gründen, die wir in Kap. 3 diskutiert haben. Die Implikationen davon sind, dass der Verkehr zwischen Benutzeragenten und den Netzwerk-PEPs für jedes zwischenliegende Netzwerkkomponente undurchsichtig wird. Wir haben dieses Thema in unserem Kapitel über IDS/IPS angesprochen und möchten es hier aus einer etwas anderen Perspektive erneut besuchen.

Netzwerkverkehr, der zwischen dem Gerät des Benutzers und einer PEP verschlüsselt ist, hat mehrere Implikationen, wie in Abb. 10-1 dargestellt.[1] In allen Fällen können zwischenliegende Netzwerkkomponenten (Middleboxes) weiterhin Kern-Firewall-Funktionen ausführen, die auf Netzwerkheader-Ebene arbeiten und keinen Zugriff auf verschlüsselte Nutzdaten benötigen. Alle Funktionen, die Zugriff auf Nutzdaten benötigen, können „hinter“ der PEP bereitgestellt werden, wenn der Netzwerkverkehr aus dem verschlüsselten Tunnel extrahiert wurde und mit seinem nativen Anwendungsprotokoll übertragen wird. Beachten Sie, dass dies per Definition innerhalb der impliziten Vertrauenszone stattfindet, wie in Abb. 10-1, Szenario A dargestellt.

Wenn die vernetzte Komponente dazu bestimmt ist, Analysen durchzuführen oder Maßnahmen auf der Grundlage der Nutzdaten zu ergreifen, hat sie keine andere Wahl, als die Nutzdaten zu entschlüsseln, wie in Szenario B dargestellt. Dies impliziert, dass

[1]Beachten Sie, dass dieses Diagramm das Enklaven-basierte Bereitstellungsmodell darstellt. Ähnliche Argumente gelten für die anderen Zero Trust-Bereitstellungsmodelle.

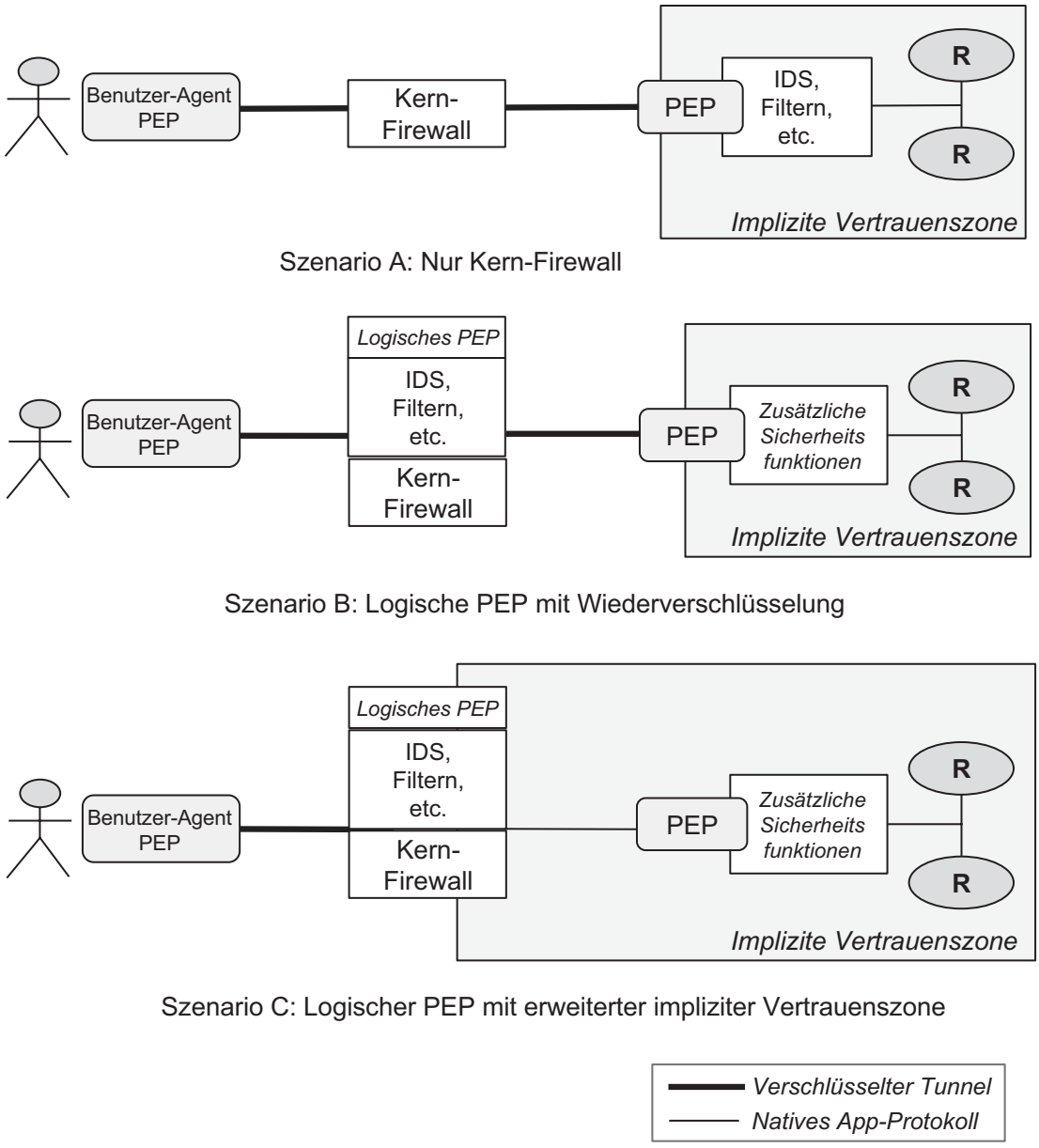

Abb. 10-1. *Next-Generation Firewall Bereitstellungsszenarien*

die NGFW eine logische Zero Trust-PEP ist – aus unserer Sicht muss sie, wenn sie Zugang zum Verschlüsselungsschlüssel hat, als Teil der Zero Trust-Plattform betrachtet werden. Diese logische PEP führt eine oder mehrere Sicherheitsfunktionen aus (wie IDS oder URL-Filterung), die auch das Proxying von Anwendungsverkehr erfordern können.

Szenario B stellt die Situation dar, in der diese Komponente den Netzwerkverkehr erneut verschlüsselt und ihn zur zweiten PEP und durch einen weiteren Tunnel in die implizite Vertrauenszone sendet. Dieses Szenario erfordert eine erhebliche Verarbeitung durch die NGFW, was Netzwerklatenz hinzufügt und möglicherweise ein leistungsfähigeres (und teureres) Gerät mit der notwendigen Leistung erfordert.[2]

Alternativ kann die NGFW den Anwendungsverkehr zur zweiten PEP senden, ohne ihn erneut zu verschlüsseln, wie in Szenario C gezeigt. Dies reduziert (etwas) die Arbeitslast auf der NGFW, führt aber auch zu einer erweiterten impliziten Vertrauenszone, so dass Sie die Implikationen davon in Ihrer Umgebung und Ihrem Netzwerk verstehen müssen. In beiden Szenarien B und C können die bestehende PEP (oder Komponenten dahinter) zusätzliche Sicherheitsdurchsetzungsfunktionen ausführen.

Es ist sehr wichtig, sich über mögliche Missverständnisse der Richtlinien im Klaren zu sein, die von der NGFW als logische PEP und der zweiten PEP durchgesetzt werden. Dies ist besonders wichtig, wenn diese Sicherheitskomponenten von verschiedenen Anbietern bereitgestellt werden oder unterschiedliche Richtlinienmodelle haben. Nichts davon soll implizieren, dass Zero Trust-Plattformen von den NGFW-Anbietern grundsätzlich besser oder effektiver sind als Alternativen – tatsächlich gibt es, wie wir gleich sehen werden, zusätzliche Kompromisse und Überlegungen, die Beachtung verdienen.

Netzwerkarchitekturen

In jeder Zero Trust-Architektur ist es entscheidend, dass Ihr Team ein solides Verständnis der gesamten Netzwerk-Topologie einer Lösung hat und wie sie mit Ihrer Unternehmensnetzwerkarchitektur übereinstimmt. Solche Architekturen entwickeln sich in gewisser Weise ständig weiter – beispielsweise durch die Einführung von Cloud-basierten Ressourcen – und sind in gewisser Weise sehr statisch oder unveränderlich, zum Beispiel WAN-Verbindungen, die möglicherweise seit Jahren bestehen.

Wir untersuchen dieses Thema hier, weil einige auf NGFW basierende Lösungen bestimmte Netzwerkarchitekturen erfordern oder bestimmte Einschränkungen auferlegen können, die die Fähigkeit, reibungslos auf Ihrem Weg zu Zero Trust

[2]Zu interpretieren als RAM, CPU-Geschwindigkeit, etc.

fortzufahren, einschränken können. Schauen wir uns zwei Beispiele für Zero Trust-Netzwerkarchitekturen an, die in Abb. 10-2 dargestellt sind.

Szenario A zeigt eine Architektur, die von auf NGFW basierenden Zero Trust-Plattformen auferlegt werden kann, mit einem einzigen Zugangspunkt zum Unternehmensnetzwerk für Remote-Benutzer. Verteilte Ressourcen (die heute alle modernen Unternehmen nutzen) erfordern ein Wide Area Network oder Rückgrat. Das WAN hat einfache Firewalls an den Eingangspunkten der Remote-Netzwerke, die grundlegende Netzwerkzugriffssteuerungslisten (ACL) durchsetzen.

Das übergreifende Problem mit diesem Ansatz ist, dass es die Vorstellung von einem harten Perimeter mit einem weichen internen Netzwerk aufrechterhält. Da PEP1 der einzige Punkt ist, an dem Zero Trust-Grundsätze durchgesetzt werden, bleibt diese

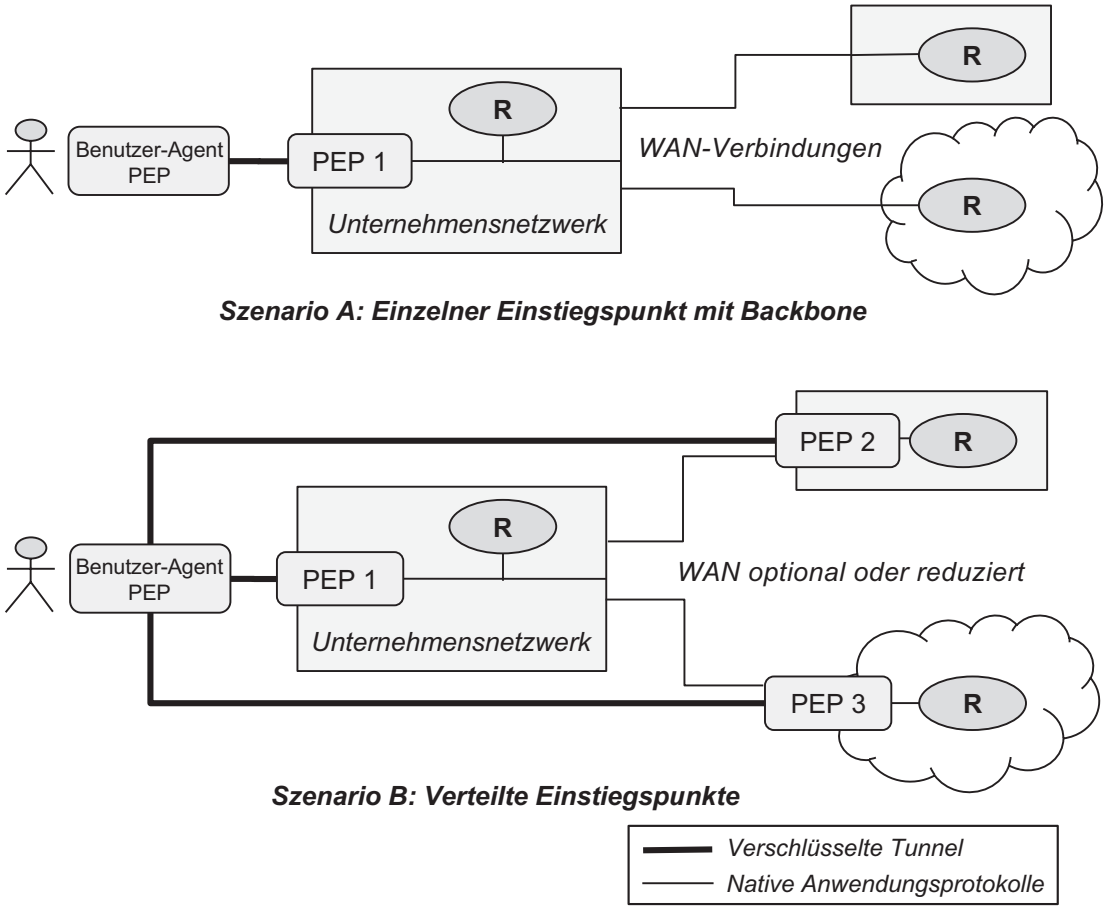

Abb. 10-2. *Zero Trust Netzwerkarchitekturen*

Architektur hinter unseren Zielen zurück. Es gibt auch zwei weitere Probleme mit diesem Ansatz.

Erstens verursacht das WAN selbst zusätzliche Netzwerklatenz, die im Wesentlichen eine Rückführung des gesamten Benutzerverkehrs zum PEP 1-Eingangspunkt erfordert. Und natürlich hat die WAN-Bandbreite Kosten für die Organisation. Zweitens kann dieser Ansatz einen Verlust an Genauigkeit in Bezug auf Richtlinien verursachen – PEP1 ist so „weit entfernt" von den Ressourcen an den Remote-Standorten, dass es schwierig für ihn ist, sehr effektiv in Bezug auf die Durchsetzung von feinkörnigen oder dynamischen Zugriffsrichtlinien zu sein.

Vergleichen wir dies mit Szenario B, das verteilte Zugangspunkte hat – Benutzer verbinden sich direkt mit ihren autorisierten PEPs. Dies beseitigt die Notwendigkeit, Benutzerverkehr zu PEP1 zurückzuführen, reduziert Latenz und WAN-Kosten. Organisationen können ihren WAN-Verbrauch erheblich reduzieren und ihn oft vollständig ersetzen, indem sie ihn durch einfache Internetverbindungen ersetzen. Dies hat auch den Vorteil, die vollständige Genauigkeit zu behalten – alle PEPs haben ihre volle Fähigkeit, feinkörnige, identitätszentrierte, dynamische Richtlinien gegen ihre lokalen Ressourcen durchzusetzen. Außerdem haben PEP 2 und PEP 3 als vollständige Zero Trust-Durchsetzungsknoten die Fähigkeit, API-Aufrufe zu tätigen und Attribute über ihre geschützten Umgebungen und Ressourcen zu entdecken.

Vergewissern Sie sich, dass tatsächliche Architekturen von dieser abweichen können – viele Anbieter unterstützen ein gemischtes oder hybrides Modell, und Ihr Unternehmen wird zweifellos einzigartige Aspekte haben. Wir ermutigen Sie, gute Fragen zu stellen und sicherzustellen, dass Sie die Zeit und Energie investieren, um Ihre aktuelle und geplante Netzwerk-Topologie aus den diskutierten Perspektiven zu verstehen.

Zusammenfassung

Zusammenfassend glauben wir, dass die Einführung von Zero Trust einen erheblichen Einfluss auf den NGFW-Markt haben wird und weiterhin seine Grenzen als zuvor gut definiertes und eigenständiges Segment verwischt. Genau wie der „Unternehmens-Firewall"-Markt gereift ist, so dass heute im Grunde jede Unternehmens-Firewall Funktionen hat, die zuvor als „Next-Gen" betrachtet wurden, sehen wir NGFW-Anbieter, die Zero Trust-Fähigkeiten hinzufügen.

Wir glauben, dass Unternehmen in Zukunft zunehmend Netzwerksicherheitslösungen einsetzen werden, die Zero Trust-Prinzipien umfassen, die per Definition eine breitere Perspektive und ein breiteres Richtlinienmodell erfordern. Dies ist eine gute Sache – Organisationen suchen konsequent nach der Bereitstellung weniger Lösungen, die einen breiteren Bereich abdecken; sie erkennen, dass isolierte Sicherheitslösungen dem Zero Trust-Ansatz widersprechen. Als Ergebnis sollten sie sicherstellen, dass ihre ausgewählten Sicherheitskomponenten reichhaltige APIs unterstützen und die Möglichkeit haben, leicht integriert zu werden (eines unserer erweiterten Zero Trust-Prinzipien).

In unseren Köpfen sind die Schlüsselentscheidungen über eine Zero Trust-Architektur die Quellen der Identität und des Kontexts, die dem PDP zur Verfügung stehen, und wie breit das Richtlinienmodell über PEPs angewendet werden kann, die über Unternehmensressourcen verteilt sind. Es gibt heute keine einzige kommerziell verfügbare Plattform mit einem Richtlinienmodell und einer Reihe von PEPs, die universell auf Ihre Benutzer, Infrastruktur und Anwendungsfälle angewendet werden können. Dies ist einer der Gründe, warum Zero Trust eine Reise ist.

Dies unterstreicht die Wichtigkeit einer klugen Wahl – sicherzustellen, dass Ihre ausgewählten Plattformen und Tools gut mit Ihren anfänglichen Anwendungsfällen übereinstimmen und dass sie die Fähigkeit haben, mit dem Rest Ihrer Umgebung und PEPs integriert zu werden. Sie könnten sich dafür entscheiden, die Plattform eines NGFW-Anbieters als zentralen Teil Ihrer Zero Trust-Architektur zu verwenden, und das könnte durchaus eine sinnvolle Entscheidung sein. Stellen Sie nur sicher, dass Sie sich der Grenzen (Grenzen) der Plattform bewusst sind, stellen Sie einige harte Fragen darüber, wie sie in Ihr breiteres Ökosystem integriert werden kann, und seien Sie sich über eventuelle architektonische Einschränkungen im Klaren. Sie werden PEPs haben, die außerhalb der Plattform des Anbieters liegen, aber dennoch integriert werden müssen. Stellen Sie sicher, dass Ihre ausgewählte Plattform dies effizient und effektiv in Ihrer Umgebung unterstützen wird.

KAPITEL 11

Sicherheitsoperationen

Viele Unternehmen haben in die Schaffung eines Security Operations Center (SOC) als physische oder virtuelle Organisation investiert, die eine Gruppe von fokussierten Menschen, Prozessen und Technologien zusammenstellt, um Bedrohungen, Schwachstellen und Incident Response zu adressieren. Dieses Kapitel untersucht zwei primäre Tools, die in SOCs verwendet werden—Security Information and Event Management (SIEM) und Security Orchestration, Automation, and Response (SOAR). Wir werden diese Tools aus der Perspektive von Zero Trust betrachten und untersuchen, wie sie zusammen die Effektivität und Effizienz des täglichen Betriebs im SOC verbessern können. Aber bevor wir diese Systeme zusammenbringen können, lassen Sie uns einige der Gründe diskutieren, warum SIEM und SOAR Tools existieren.

Moderne IT-Systeme erzeugen immense Mengen an Log-Daten, in wild unterschiedlichen Formaten, Standorten und Schemata. Diese Logs dienen mehreren Zwecken, wie z. B. periodischem IT-Zugriff für Fehlerbehebung oder Diagnose, laufender Anomalieerkennung und längerfristigen Archiven für forensische oder Audit-Zwecke. Diese Logs bieten nicht nur ein breites Bild der Infrastrukturelemente und ihrer Interaktionen, sondern ermöglichen es auch SOC-Analysten und Tools, Ereignisse im gesamten IT-Umfeld zu überprüfen und zu synthetisieren. SIEM-Tools haben sich entwickelt, um die großen Mengen und die breite Vielfalt der Log-Daten zu bewältigen, und sind zu einem unverzichtbaren Teil moderner SOCs geworden.

Natürlich machen Sicherheitsanalysten viel mehr als nur Logs zu untersuchen – sie verbringen viel Zeit und Mühe mit Incident Response und Event Management. Glücklicherweise bieten SOAR-Tools automatisierte (oder zumindest halbautomatisierte) Workflows, die schnell integriert werden können, um die notwendigen Incident Response-Anforderungen über die Breite der Tools im SOC zu unterstützen. Da SOC-Operationen für das Sicherheitsprogramm einer Organisation von zentraler Bedeutung sind, werden die wachsenden Fähigkeiten von SOAR-Tools dazu beitragen, wie SOC-Teams die immense Menge an Daten und die Anzahl der Sicherheitsereignisse nutzen, um effektiver zu werden.

J. Garbis und J. W. Chapman, *Zero Trust Sicherheit*, https://doi.org/10.1007/979-8-8688-0105-1_11

In der Praxis werden SIEMs und SOARs zunehmend zu zwei untrennbaren Teilen eines SOC. Der Wert von SIEMs und SOARs wird in der Tat nur weiter wachsen, wenn Organisationen Zero Trust-Architekturen übernehmen, und in diesem Kapitel erklären wir, wie und warum diese Tools davon profitieren, gut in eine Zero Trust-Architektur integriert zu sein, da der Identitätskontext im gesamten Sicherheitsökosystem immer häufiger wird.

Sicherheitsinformationen und Ereignismanagement

SIEM Tools bieten Mechanismen zum Sammeln, Aggregieren und Normalisieren von Log-Daten zur Erkennung und Bewertung von Sicherheitsereignissen innerhalb einer Organisation. IT-Organisationen nutzen seit Jahrzehnten Logs und aggregieren Log-Management-Systeme, und der sicherheitsspezifische Markt, den wir heute als SIEM bezeichnen, entstand um 2005. SIEM-Anbieter innovierten über das grundlegende Log-Management hinaus und entwickelten eine Reihe von sicherheitsfokussierten Fähigkeiten zur Vereinheitlichung, Normalisierung, Aggregation, Korrelation und Analyse von Log-Daten, um sie in Sicherheitsinformationen und (idealerweise) handlungsrelevante Ereignisse umzuwandeln. Diese Log-Daten werden typischerweise nicht nur von der IT-Infrastruktur (Server, Firewalls, etc.) sondern auch von Sicherheitssystemen wie IDS/IPS, Endpoint-Management, Authentifizierungssystemen und anderen aufgenommen.[1]

Diese Arten von Unternehmenssystemen und Netzwerken erzeugen große Mengen an Log-Daten, die oft überwältigend für Analysten sind. SIEMs helfen dabei, dies zu sortieren und bieten Analysen, Filter, Visualisierungen und andere Tools, zum Beispiel, um die Anzahl der Falschmeldungen zu reduzieren.

Historisch gesehen wurden SIEM-Anbieter in einem On-Premises-Modell eingesetzt, haben sich aber in letzter Zeit in Richtung eines Cloud-basierten Modells verschoben. Es gibt Vor- und Nachteile der beiden SIEM-Bereitstellungsmodelle

[1]Wir haben einige der Systeme erwähnt, die Daten an das SIEM liefern; andere sind Antiviren-Systeme, Endpoint Detection and Response, User and Entity Behavior Analytics (UEBA), Mobile Device Management (MDM) und Unified Endpoint Management (UEM). Kurz gesagt, jedes Unternehmens-IT-System-Log kann in ein SIEM eingespeist werden.

(On-Prem vs. Cloud), aber aus einer Zero Trust-Perspektive sind diese Unterschiede weitgehend irrelevant – die Integrationsszenarien, Anforderungen und Vorteile, die wir später diskutieren, sind identisch. Das heißt, unabhängig von Ihrem SIEM-Standort können Sie einen erheblichen Wert erzielen, indem Sie es in Ihre Zero Trust-Architektur integrieren.

Neben der Aggregation von Logs können SIEMs helfen, die Netzwerkinfrastruktur einer Organisation zu kartieren, indem sie diese Rohdaten synthetisieren. Dies kann Sicherheits- und IT-Teams zugute kommen, da es nützlichen Kontext darüber liefert, wo Ereignisse in einem Netzwerk stattfinden. Dies ist interessant, weil es anfängt, Informationen über hochwertige (oder zumindest stark genutzte) Vermögenswerte in der Organisation zu liefern, die den Organisationen helfen können, ihre Zero Trust-Strategie und -Architektur besser zu definieren und zu planen, zum Beispiel durch Beeinflussung von Richtliniendefinitionen oder Bereitstellungsorten für PEPs.

SIEMs haben sich als sehr nützlich erwiesen, indem sie Daten aggregieren und bei der Entscheidungsfindung für Sicherheitsanalysten helfen, und eine natürliche Erweiterung für diese Plattformen war es, strukturierte und ereignisgesteuerte Wege zur Automatisierung von Antworten und Aktionen auf erkannte Ereignisse zu bieten. Diese Fähigkeiten haben sich zu einem Angebotssatz zusammengefasst, den wir als SOAR bezeichnen.

Sicherheitsorchestrierung, Automatisierung und Reaktion

SOARs werden oft in Verbindung mit SIEMs verwendet; tatsächlich werden sie manchmal vom selben Anbieter als Teil einer integrierten Plattform bereitgestellt. Ein SOAR wird Informationen (und erkannte Ereignisse oder Schwellenwertwarnungen) von einem SIEM aufnehmen und ein Modell und einen Mechanismus zur Automatisierung einer Reihe von Reaktionsaktionen bereitstellen, oft geleitet durch maschinelles Lernen.

Dies ist hilfreich, denn während SOARs die große Anzahl von Ereignissen, die von einem SIEM ausgegeben werden, durchsieben, bieten sie einen gemeinsamen Kontext für Ereignisse und automatisieren letztendlich Prozesse oder Workflows als Reaktion auf das Ereignis. Diese integrierte Automatisierung hilft, die Anzahl der Falschmeldungen in einer Umgebung zu reduzieren, so dass echte Vorfälle von Sicherheitsingenieuren überprüft werden können.

Der Wert eines SOAR liegt nicht nur in der Automatisierung, sondern auch in der Modellierung der logischen Analyse- und Reaktionsabläufe. Diese Workflows enthalten Informationen über Unternehmensnetzwerke, Systeme, Abhängigkeiten und wie man mit ihnen arbeitet – was allzu oft nur „Stammeswissen" ist, das ausschließlich in den Köpfen von Senior-Analysten existiert. Mit einem SOAR kann dieses Wissen in eine automatisierte, wiederholbare und zuverlässige Plattform eingebaut werden, die nie einen Arbeitstag frei nehmen muss. Dieses kodifizierte Wissen kann (und sollte) ein SOC in eine nahtlose Integration von Menschen, Prozessen und Technologie verwandeln. Aus einer Zero Trust-Perspektive erfordert das Erreichen dieser Prinzipien mehr als eigenständige Technologien – es erfordert Integration und Koordination sowie „Reichweite", um Veränderungen in der gesamten Unternehmenssicherheitsinfrastruktur zu bewirken – etwas, das ein SOAR gut erreichen kann, wenn es mit einer Zero Trust-Plattform verbunden ist. Insbesondere helfen SOARs SOCs, ihre Mission zu erfüllen, indem sie die Automatisierung von wiederholbaren, vorhersehbaren Prozessen ermöglichen. Die meisten SOARs erkennen Entscheidungsmuster und helfen bei der Verwaltung des gesamten Incident Response-Lebenszyklus, während sie auch aktiv Bedrohungsintelligenz sammeln und auf Daten reagieren und Kontext dazu liefern. Darüber hinaus sind Vulnerability Management[2] und Threat Intelligence Kernverantwortlichkeiten in einem SOC – mit dem SOAR, der einen guten Workflow und Incident Response-Muster zur Unterstützung dieser bietet, und deren Ergebnisse tragen zum kontinuierlichen Wachstum und Lernen der SOAR-Lösung bei.

Die Analyse und Aktionen, die SIEM und SOAR bieten, sind sehr wichtige Komponenten eines effektiven Zero Trust-Systems – als zusätzlicher Kontext für und Katalysatoren für Entscheidungen, die vom PDP getroffen werden sollen, was wir im nächsten Abschnitt weiter untersuchen werden.

Zero Trust im Security Operations Center

SIEMs und SOARs werden weiterhin Schlüsselkomponenten der Unternehmenssicherheit sein, und tatsächlich wird ihr Wert und ihre Bedeutung zunehmen, wenn Organisationen Zero Trust übernehmen. Das heißt, wenn

[2]Vulnerability Management wird auf viele Arten interpretiert, aber letztendlich geht es darum, sicherzustellen, dass Ihr Netzwerk und Ihre Geräte durch geeignete Techniken gesichert sind und Sichtbarkeit in den Status dieser Geräte bieten.

Unternehmen auf ihrem Weg zu Zero Trust voranschreiten, sollten sie eine verbesserte Breite, Tiefe und allgemeine Wirksamkeit ihrer SIEM/SOAR erwarten (und fordern). Darüber hinaus wird das automatisierte Lernen, das durch eine Zero Trust-integrierte SOAR erreicht wird, nur die Entscheidungen, die von der PDP zur Unterstützung der gesamten Umgebung getroffen werden, verbessern. Lassen Sie uns nun die Wege erkunden, wie dies geschieht.

Bereicherte Log-Daten

Eine der Schlüsselfunktionen von SIEMs ist ihre Fähigkeit, Daten aus isolierten Systemen zu korrelieren – wie die Zuweisung einer dynamischen IP-Adresse an einen Benutzer und Netzwerkaktivitäten, die später von dieser IP-Adresse ausgeführt werden. Allerdings sind SIEMs auf den Datensatz beschränkt, der von ihren Quellsystemen bereitgestellt wird, und werden oft durch zugrunde liegende technische Einschränkungen und isolierte Infrastrukturelemente behindert. Zum Beispiel durchläuft der Netzwerkzugriff oft Netzwerkgrenzen, an denen Network Address Translation (NAT) stattfindet, was es schwierig oder unmöglich machen kann, Aktionen auf einer IP-Adresse einem bestimmten Benutzer zuzuordnen. Auch werden in vielen Fällen Logs von Systemen generiert, die isolierte oder getrennte Identitätsverwaltungssysteme nutzen, was es für SIEMs und Sicherheitsanalysten schwierig macht, Benutzer-IDs über verschiedene Log-Quellen hinweg zu konsolidieren oder zu entwirren.

Zero Trust-Systeme beseitigen nicht nur viele dieser technischen Einschränkungen, sie erhöhen auch erheblich die Reichhaltigkeit der von SIEMs aufgenommenen Daten und erhöhen daher ihre Fähigkeit, sicherheitsrelevante Ereignisse zu korrelieren und zu erkennen. Insbesondere – weil es grundsätzlich identitätszentriert ist, wird ein Zero Trust-System in der Lage sein, detaillierte identitätsbereicherte Daten in ein SIEM zu loggen. Diese bereicherten Log-Daten werden für das SIEM und für SOC-Ingenieure aussagekräftiger sein und ihre Fähigkeit zur effektiven Reaktion verbessern. Anders ausgedrückt – ein Zero Trust-System sollte in der Lage sein, alle Netzwerkzugriffe aller Benutzer zu protokollieren und diese Log-Daten mit Informationen über ihre Identität, Geräte und den allgemeinen Kontext zu bereichern. Dies sollte unabhängig davon gelten, wo sich ein Benutzer befindet, wie viele Zwischennetzwerkgrenzen überschritten werden, welches Netzwerkprotokoll verwendet wird oder wie ein bestimmtes Anwendungssystem einen bestimmten Benutzer bezeichnet.

Orchestrierung und Automatisierung (Trigger und Ereignisse)

Enterprise Zero Trust-Systeme erfordern einen hohen Grad an Automatisierung und müssen in der Lage sein, verschiedene Trigger und Ereignisse im großen Maßstab zu erkennen und darauf zu reagieren. Wie wir im Laufe der Diskussion festgestellt haben, ist der *dynamische* Aspekt des Zero Trust-Policy-Modells ein bedeutender Beitrag zu seinem Wert. SOAR-Systeme, weil sie einen breiteren Anwendungsbereich als Zero Trust haben, können die Wirksamkeit eines Zero Trust-Systems verbessern und erhöhen. Tatsächlich wird die Kombination von SOAR und Zero Trust durch eine Reihe von koordinierten Ereignissen, orchestrierten API-Aufrufen und Triggern beiden Systemen zugute kommen.

Die Details, welche Komponente welche Funktion ausführt, hängen von Ihrer spezifischen Architektur und Plattformen ab, aber im Allgemeinen werden Workflows, die zwischen einem PDP und einem SOC-Sicherheitsanalysten koordiniert sind, Echtzeit-Entscheidungen und Aktionen informieren und ausführen. Wir werden in den folgenden Abschnitten einige Beispiele untersuchen. Natürlich erfordert diese Integration eine Reihe von bidirektionalen APIs,[3] , um Aktionen wie den Austausch aktualisierter Daten, das Auslösen einer Policy-Evaluierungsaktualisierung oder das programmgesteuerte Erstellen neuer Policies oder virtueller Infrastrukturkomponenten durchzuführen.

Wir werden diese später in Kap. 17 ausführlicher behandeln, aber wir wollten hier einen Überblick geben, da es für diese Diskussion relevant ist. Aus der Perspektive eines Zero Trust-Systems gibt es vier Haupttypen von Triggern, die natürliche Wege sind, um mit externen Systemen wie SIEMs und SOARs zu interagieren. Drei davon werden vom Zero Trust-System initiiert, der vierte von einem externen System.

[3]Streng genommen könnte diese Integration über APIs, Messaging, das Einlesen von Konfigurationsdateien wie YAML oder andere Mittel erfolgen. Sie können auch synchron oder asynchron sein. Gute Zero Trust- und SOAR-Plattformen unterstützen mehrere Integrationsmittel. Wir stellen diese Integrationen hier als synchrone API-Aufrufe dar, um die Einfachheit zu wahren, aber bewerten Sie die spezifischen Fähigkeiten Ihrer Plattformen und wählen Sie den am besten geeigneten Mechanismus für den vorliegenden Anwendungsfall.

Authentifizierungs-Trigger

Für Benutzer tritt dies in der Regel nur einmal oder ein paar Mal pro Tag auf. Für Dienste (nicht-personenbezogene Einheiten) kann dies viel seltener sein. Dieser Trigger initiiert natürlich eine Policy-Evaluierung durch die PDP und ist ein natürlicher Zeitpunkt für die PDP, Anfragen an ein SIEM/SOAR zu stellen, um zusätzlichen Benutzer- oder Umgebungskontext zu erhalten.

Ressourcenzugriffs-Trigger

Identitäten greifen natürlich viele, viele Male im Laufe eines jeden Tages über einen PEP auf Ressourcen zu. Es ist oft angebracht, dass ein PEP gelegentlich Anrufe an ein SIEM/SOAR macht, um aktuelle Kontextinformationen zu erhalten, insbesondere für Attribute, die sich seit der Authentifizierung geändert haben könnten, wie das Geräterisikoniveau auf der Grundlage beobachteter Aktivitäten. PEPs sollten nicht bei jedem Zugriff Dinge neu bewerten, also schauen Sie, wie Ihr Zero Trust-System diesen Trigger modelliert.

Periodischer (Sitzungsablauf) Trigger

Viele Zero Trust-Systeme haben ein Konzept einer Identitätssitzung, die natürlich eine begrenzte Lebensdauer hat (wie mehrere Stunden). Bei Ablauf der Sitzung führen Zero Trust-Systeme oft eine Aktualisierung der zugewiesenen Richtlinien der Identität durch, und dies ist auch ein natürlicher Zeitpunkt für die PDP, Anrufe an das SIEM/SOAR zu tätigen, ähnlich wie zur Authentifizierungszeit, um zusätzlichen Kontext zu erhalten.

Externer Trigger

Schließlich unterstützen viele Zero Trust-Systeme eingehende APIs, mit denen externe Komponenten Ereignisse auslösen und Kontextinformationen aktualisieren können.

Natürlich muss Ihr SIEM/SOAR eine entsprechende Reihe von sowohl eingehenden als auch ausgehenden APIs unterstützen, um den maximalen Nutzen aus einem Zero Trust-System zu ziehen. Wenn Sie Zero Trust-Systeme evaluieren, suchen Sie nach einem, das eine reiche Reihe von Aktionen bietet, um eine Vielzahl von Integrationen zu unterstützen. Lassen Sie uns in drei Beispiele für Integrationen zwischen Zero Trust und SIEM/SOAR eintauchen, um dies zu konkretisieren.

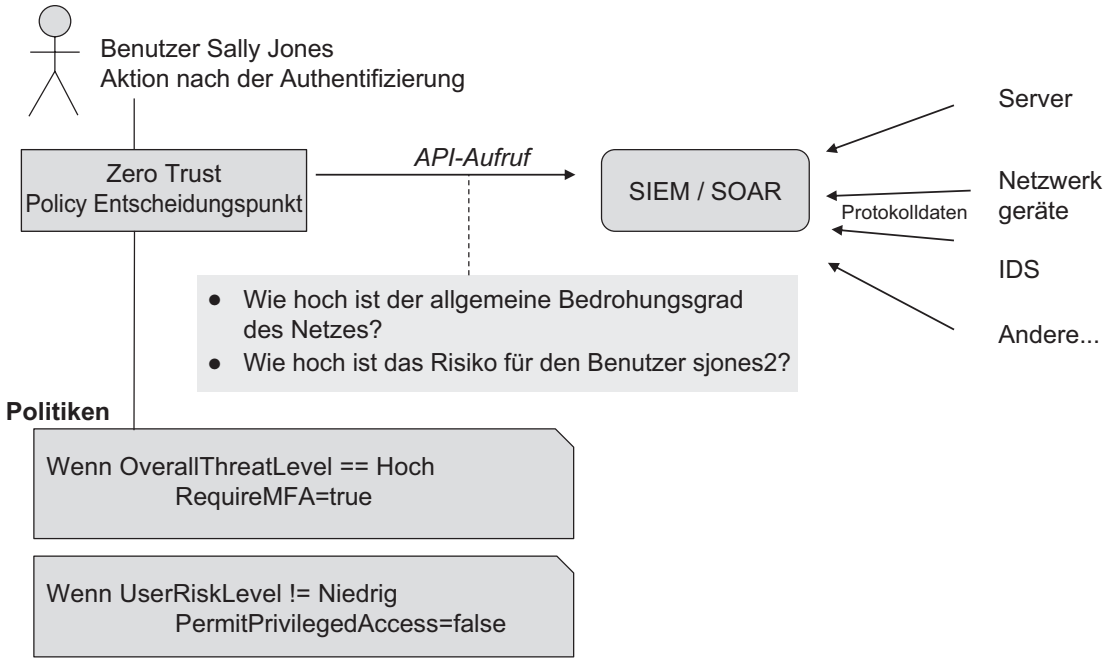

Abb. 11-1. *Zero Trust-System trifft Entscheidung basierend auf SIEM/SOAR*

Zero Trust Abfragen für zusätzlichen Kontext (Authentifizierungsauslöser)

In unserem ersten Szenario führt ein Zero Trust-System API-Aufrufe in ein SIEM[4] aus, wie in Abb. 11-1 dargestellt, zum Zeitpunkt der Benutzerauthentifizierung. Diese Integration soll dem PDP zusätzliche Informationen für eine bessere Entscheidungsfindung liefern.

In diesem Beispiel geht das Zero Trust-System den unmittelbaren nächsten Schritt, nachdem Sally erfolgreich authentifiziert wurde, und übernimmt daher seine Rolle als PDP – es bewertet Richtlinien und trifft Entscheidungen darüber, auf welche Ressourcen Sally zu diesem Zeitpunkt zugreifen darf, basierend auf relevanten

[4]Beachten Sie, dass dies sich von den Basiskapazitäten unterscheidet, Zero Trust-Protokolldaten in das SIEM einzuspeisen, über die wir zuvor gesprochen haben.

Kontextinformationen. In unserem Beispiel verwendet das Zero Trust-System zwei Attribute, die es über den API-Aufruf vom SIEM-System erhält – das allgemeine Bedrohungsniveau im Netzwerk und das mit Sally verbundene Risikoniveau.

Die gezeigten Richtlinien bewerten diese Attribute und verwenden sie innerhalb der Durchsetzungsmittel des Zero Trust-Systems. Die erste Richtlinie erfordert MFA, wenn das SIEM angegeben hat, dass das allgemeine Netzwerkbedrohungsniveau hoch ist. Die zweite Richtlinie verhindert den Zugriff auf als privilegiert eingestufte Ressourcen, wenn der betreffende Benutzer nicht als aktuell niedriges Risikoniveau gekennzeichnet ist – möglicherweise basierend auf der Gerätehaltung oder dem beobachteten Netzwerkverhalten.

Das vorherige Beispiel zeigt das PDP, das das SIEM/SOAR als Reaktion auf den Authentifizierungsauslöser abfragt. Das Zero Trust-System wird auch davon profitieren, eine ähnliche Abfrage basierend auf dem Sitzungsablaufauslöser sowie dem Ressourcenzugriffsauslöser durchführen zu können. Betrachten wir nun einen API-Aufruf in die entgegengesetzte Richtung.

SIEM/SOAR ruft Zero Trust-System auf (externer Auslöser)

Dieses Beispiel zeigt, wie ein SOAR-System einen API-Aufruf durchführt, um einen Prozess mit dem PDP zu initiieren. Diese Aktion wird durch die Durchführung einer Analyse durch das SOAR-System ausgelöst und die Feststellung, dass etwas in einem Server, auf dem Gerät eines Benutzers oder im Netzwerk nicht stimmt und daher eine Reaktion erforderlich ist.[5] Wie in Abb. 11-2 gezeigt, kann dieser Aufruf Informationen enthalten, die spezifisch für einen einzelnen Benutzer sind oder breiter gelten (wie das allgemeine Bedrohungsniveau für das Netzwerk).

In diesem Szenario muss das Zero Trust-System natürlich in der Lage sein, angemessen auf den API-Aufruf vom SOAR zu reagieren, basierend auf Richtlinien. Zum Beispiel könnte das Zero Trust-System angesichts einer Beobachtung von anomalem Verhalten auf Sallys Gerät Maßnahmen ergreifen, die einschließen

[5]Dies kann durch einen SIEM-Analysten im Security Operations Center ausgelöst werden oder die automatisierte Antwort eines SOAR sein.

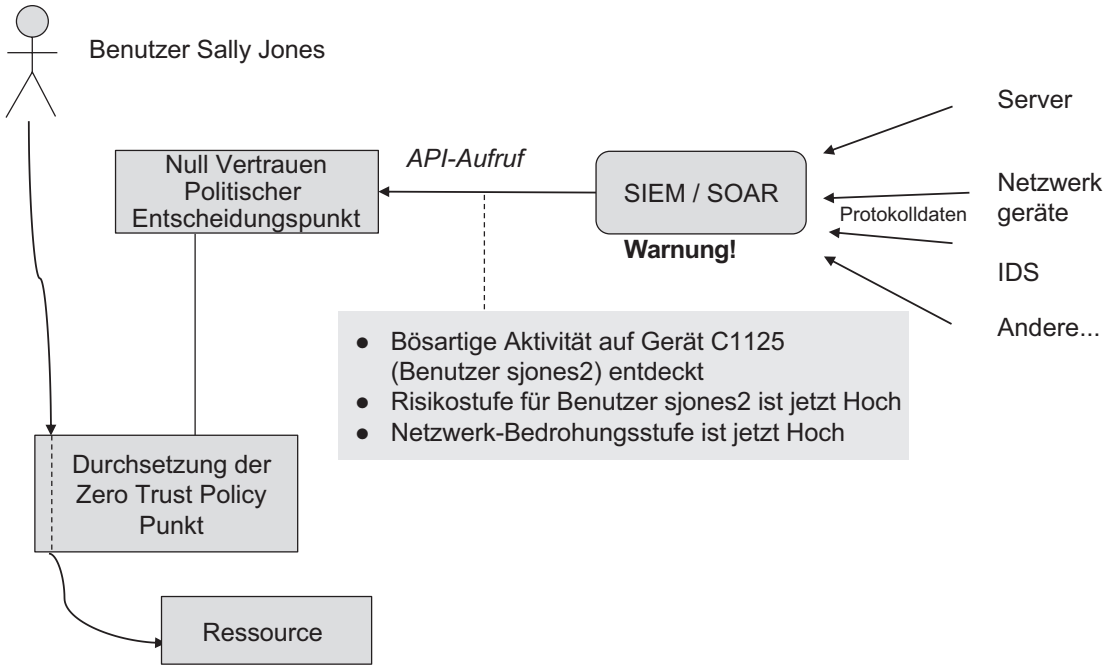

Abb. 11-2. *SOAR initiiert Workflow/Antwort*

- Aufforderung an Sally, sich auf diesem Gerät erneut zu authentifizieren[6]
- Aufforderung an Sally zu einer Art von MFA
- Sofortige Einschränkung des Zugriffs von Sallys Gerät, etwa durch Quarantäne im Netzwerk
- Warnung an Sally

[6]Sicherheitsteams sollten einige Überlegungen zu ihrem Bedrohungsmodell und der gewünschten Benutzererfahrung anstellen, wenn sie diese Antworten entwerfen. Wenn die Prämisse ist, dass auf Sallys Gerät aktiv Malware läuft, ist es vernünftig anzunehmen, dass sie Tastenanschläge und Bildschirmaufnahmen aufzeichnet. Daher könnte die Aufforderung an Sally, ihre Anmeldeinformationen oder eine OTP auf diesem infizierten Gerät einzugeben, eine schlechte Wahl sein, die die Sicherheit weiter gefährden kann. Viel besser wäre es, auf einem separaten Gerät (z. B. Smartphone) nach MFA zu fragen oder das Gerät einfach zu isolieren. Die Schwere der Reaktion muss von der Sicherheit in der bösartigen Aktivität und der Erfahrung des Teams mit Falschpositiven von ihrem SIEM und SOC abhängen.

Indirekte Integration (Externer Auslöser)

Eine letzte Anmerkung zur Interaktion zwischen dem SIEM und dem Zero Trust-System. Das vorherige Beispiel, obwohl einfach in seiner Interaktion, ist tatsächlich komplex hinter den Kulissen – es erfordert, dass das SIEM/SOAR so konfiguriert ist, dass es weiß, welche Daten das Zero Trust zur Auswertung seiner Richtlinien benötigt. Dies fügt Komplexität und betrieblichen Overhead zum System hinzu, da nun eine bidirektionale Abhängigkeit von Daten zwischen diesen beiden Systemen besteht. Wenn eine Richtlinie im Zero Trust-System so konfiguriert ist, dass sie ein neues Attribut aus dem SIEM/SOAR verwendet, muss nun auch das SIEM/SOAR geändert werden, um dieses Attribut in seinen API-Aufrufen in das Zero Trust-System einzuschließen. Dies erfordert koordinierte Änderungen auf beiden Seiten und fügt Komplexität hinzu. Eine alternative und einfachere Herangehensweise besteht darin, dass das Zero Trust-System das SIEM/SOAR nach den benötigten Daten fragt. Auf diese Weise erfordern Änderungen an einer Zero Trust-Richtlinie keine Änderungen am SIEM – solange es die gefragten Daten enthält, kann es diese bereitstellen. Dieses Modell ist in Abb. 11-3 dargestellt.

In diesem Diagramm – zur Vereinfachung als Schwimmbahn dargestellt – hat Sally sich bereits authentifiziert und wurde autorisiert, auf eine sensible Arbeitslast zuzugreifen. Dann bemerkt das SOAR-System eine anomale Aktivität, die mit Sally oder

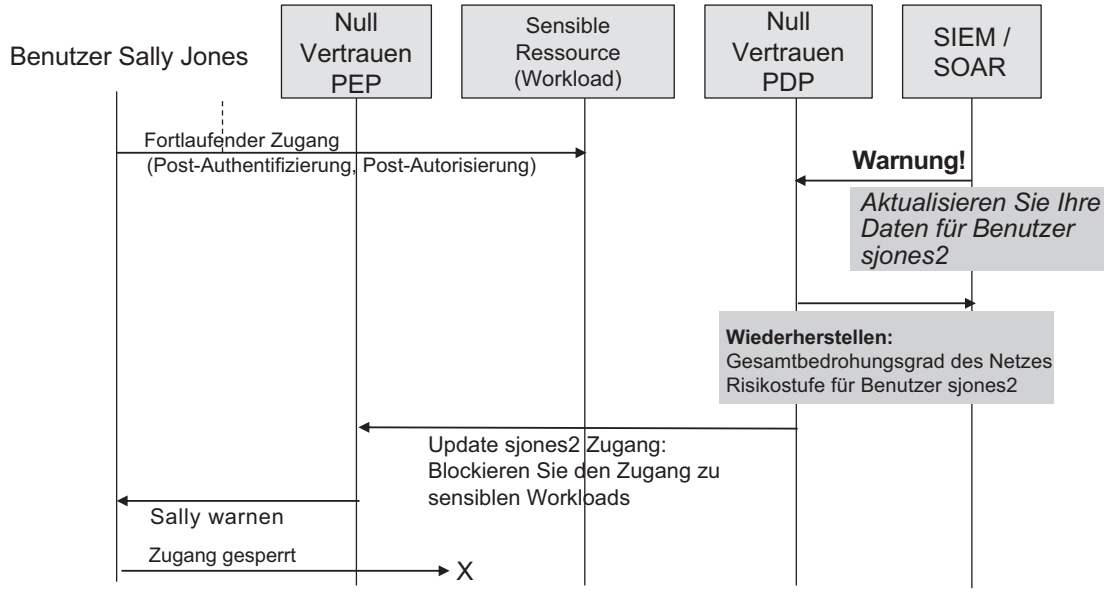

Abb. 11-3. *Schwimmbahn von SOAR und PEP Interaktion*

ihrem Gerät in Verbindung steht, und macht einen einfachen API-Aufruf in das Zero Trust PDP und teilt ihm mit, dass sich etwas geändert hat und dass das Zero Trust-System seine Informationen für Sally (Benutzer sjones2) aktualisieren muss. Basierend auf diesem API-Aufruf reagiert das Zero Trust-System dann – wahrscheinlich durch erneute Bewertung des gesamten Richtliniensatzes für Sally, einschließlich der Aktualisierung von Informationen über sie aus mehreren Systemen, einschließlich des SOAR. Beachten Sie, dass es das Zero Trust-System ist, nicht das SOAR, das entscheidet, welche Informationen es benötigt – das bedeutet, dass das SOAR nicht wissen muss, welche Datenelemente das PDP benötigt, um seine Richtlinien zu bewerten. Basierend auf diesen aktualisierten Informationen trifft das PDP die Entscheidung, dass Sally keinen Zugang mehr zu der sensiblen Ressource haben sollte, und informiert das PEP über diese Änderung. In unserem Beispiel hat das Sicherheitsteam auch beschlossen, Sally zu warnen, vielleicht über eine Pop-up-Nachricht oder eine SMS.

Zusammenfassung

SIEM- und SOAR-Tools sind unverzichtbare Elemente moderner SOCs geworden und bieten Sicherheitsanalysten unschätzbare Analyse-, Visualisierungs- und Reaktionsfähigkeiten. In einer Zero Trust-Architektur können (und sollten) das SIEM oder SOAR eine entscheidende Rolle dabei spielen, Lösungen für eine sofortige und nahezu Echtzeit-Analyse und Reaktion zusammenzubringen. Die hier diskutierten Integrationsszenarien veranschaulichen, wie diese Systeme zu unterschiedlichen Zeiten, basierend auf unterschiedlichen Auslösern, zusammengebracht werden können, um die Sicherheit und die Effizienz und Wirksamkeit der Reaktion zu verbessern. Diese Beispiele sind bei weitem nicht erschöpfend – es gibt viele andere Möglichkeiten, wie Zero Trust-Systeme und SIEM/SOAR integriert werden können, um wertvolle und interessante Funktionen auszuführen. Schauen Sie sich an, wie Ihr SOC-Team mit den vorhandenen Tools arbeitet, und informieren Sie sie über die Art von Identitäts- und Kontext-angereicherten Daten, die Ihr Zero Trust-System in ihre Plattformen einspeisen kann. Es ist sehr wahrscheinlich, dass Sie gemeinsam eine Vielzahl von Möglichkeiten finden, wie diese Integrationen Ihrer Organisation helfen können. Und das Einbeziehen des SOC-Teams kann nur dazu beitragen, Ihre Zero Trust-Reise zu beschleunigen.

KAPITEL 12

Privilegiertes Zugriffsmanagement

Privileged Access Management (PAM) ist ein Sektor der IT-Sicherheitsindustrie, mit Anbieterangeboten, die steuern, verwalten und berichten, wie privilegierte Benutzer (Systemadministratoren) auf Systeme oder Ressourcen zugreifen, über eine Reihe von Sicherheitsfunktionen und -prozessen. PAM kann verwendet werden, um den Zugriff auf *jedes* System zu kontrollieren, wird aber in der Regel nur auf hochwertige Ressourcen wie Domänencontroller und Produktionsserver angewendet. Zero Trust-Sicherheit basiert natürlich auf der Prämisse, dass sie zum Schutz *aller* Systeme verwendet werden sollte, aber hochwertige Systeme – diejenigen, die typischerweise auch durch PAM geschützt sind – sind gute Kandidaten für erste Zero Trust-Projekte oder -Bereiche.

PAM-Lösungen haben sich weiterentwickelt und erweitert, da der Markt gereift ist und bieten heute Funktionen, die sich auf Passwort-Tresore, Geheimnisteilung und Sitzungsmanagement konzentrieren. Obwohl PAM typischerweise Benutzer mit Unternehmensidentitätsanbietern authentifiziert und oft Gruppenmitgliedschaften zur Zugriffskontrolle verwendet, glauben wir, dass es sinnvoll ist, diese Lösungen als identitätsbewusst und nicht als identitätszentriert zu kategorisieren. Diese Unterscheidung ist notwendig zu verstehen, weil eine PAM-Lösung in gewisser Weise wie ein Zero Trust-System aussehen kann und sogar einige PEP-ähnliche Fähigkeiten bieten kann, aber nicht als eigenständige Zero Trust-Lösung betrachtet werden kann. Wir werden zu diesem Thema am Ende dieses Kapitels zurückkehren, aber zuerst werfen wir einen Blick auf die drei Kernfunktionen, die typischerweise von PAM bereitgestellt werden.

J. Garbis und J. W. Chapman, *Zero Trust Sicherheit*, https://doi.org/10.1007/979-8-8688-0105-1_12

Passwort-Tresore

PAM-Lösungen begannen mit dem einfachen Konzept eines *Passwort-Tresors* – anstatt sich darauf zu verlassen, dass Admin-Benutzer individuell Passwörter für privilegierte Konten pflegen, werden diese Anmeldeinformationen stattdessen in einem sicheren Repository gespeichert. Der Tresor bietet sichere Speicherung und Zugriffsmanagement für Passwörter und automatisiert auch ihren Lebenszyklus, einschließlich Ablauf und Rotation. Diese Systeme implementieren die erforderlichen Geschäftsprozesse, einschließlich Zugriffsanforderungs- und Genehmigungsprozesse zum „Auschecken" von Passwörtern zur Verwendung (historisch gesehen fungierten Passwort-Tresore wie eine Bibliothek für Passwörter, und Benutzer „checkten" Passwörter auf die gleiche Weise aus, wie Kunden ein Buch aus einer Bibliothek ausleihen). In der Praxis sind Anmeldeinformationen heute tatsächlich oft flüchtig und werden in der Regel nach Ablauf der festgelegten Frist rotiert. Manchmal sehen die Benutzer das Passwort nie; sie werden automatisch authentifiziert, wobei das PAM-System sie im Hintergrund in das Zielsystem einloggt.

Heute hat sich das Passwort-Tresor von einem einfachen Prozess zur Speicherung von Passwörtern für privilegierte Konten zu einem Prozess entwickelt, der Passwörter über APIs zur Unterstützung von Dienstkonten sowie Passwortmanagement für diese Konten bereitstellt. Diese API-Fähigkeiten helfen Anwendungen, Skripten und Dienstkonten, Passwörter nicht im Klartext zu speichern oder an Orten, die anfällig für Kompromisse sind.

Im Kontext von PAM ist das Passwort-Tresor wertvoll, weil es ein Mittel zur Erreichung mehrerer Ziele ist. Erstens bietet es ein Modell mit minimalen Privilegien für den Zugriff auf Anmeldeinformationen, was offensichtlich eine Komponente von Zero Trust-Umgebungen ist. Zweitens hilft es, Geschäftsprozesse zur Erlangung des Zugriffs auf sensible Ressourcen durchzusetzen. Zuletzt stellt es sicher, dass der Zugriff auf privilegierte Systeme protokolliert und prüfbar ist, was in vielen regulierten Umgebungen wichtig ist.

Geheimnisverwaltung

Im Laufe der Zeit haben PAM-Lösungen sich von der Speicherung und Verwaltung relativ einfacher Benutzerpasswörter zu einer breiteren Palette von *Geheimnisverwaltung* Fähigkeiten erweitert. Geheimnisse beschränken sich nicht auf

Passwörter, sie können jede Art von Informationen umfassen, die notwendig sind, um Systeme direkt oder indirekt zu sichern. Die folgenden sind Beispiele für Elemente, die neben Passwörtern in einer Geheimnisteilungslösung gespeichert werden können:

- Hashes
- Zertifikate
- Cloud-Mieterinformationen
- API-Schlüssel
- Datenbankspeicherinformationen
- Persönliche Informationen
- SSH-Verbindungsinformationen

Was diese alle gemeinsam haben, ist die Notwendigkeit, diese sensiblen Informationen auf eine Weise zu speichern, die nur für authentifizierte und autorisierte Identitäten zugänglich ist und ihre Datenintegrität (d. h., sie können nicht manipuliert werden) aufrechterhält. Geheimnisverwaltungssysteme müssen sowohl den Benutzer- als auch den Systemzugriff auf eine Weise unterstützen, die sicher und prüfbar ist.

Neben den technischen Vorteilen der Geheimnisverwaltung gibt es auch einige geschäfts- und prozessorientierte Vorteile – insbesondere die Workflows und Prozesse, die eingerichtet werden, um diese Geheimnisse sowohl zu speichern als auch zu erhalten. Die einfache Tatsache, dass es einen (kontrollierten) Ort und sichere Speicherung gibt, bietet Organisationen die Möglichkeit, sicherzustellen, dass sie die ad-hoc-Speicherung von Anmeldeinformationen vermeiden, wodurch das Risiko verringert wird, dass sie gestohlen oder verloren gehen.

Und als letzte Anmerkung, wie bereits erwähnt, können nicht-personenbezogene Entitäten, die über API-Mechanismen auf den Geheimnisverwaltungsort zugreifen, zur Automatisierung der Abholung von Geheimnissen in einer Anwendung oder einem Server während des Bootstrapping dieser Umgebung verwendet werden.

Verwaltung privilegierter Sitzungen

Verwaltung privilegierter Sitzungen (PSM) ist einer der wichtigsten Aspekte von PAM – insbesondere da es normalerweise kein nativer Teil einer Zero Trust-Lösung ist. Oft sind Compliance-Anforderungen und Audit-Probleme die Treiber, die Organisationen dazu

veranlassen, ein Budget für eine PSM-Lösung bereitzustellen und diese einzusetzen, anstatt einen strengen Sicherheitstreiber. PSM-Lösungen fungieren im Wesentlichen als Vermittler oder Proxy für den Systemadministratorzugriff auf Zielsysteme und bieten einen Mechanismus zur Überwachung, Aufzeichnung und Einschränkung des Admin-Zugriffs über Protokolle wie Remote Desktop Protocol (RDP) und Secure Shell (SSH) Zugriff.

PSM-Lösungen bieten in der Regel zwei Hauptfunktionen für Unternehmen. Erstens können sie eine Protokollierung oder Aufzeichnung von Admin-Zugriffen bereitstellen, um sicherzustellen, dass alle solche Aktivitäten für Audit-, Compliance- und forensische Zwecke protokolliert werden. Zweitens können sie auch einen „überwachten" Admin-Zugriff bereitstellen, bei dem eine zweite Person die Sitzung eines Admins in Echtzeit einsehen kann, um eine Aufsicht über risikoreiche Aktivitäten zu gewährleisten.

PSM wird auch oft verwendet, um rollenbasierten Zugriff auf einem privilegierten System durchzusetzen, indem Benutzern nur die für notwendige Aufgaben erforderlichen Berechtigungen gewährt werden. Dies kann in Form von eingeschränkten Berechtigungen für das Admin-Konto erfolgen, aber auch durch das tatsächliche Blockieren bestimmter Befehle auf dem Zielgerät. Stellen Sie sich zum Beispiel vor, dass ein Windows-Entwickler Code bereitstellen und dann eine bestimmte Site auf einem IIS-Server neu starten muss, aber daran gehindert werden sollte, einen IISRESET-Befehl auszugeben. Das PSM kann sicherstellen, dass ihre gewährte Rolle nur die minimal notwendigen Berechtigungen hat. Ein weiteres Beispiel für ein Linux-System wäre, dass das Sitzungsverwaltungssystem Benutzer daran hindert, sich seitlich über den *ssh*-Befehl zu bewegen.

Zusammenfassend unsere Einführung in PAM zeigt Abb. 12-1 eine Möglichkeit, wie eine PAM-Lösung eingesetzt werden kann, mit einem zentralen PAM-Richtlinienserver

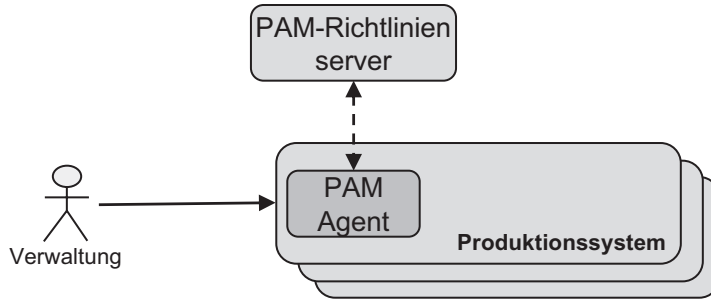

Abb. 12-1. *PAM bietet Zugriffskontrolle durch Sitzungsverwaltung*

und einer verteilten Reihe von PAM-Agenten, die auf Produktionsservern (den geschützten Ressourcen) laufen. In diesem Beispiel hat die Organisation möglicherweise beschlossen, ihre PAM-Lösung als Alternative zu anderen Ansätzen, wie Jump-Boxen, zu verwenden.

In diesem Beispiel erhält der Agent Informationen vom Richtlinienserver, der definiert, welche Berechtigungen ein bestimmter Benutzer auf dem Zielsystem ausführen kann. Das heißt, während der Benutzer direkten Zugriff auf den Server hat, kontrolliert der Agent, wer sich anmelden kann, und kann auch RBAC-Kontrollen sowie die Kontrolle von Admin-Aktionen bereitstellen. Beachten Sie, dass wir die PAM-Komponenten absichtlich mit einer Terminologie darstellen, die mit Zero Trust übereinstimmt, da es in gewisser Weise Gemeinsamkeiten zwischen ihnen gibt. Es gibt auch einige wichtige Unterschiede, die wir im nächsten Abschnitt untersuchen werden.

Schließlich, wenn wir nach vorne blicken (und breiter als nur Zero Trust), verändert die zunehmende Einführung von serverlosem Computing und DevOps-Stil „unveränderlicher Infrastruktur“ die Art und Weise, wie Admins privilegierte Aktionen ausführen, und macht traditionelle PSM (und in gewissem Maße auch Passwort-Tresore) weniger relevant. Wenn Organisationen diese philosophische Veränderung vornehmen, wechseln sie dazu, dass Admins *nie* tatsächlich auf ein Produktionssystem zugreifen müssen, um eine manuelle Aufgabe auszuführen. Richtig gemacht, führt dies zu schnelleren und zuverlässigeren Ergebnissen, bei denen mehr „als Code“ gesteuert und weniger manuell Aufgaben ausgeführt wird. Beachten Sie, dass wir später im DevOps-Szenario in Kapitel 18 darüber sprechen werden.

Zero Trust und PAM

Jetzt, wo wir uns PAM aus der Perspektive der traditionellen IT und Sicherheit angesehen haben, sprechen wir darüber, wie die Elemente von PAM in einer Zero Trust-Umgebung existieren. Bedenken Sie, dass PAM-Funktionen (Vaulting, Secrets, Session-Aufzeichnung) weiterhin eine wichtige Rolle in Sicherheitsarchitekturen spielen werden, es jedoch einige Änderungen (und mögliche Verminderungen) in einer Zero Trust-Umgebung geben kann.

Wie wir bereits erwähnt haben, verfügen viele PAM-Lösungen bereits über ein integriertes Richtlinien- und Zugriffsmodell und können sich mit Identitätsanbietern für Benutzerauthentifizierung, rollenbasierte Zugriffskontrolle und attributbasierte

Zugriffskontrolle integrieren. In dieser Hinsicht agieren sie in gewissem Maße wie Richtliniendurchsetzungspunkte. Aber lassen Sie uns zuerst das „800-Pfund-Gorilla“ von PAM - Password Vaulting - ansprechen. Die gesamte Prämisse von Password Vaulting basiert auf dem nicht-Zero Trust-Ansatz eines zu offenen Netzwerks, in dem jeder Benutzer ständigen Netzwerkzugriff auf jeden Server hat und daher ein Tresor mit Server-Passwort-Verschleierung und -Rotation erforderlich ist. Diese Prämisse ist mit Zero Trust nicht mehr wahr! Theoretisch könnten Sie in einem Zero Trust-Netzwerk tatsächlich auf Passwörter für privilegierten Zugriff auf Server verzichten und stattdessen auf die PEPs vertrauen, um Zero Trust-Richtlinien durchzusetzen, die an Kontext und Geschäftsprozesse gebunden sind. Jetzt schlagen wir nicht vor, dass Sie dies tatsächlich tun, aber es ist eine wichtige Perspektive und zeigt, wie ein Zero Trust-Netzwerk das Wertversprechen eines Passwort-Tresors verändern kann. Wir empfehlen nicht, PAM-Tresore aktiv außer Betrieb zu setzen, aber Sie sollten in Betracht ziehen, PAM-Tresore für neue Umgebungen und Projekte nicht zu verwenden. Bedenken Sie, dass die anderen Funktionen innerhalb von PAM – Secrets Management und Session-Aufzeichnung – in einer Zero Trust-Welt relevant bleiben werden.

Lassen Sie uns weiter erforschen, wie PAM sich auf Zero Trust bezieht. Der einfachste und am leichtesten zu erreichende Ansatz besteht darin, den Zugriff auf den PAM-Server selbst zu schützen, indem man ihn hinter einen PEP stellt, wie in Abb. 12-2 dargestellt. In diesem Szenario ist die PAM-Lösung eine geschützte Ressource innerhalb der Zero Trust-Architektur. Obwohl dies einfach ist, ist es dennoch sinnvoll und wertvoll – es erhöht die Sicherheit der PAM-Lösung, indem es unautorisierten Benutzern oder Geräten den Zugriff darauf verwehrt. Dies ist eine gute Sicherheitspraxis – schließlich, wenn der PAM-Server die „Schlüssel zum Königreich“ beherbergt, ist er ein natürliches Ziel für bösartige Akteure.

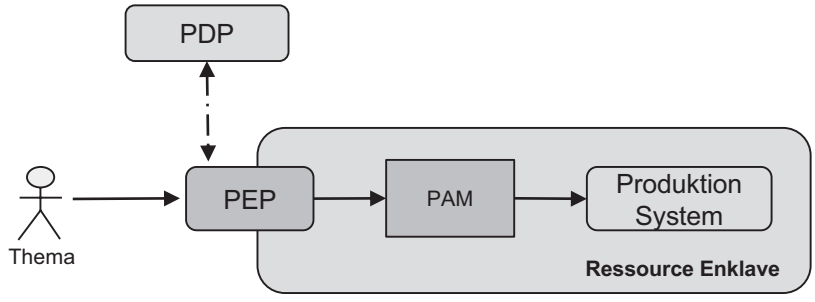

Abb. 12-2. *Implementierung des PAM hinter einem PEP*

Wenn wir über dieses einfache Szenario hinausgehen, lassen Sie uns untersuchen, wie PAM besser mit einer Zero Trust-Lösung integriert werden könnte, beispielsweise durch die Verwendung von Identitätskontext oder die Unterstützung bei der Durchsetzung von Richtlinien.

Eine mögliche Integration wird in Abb. 12-3 dargestellt, die zeigt, wie ein PDP mit PAM-Informationen oder -Richtlinien integriert und in der Lage sein kann, diese zu konsumieren, um sie in das Zero Trust-Richtlinienmodell zu integrieren. Diese Integration könnte so einfach sein wie die Verwendung des PAM, um den PDP darüber zu informieren, welche hochwertigen Server eine stärkere Authentifizierung oder Gerätehaltungsprüfungen erfordern. Oder es könnte eine komplexere Integration sein, bei der der PDP PAM-definierte Richtlinien darüber konsumiert, welche Administratoren Zugriff auf welche Server haben sollten, und diese an den PEP zur Durchsetzung weiterleitet.

Ein weiteres Szenario wird in Abb. 12-4 gezeigt, die zeigt, wie das PAM Informationen vom PDP konsumiert und diese verwendet, um den Zugriff besser zu kontrollieren. Dies könnten Identitäts- oder Geräteattribute sein, die verwendet werden können, um

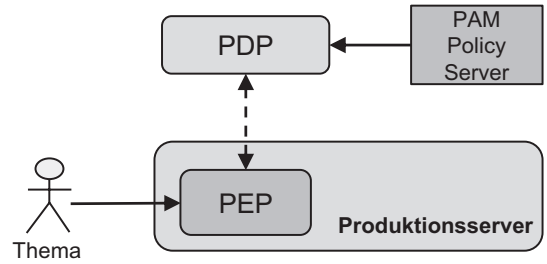

Abb. 12-3. *PAM Integration mit Zero Trust*

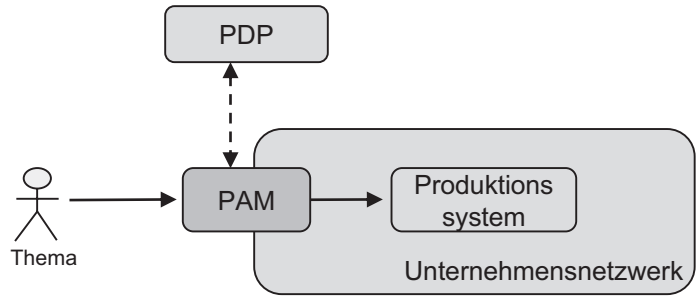

Abb. 12-4. *PAM Konsumiert Zero Trust-Kontext vom PDP*

bessere Entscheidungen darüber zu treffen, ob der Zugriff auf das Zielsystem erlaubt werden soll. Zum Beispiel haben die meisten PAM-Lösungen keine eingebauten Remote-Zugriffsfunktionen, während Zero Trust-Lösungen dies tun. Ein PDP könnte die Geolokalisierungsinformationen des Benutzers für das PAM verfügbar machen, das diese dann als Faktor bei der Entscheidung, ob der Zugriff erlaubt werden soll, verwenden könnte.

Obwohl diese letzten beiden Beispiele eher zukunftsorientiert sind als Szenarien, die heute tatsächlich praktiziert werden, glauben wir, dass Zero Trust-Plattformen, wenn sie weiter verbreitet werden, auch offener werden und diese Arten von Integrationen über verschiedene Sicherheitskomponenten von verschiedenen Anbietern unterstützen. Sie könnten auch schneller auftreten, wenn PAM-Anbieter in die Zero Trust-Arena expandieren.

Wir glauben, dass dies auch die Wege hervorhebt, auf denen PAM-Lösungen heute eher identitätsbewusst als identitätszentriert sind. Obwohl sie oft einen Unternehmensidentitätsanbieter zur Authentifizierung von Benutzern verwenden und Gruppenmitgliedschaften verwenden können, um Zugriffsrichtlinien zu bestimmen, ist dies in der Regel der Umfang ihrer Reichweite. Die zukunftsorientierten Szenarien, die wir in den Abb. 12-3 und 12-4 dargestellt haben, sind interessant und werden dazu beitragen, PAM-Lösungen in die dynamische und identitätszentrierte Welt von Zero Trust zu bringen.

Zusammenfassung

PAM bietet eindeutig wertvolle Passwort- und Zugriffsmanagementfunktionen und kann dazu beitragen, Sicherheits-, Compliance- und Audit-Anforderungen zu erfüllen. Während es auch dazu beiträgt, einige Aspekte des Prinzips der geringsten Privilegien zu erreichen, und Identitätsattribute zur Verwaltung des Zugriffs verwenden kann, ist es kein Ersatz für eine vollständige Zero Trust-Plattform. Aber die Integration eines PAM mit einer Zero Trust-Plattform kann den Wert beider Systeme erhöhen, und Organisationen, die ein PAM haben, sollten den Schutz des PAM-Servers selbst priorisieren. Sie könnten auch die Möglichkeiten betrachten, wie diese beiden Lösungen Informationen austauschen könnten, um gemeinsam bessere Zugriffsentscheidungen zu treffen, obwohl dies wahrscheinlich ein fortgeschrittener oder zukünftiger Anwendungsfall sein wird.

KAPITEL 13

Datenschutz

Forrester stellt Daten in den Mittelpunkt ihres Zero Trust eXtended (ZTX) Framework und das aus gutem Grund: Wertvolle Daten existieren in jeder Organisation und müssen geschützt werden. Aus unserer Zero Trust Perspektive ist Daten, die oft *das* primäre Ziel von Angreifern sind, eine Schlüsselressource des Unternehmens, die durch PEPs durch Integration mit einem PDP, über ein Identitäts- und Metadaten-zentriertes Richtlinienmodell, gesichert werden muss.

Datenmengen sind in den meisten Organisationen exponentiell gewachsen und hochwertige Daten werden nun regelmäßig gespeichert, abgerufen und verarbeitet über eine Vielzahl von Systemen, einschließlich On-Premises, Cloud-basiert und mobile Geräte. Das Volumen und die Komplexität der Daten werden nur weiter wachsen, wenn Organisationen mit Cloud-Migrationen und digitalen Transformationen fortfahren. Dieses Wachstum muss effektiv verwaltet und gesichert werden durch effektive Datenlebenszyklus- und Nutzungsinitiativen. In diesem Kapitel werden wir den Datenlebenszyklus, den Datenschutz und die Datennutzung (einschließlich Tagging und Klassifizierung) diskutieren und letztendlich, wie die Datensicherheit mit einer Zero Trust Strategie integriert werden sollte.

Datentypen und Datenklassifizierung

Daten können im Allgemeinen als einer von zwei verschiedenen Typen betrachtet werden: strukturiert und unstrukturiert. Der Unterschied zwischen diesen ist wichtig, da er beeinflusst, wie Sicherheit angewendet werden kann oder wie Technologie zur Unterstützung der Datensicherheit verwendet werden kann.

Strukturierte Daten sind Daten, die in einer Art Datenbank gespeichert sind und über einen spezifischen Mechanismus abgerufen und erstellt werden (z. B. über Structured Query Language, SQL). Der genaue Prozess der Datenspeicherung in einer Datenbank wird durch die gewählte Datenbanktechnologie bestimmt, aber in der Regel

J. Garbis und J. W. Chapman, *Zero Trust Sicherheit*, https://doi.org/10.1007/979-8-8688-0105-1_13

werden sie in einem binären Format gespeichert mit Zugriffskontrolle, die innerhalb des Datenbanksystems selbst definiert ist. Und Datenbanken verwenden im Allgemeinen ein definiertes Schema, das zulässige Datentypen einschränkt und Metadaten wie Spaltennamen zuweist. Zum Beispiel könnte eine Datenbanktabelle, die Mitarbeiterdatensätze speichert, eine Reihe von definierten Spalten haben, wie *Geburtsdatum* (Datentyp), *Straßenadresse* (freiform Text) und *Mitarbeiter-ID* (Integer-Typ). Dies legt eine implizite Ebene der Klassifizierung fest, die mit den Spalten der in dieser Tabelle gespeicherten Daten verbunden ist, die Anleitung über ihre Sicherheitsanforderungen gibt und wie sie behandelt werden sollte.

Unstrukturierte Daten sind Daten, die auf beliebige Weise erstellt und vom Benutzer oder der Technologie, die die Daten speichert, formatiert werden. Am wichtigsten ist, dass unstrukturierte Daten nicht in ein vordefiniertes Schema passen und daher eine Unfähigkeit zeigen, Sicherheitsanforderungen und Klassifizierung entweder ganzheitlich oder auf einer pro-Feld-Basis automatisch zu definieren. Das heißt, die Dateien selbst, weil sie unstrukturiert sind, liefern nicht von Natur aus Informationen über die in ihnen enthaltenen Daten. Im Gegensatz zum *Geburtsdatum* Datenbankspaltenbeispiel, gibt ein Dokument nicht explizit an, dass es Geburtsdaten von Mitarbeitern enthält. Darüber hinaus haben unstrukturierte Dateien andere Sicherheitsunterschiede von Daten in einer Datenbank. Dateien, die auf einem Dateifreigabe gespeichert sind, sind möglicherweise nicht verschlüsselt oder verschleiert durch andere Mittel als die Software, die die Datei erstellt hat. Während die Dateien in einem proprietären Format geschrieben sein können, ist der rohe Zugriff auf die Dateien abhängig von den Kontrollen, die auf den Speicherort gelegt werden, sei es eine Netzwerkdateifreigabe oder ein SaaS-basierter Dienst.

Natürlich gibt es ein Kontinuum zwischen diesen Klassifizierungen, da unstrukturierte Daten einen gewissen Grad an Kennzeichnung enthalten können und durch Konvention oder Geschäftsprozess eine gewisse implizite Struktur auferlegt bekommen können. Ebenso kann ein strukturiertes Datenschema unbeabsichtigt oder böswillig missbraucht werden und leicht effektiv unstrukturiert werden; zum Beispiel gibt es wenig mehr als Konvention, die die Verwendung eines „Kundenkontonotizen“ Feldes zur Speicherung von Sozialversicherungsnummern verhindert. Letztendlich ermöglichen uns die Verwendung eines Datenschemas und Betriebskonventionen zusammen, das ermöglichte Merkmal der Datensicherheit zu erreichen: Klassifizierung.

Sowohl strukturierte als auch unstrukturierte Daten erfordern eine Klassifizierung, um ein Datensicherheitssystem darüber zu informieren, wie es behandelt werden sollte. Klassifizierung ist der Prozess der Identifizierung des Risikolevels, das mit den Daten verbunden ist, basierend auf seiner potenziellen Auswirkung auf die Organisation. Das einflussreiche Dokument „Standards für die Sicherheitskategorisierung von Bundesinformationen und Informationssystemen" – FIPS Pub 199[1] – definiert die folgenden Levels:

- Niedrig: Verlust von Vertraulichkeit, Integrität und Verfügbarkeit mit begrenzten negativen Auswirkungen auf Geschäftsfunktionen (z. B. Marketing oder Website-Inhalt)
- Mittel: Verlust von Vertraulichkeit, Integrität und Verfügbarkeit mit ernsthaften negativen Auswirkungen auf Geschäftsfunktionen (z. B. Kundeninformationen, Preislisten, Geschäftspläne oder Strategiedokumente)
- Hoch: Verlust von Vertraulichkeit, Integrität und Verfügbarkeit mit schweren oder katastrophalen Auswirkungen auf Geschäftsfunktionen (z. B. Quellcode, Bankdaten oder Anmeldeinformationen)

Diese Klassifizierungen, obwohl auf hoher Ebene, können verwendet werden, um die initialen Zugriffsrichtlinien in einer Zero Trust Umgebung zu beeinflussen. Wir werden diese Klassifizierungen und Auswirkungen auf Zero Trust später in diesem Kapitel diskutieren und noch einmal im Kapitel zum Richtlinienmodell.

Datenlebenszyklus

Ähnlich wie eine Identität hat auch Daten einen konkreten Lebenszyklus. Der Lebenszyklus von Daten beginnt bei der Datenerstellung, setzt sich fort durch die Datennutzung und endet schließlich mit der Datenzerstörung. Jede dieser Phasen erfordert unterschiedliche Sicherheitsmethoden und -ansätze.

[1]FIPS Pub 199 ist Teil der Federal Information Processing Standards Serie vom US National Institute of Standards and Technology und bietet Richtlinien zur Bestimmung der Auswirkungen eines Datenverstoßes.

Datenerstellung

Daten können auf verschiedene Weisen erstellt werden; wie sie erstellt werden, bestimmt, ob die Daten als strukturiert oder unstrukturiert organisiert sind. Wie in Abb. 13-1 dargestellt, können Daten als Datei oder als Datensatz innerhalb einer Datenbank erstellt werden. Darüber hinaus werden Daten nicht immer von einer Person oder einem Benutzer erstellt – eine Anwendung oder ein Prozess kann für die Erstellung von Daten verantwortlich sein, entweder in einem strukturierten oder unstrukturierten Format. Daten umfassen auch eine Vielzahl von Typen, einschließlich Geschäftsdateien (z. B. Dokumente oder Tabellenkalkulationen), maschinell erzeugte Daten (z. B. Sensordaten oder berechnete Analyseergebnisse) oder wertvolles geistiges Eigentum (z. B. Quellcode, Geräteentwürfe oder genetische oder pharmazeutische Daten).

Unabhängig davon, wie diese Daten erstellt werden, sind Metadaten oder Tagging notwendig, um Klassifizierungsrichtlinien zu unterstützen. Es gibt mehrere Methoden, um diese Klassifizierungstags oder -labels zu erstellen: automatisiert, benutzerbasiert oder Discovery-Lösungen. Automatisierte Datenklassifizierung ist, wo Software Dokumente durch mehrere Mittel analysiert und klassifiziert, einschließlich Inhaltsanalyse, Dokumentenstandort, Benutzerabteilung oder die zugehörige Anwendung oder Geschäftsprozess. Diese Klassifizierung wird in der Regel während der Datenerstellung ausgeführt. Benutzerbasierte Klassifizierung erfordert Schulung und Fachwissen über den Inhalt der Daten. Während Benutzer ein effektives Mittel zur Bereitstellung von Tagging und Labels sein können, besteht das Risiko von Inkonsistenzen, da Menschen Tags und Labels möglicherweise unterschiedlich

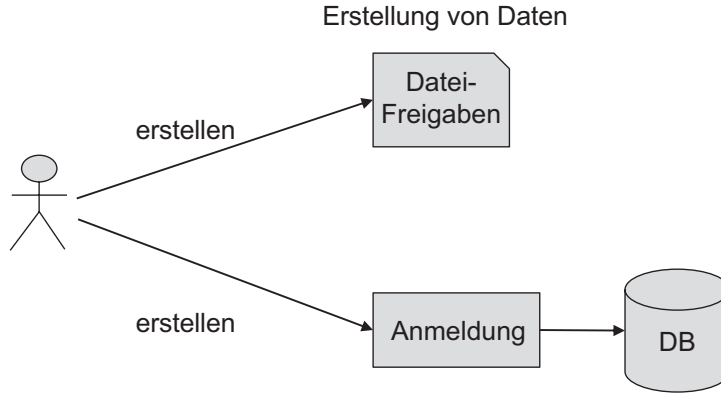

Abb. 13-1. *Datenlebenszyklus—Datenerstellung*

anwenden, selbst mit Schulung. Schließlich klassifizieren auch Discovery-Tools Daten, unterscheiden sich jedoch von automatisierten Klassifizierungslösungen dadurch, dass sie oft nach der Erstellung und Speicherung der Daten ausgeführt werden. Sie bieten Tagging und Labeling basierend auf Inhalt, Standort und angewendeten Suchregeln, sind aber im Gegensatz zu automatisierten Klassifizierungstools möglicherweise nicht über die Identität, Anwendung oder den Prozess, der die Daten erstellt hat, informiert.

Datennutzung

Obwohl alle Daten gesichert werden sollten, ermöglicht die Klassifizierung eine effektivere Sicherheit in der nächsten Phase des Datenlebenszyklus, wenn sie tatsächlich genutzt wird. Es gibt mehrere Stufen zu berücksichtigen bei der Datennutzung – Daten-im-Ruhezustand, Daten-in-Bewegung und Daten-in-Verwendung. Diese Stufen bieten sowohl Herausforderungen als auch Vorteile bei der Datenverwaltung und -sicherheit.

Abb. 13-2 veranschaulicht ein Beispiel dafür, wie Daten durch mehrere Stufen gehen können, wenn sie von einem Benutzer über eine Anwendung durch einen Webbrowser abgerufen werden. Bevor sie abgerufen werden, befinden sich die Daten im *Daten-im-Ruhezustand* Zustand. Diese Phase tritt auf, nachdem die Daten erstellt und auf eine Form von dauerhaftem Speicher geschrieben wurden. Um Daten-im-Ruhezustand zu sichern, bietet die vollständige Festplatten- oder Datenbanktabellenverschlüsselung (oder ein anderer ganzheitlicher Ansatz) ein Maß an Sicherheit, obwohl es wichtig ist zu

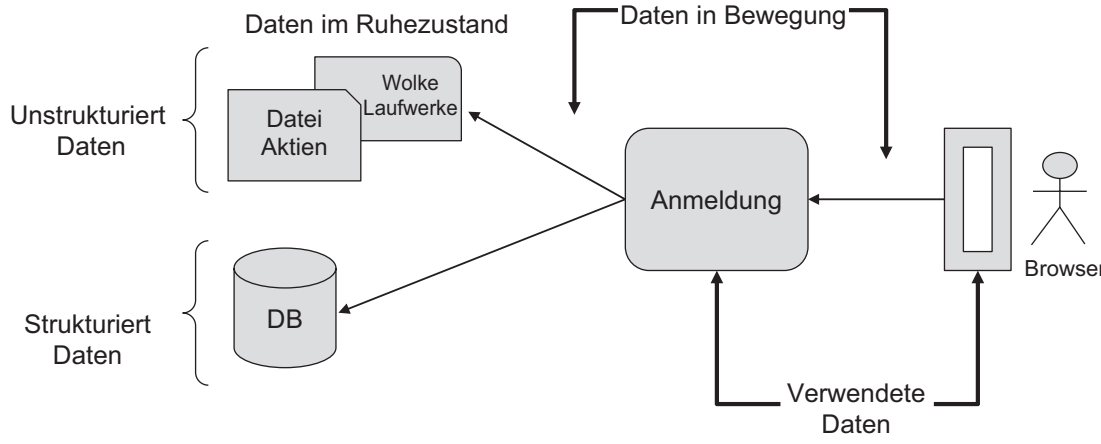

Abb. 13-2. *Datennutzung*

verstehen, dass dies die Daten nicht als Ressource schützt. Der Prozess der Verschlüsselung der gesamten Festplatte oder der Datenbanktabellenverschlüsselung schützt vor physischem oder Festplattenzugriff auf die Daten, ist jedoch nicht Teil eines Autorisierungsmodells.

Weiter mit dem in Abb. 13-2 dargestellten Beispiel, gibt es zwei Vorkommnisse von Daten-in-Bewegung, wenn der Benutzer auf die Anwendung zugreift. Die Anwendung wird einen Aufruf an den Speicherort machen, um die Daten abzurufen; dies ist die erste Möglichkeit, Daten-in-Bewegung über eine verschlüsselte Netzwerkverbindung zwischen der Anwendung und dem Speicher zu sichern. Das Netzwerk zwischen dem Benutzergerät und der Anwendung ist eine zweite Möglichkeit zur Sicherung von Daten-in-Bewegung, die HTTPS oder einen anderen sicheren TCP-Kanal verwenden sollte. Daten-in-Bewegung ist in vielerlei Hinsicht die einfachste Phase, um Daten zu sichern; es kann einfach durch die Verwendung eines verschlüsselten Netzwerkprotokolls gelöst werden und sollte in der Tat für alle Daten-in-Bewegung angewendet werden, unabhängig von ihrer Klassifizierung.

Schließlich ist Daten-in-Verwendung, wenn die Daten aktiv im Speicher innerhalb von Software wie Anwendungsklienten, Browsern oder Anwendungsservern gehalten werden. Dies ist oft der schwierigste Zustand von Daten zu sichern. Wie in Abb. 13-2 dargestellt, kann es sehr schwierig sein, die Daten zu schützen, sobald die Anwendung die Daten im Speicher lädt. Es gibt Datensicherheitstechniken, wie In-Memory-Verschlüsselung, Datentokenisierung oder Verschleierung, die verwendet werden können, um die Daten in Verwendung zu schützen. Dies ist stark anwendungs- und technologieabhängig. Für SaaS-Anwendungen können Lösungen wie CASBs helfen, während unternehmenseigene Anwendungen in der Regel auf Entwickler angewiesen sind, um bewährte Designmuster und Toolkits oder Bibliotheken zu nutzen.

Daten Zerstörung

Die letzte Phase des Datenlebenszyklus ist die Datenzerstörung. Organisationen, insbesondere solche in regulierten Branchen oder die sensible Daten verwalten, müssen Datenhaltungsrichtlinien definieren und durchsetzen, die bestimmen, wie lange Daten gespeichert und zugänglich bleiben sollten, bevor sie zerstört werden. Beachten Sie, dass verschiedene Geschäftsvertikale unterschiedliche Anforderungen haben, was die Verwaltung dieser „End-of-Life“-Richtlinien herausfordernd machen kann, insbesondere für größere oder mehrbranchige Unternehmen.

Heute gibt es eine wachsende Anzahl von Dienstleistern für den Datenlebenszyklus, die Datenlagerung und Durchsetzung von Aufbewahrungsrichtlinien als Dienstleistung anbieten, in der Regel über SaaS. Diese SaaS-Plattformen können helfen, indem sie eine konsistente und vereinfachte Durchsetzung von Klassifizierungsrichtlinien bieten, wodurch die Kosten und der Aufwand für traditionelle On-Premises-Speicher- und Verwaltungsprogramme reduziert werden.

Datensicherheit

Datensicherheit wird in verschiedenen Phasen des Datenlebenszyklus unterschiedlich erreicht. Wie im vorherigen Abschnitt erwähnt, können Daten relativ einfach für Daten-im-Ruhezustand (über vollständige Laufwerksverschlüsselung) und für Daten-in-Übertragung (über verschlüsselte Übertragungen) gesichert werden. Aber die herausforderndere und interessantere Phase ist definitiv Daten-in-Verwendung, die Data Loss Prevention (DLP) Lösungen adressieren können.

DLP-Lösungen, die von Unternehmen weit verbreitet eingesetzt werden, bieten eine Reihe von technischen Kontrollen und sind typischerweise auf die folgenden Elemente ausgerichtet:

- Gerätekontrolle: Die Möglichkeit zu definieren, wie Daten auf Geräteebene genutzt werden können (z. B. das Verhindern der Druck- oder Kopier- und Einfügefunktion, oder ob USB-Ports auf einem Gerät genutzt werden können).
- Inhaltsbewusste Kontrolle: Durchsetzung und Anpassung von Sicherheitskontrollen für Daten basierend auf dem Inhalt der Daten. Dies kann die Datenverschleierung beinhalten.
- Erzwungene Verschlüsselung: Sicherstellung, dass Daten-im-Ruhezustand auf Laufwerks- oder physischer Speicherebene verschlüsselt sind. Ihr Zweck ist es, sicherzustellen, dass die gespeicherten Daten unzugänglich bleiben, selbst wenn das Gerät verloren geht oder gestohlen wird.
- Datenerkennung: Einer der wichtigsten Aspekte der Datensicherheit, Erkennungslösungen bieten Organisationen die Möglichkeit, nicht nur unbekannte sensible Daten zu finden, sondern auch deren Klassifizierung zu automatisieren.

DLP-Lösungen haben technische Mittel zur Durchsetzung von Zugriffskontrollrichtlinien und bleiben in einer Zero Trust-Umgebung relevant. Natürlich müssen die tatsächlichen Richtlinien, die DLP-Systeme durchsetzen, von der Organisation definiert, validiert und gepflegt werden. Diese Aktivitäten finden in einem Bereich der Informationssicherheit statt, der als Data Access Governance (DAG) bekannt ist.

DAG steht in enger Beziehung zur Identitäts-Governance-Fähigkeit innerhalb von IAM und definiert, wo und wie Daten zugegriffen werden können, von wem und letztendlich, wann sie Zugang haben sollten. In einer Zero Trust-Umgebung sollte die Verwendung von DAG zur Definition der Bedingungen, unter denen auf Daten zugegriffen werden kann, idealerweise direkt an Zero Trust Richtlinien gebunden sein. DAG bietet Fähigkeiten und Zugriffsregeln, die die Daten regieren und letztendlich, wie Richtlinien in der gesamten Organisation angewendet werden.

Durch Datenklassifizierung kann Daten-Governance effektiv einen Mechanismus für die Durchsetzung von Zugriffsrichtlinien bereitstellen und weiterhin durch Metadaten-Tags verwaltet werden. Diese Metadaten-Tags können als Eingabe in Zero Trust RBAC oder ABAC Richtlinien dienen.

Digital Rights Management (DRM) ist eine weitere Art von Datensicherheitsmaßnahme, die den Eigentümern von proprietären Daten, daten, die ein Copyright haben, oder anderen geschäftlichen Daten, die wertvolles geistiges Eigentum (IP) sein könnten, Kontrollen bietet. DRM setzt technische Kontrollen durch, die vom Datenbesitzer definiert wurden, und kann steuern, wie diese Daten sowohl genutzt als auch für kurz- und langfristige Zwecke zugegriffen werden können. Einige DRM-Lösungen können und tun sich in Zero Trust-Plattformen einbinden, indem sie Kontext wie Identität und Geräteattribute nutzen.

Während DRM darauf abzielt, den Zugriff auf die Daten zu kontrollieren, verschleiern andere Ansätze wie traditionelle Datenverschlüsselung, neuere Ansätze wie Daten-Tokenisierung und aufkommende Technologien wie homomorphe Kryptographie[2] alle die Daten selbst und bieten Möglichkeiten zur Unterstützung von Zero Trust-Richtlinien im Datenschutz. Die Integration von Zero Trust in diese

[2]Diese Algorithmen ermöglichen es, arithmetische Berechnungen auf verschlüsselten Daten durchzuführen, ohne dass eine Entschlüsselung erforderlich ist. Dies beseitigt effektiv Daten-in-Verwendung und Daten-in-Übertragung als Risikofaktoren für bestimmte Anwendungsfälle.

Technologien kann die Durchsetzung von identitäts- und kontextbewussten Datenzugriffsrichtlinien ermöglichen, unabhängig von der Verschleierungsmethode. Wir werden dies im folgenden Abschnitt weiter untersuchen.

Zero Trust und Daten

In Kap. 3 haben wir mehrere Zero Trust Einsatz Modelle vorgestellt, die letztendlich Möglichkeiten bieten, wie PEPs Ressourcen schützen. Diese Ressourcen in diesen Szenarien wurden absichtlich allgemein dargestellt – sie könnten Daten, Anwendungen zur Steuerung/Modifizierung von Daten oder Transaktionen sein. In allen Fällen verwendet das Zero Trust PEP Richtlinien zum Schutz dieser Ressourcen, und wie wir diskutiert haben, müssen PDPs kontextbezogene Informationen verwenden, um Zugriffsentscheidungen zu treffen. Im Falle von Daten können deren Klassifizierung und Metadaten in Zero Trust-Richtlinien verwendet werden. Lassen Sie uns also untersuchen, wie ein PDP und ein PEP aus der Datenperspektive in einer Zero Trust-Umgebung aussehen.

Wie bereits erwähnt, wird die Datenklassifizierung durch Kennzeichnung und Tagging von Datenelementen in der Umgebung erreicht. Wenn möglich, sollten diese Kennzeichnung und Tagging als Elemente von Zero Trust-Richtlinien verwendet werden. Diese Richtlinien gewähren Zugriff basierend auf Rollen, Attributen oder anderen Identitätsdaten und sollten auch Zugriffsentscheidungen basierend auf Datenattributen enthalten. Während diese Klassifizierungen und Richtlinien direkt aus regulatorischen oder Compliance-Standards resultieren können, die der Organisation auferlegt werden, müssen die tatsächlichen Kontrollen, die vom Sicherheitssystem durchgesetzt werden, auf dem Risikomodell und der Risikotoleranz der Organisation basieren.

Um dieses Konzept zu erweitern, wird das Audit- und Sicherheitsteam einer Organisation in der Regel Kontrollen definieren, um regulatorische und Compliance-Standards zu unterstützen. Zum Beispiel sind börsennotierte Unternehmen in den Vereinigten Staaten Sarbanes Oxley (SOX) Standards unterworfen. Da SOX-Standards sich auf Daten konzentrieren, wird die Klassifizierung durch Tagging und Kennzeichnung Unterstützung für Richtlinien bieten, wie sie von Audit- und Sicherheitsteams in Bezug auf Finanzdaten definiert werden. Um einige dieser Richtlinien umzusetzen, kann eine Lösung für die Datenzugriffssteuerung verwendet werden, um diese Fähigkeiten bereitzustellen.

Abb. 13-3 zeigt, wie eine Datensicherheitslösung möglicherweise innerhalb des enklavenbasierten Zero Trust-Modells eingesetzt wird. Die *Ressource,* in diesem Modell, sind die Daten, die vom PEP geschützt werden, der Richtlinien verwendet, die vom PDP mit Eingaben von einer DAG-Lösung definiert wurden. In dieser Darstellung könnte der geschützte Zugriff ein direkter Zugriff des Benutzers von seinem Gerät sein, oder eine Anwendung, die auf die Daten im Auftrag des Benutzers zugreift. Zum Beispiel, wenn die gesamte Datenressource als „Kundenakten" gekennzeichnet ist, dann sollten nur Identitäten, die in einer bestimmten Gruppe (Kundendienstteam) sind, überhaupt Zugriff auf diese Datenressource haben. Die Implikation dieser Richtliniendurchsetzung ist, dass eine Anwendung, die versucht, auf diese Daten von außerhalb der Ressourcenenklave zuzugreifen, vom PEP blockiert werden kann. In dieser Situation muss die Anwendung möglicherweise eine authentifizierte Zero Trust-Identität sein und Identitätskontext bereitstellen, um Zugang zu erhalten.

In einem effektiven Zero Trust-System würde es eine bidirektionale Integration zwischen dem PEP und dem Datenmanagementsystem oder der Anwendung geben. Das Datenmanagement-Tool würde Datenattribute an das PDP und PEP liefern, zur Verwendung innerhalb von Richtlinienentscheidungen und Durchsetzung. Und das Datenmanagementsystem wäre in der Lage, kontextbezogene Informationen aus dem Zero Trust-System zu konsumieren, um Echtzeit-Richtliniendurchsetzungsaktionen durchzuführen.

Natürlich können einige Daten lokal auf Benutzergeräten gespeichert werden und müssen dennoch gesichert werden. Zero Trust kann in Verbindung mit Datensicherheitslösungen auf zwei verschiedene Arten arbeiten, dargestellt in den Abb. 13-4 und 13-5.

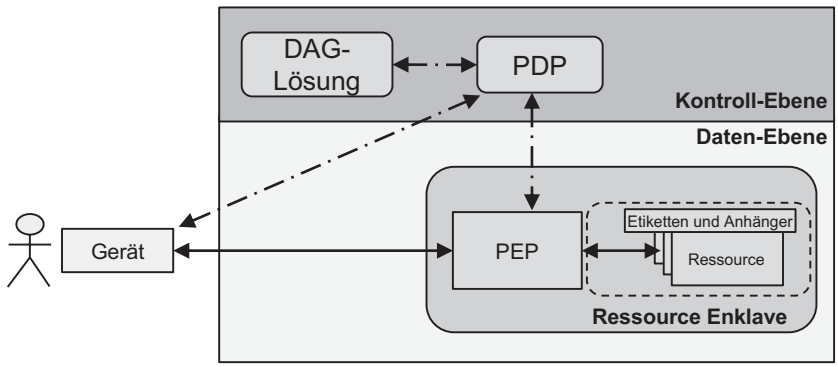

Abb. 13-3. *Datenmanagement im Enklavenbasierten Modell*

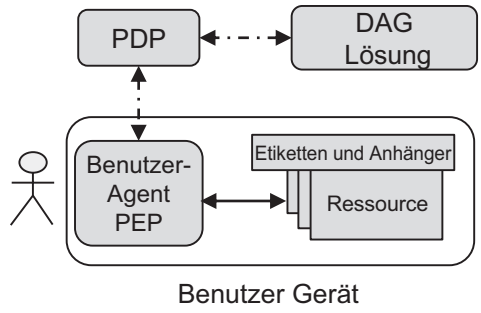

Abb. 13-4. *Datenzugriffssteuerung und Datenschutz auf einem Benutzergerät*

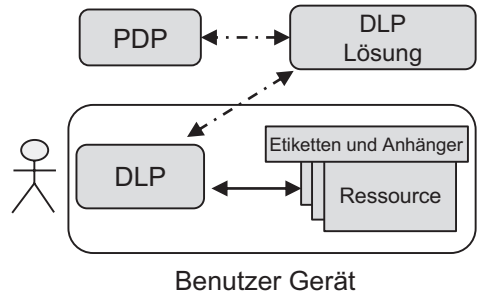

Abb. 13-5. *Verhinderung von Datenverlust und Datenschutz auf einem Benutzergerät*

Abb. 13-4 zeigt, wie ein Zero Trust-System mit einer Datenzugriffssteuerungslösung in Verbindung mit einem auf dem lokalen Gerät des Benutzers laufenden Benutzeragenten-PEP arbeiten kann. Da DAG-Lösungen Richtlinien definieren, anstatt aktiv Zugriffskontrollen durchzusetzen, liefert das DAG-System Eingaben in das PDP. Diese zusätzlichen Informationen sollten das PDP über Datenrichtlinien informieren und helfen, das PEP dazu anzuweisen, Zugriffskontrollen lokal auf der Grundlage der Etiketten und Tags der Daten durchzusetzen. Dies steht im Gegensatz zu Abb. 13-5, die zeigt, wie das Gerät des Benutzers eine DLP-Komponente hat, die aktiv Kontrollen durchsetzt.

In diesem Beispiel stellt das Zero Trust-System Identitäts- und Sitzungskontextinformationen für das DLP-System zur Verfügung, um sie innerhalb seines internen Autorisierungsmodells (Zugriffskontrolle) zu verwenden. Zum Beispiel könnte ein Zero Trust-System Benutzergeolokalisierungsinformationen bereitstellen, die es dem DLP ermöglichen, Datenresidenzanforderungen durchzusetzen. Beachten Sie, dass dies die lokale DLP-Mechanik effektiv zu einem (Mini) Zero Trust PEP macht.

Zusammenfassung

In diesem Kapitel haben wir uns auf Daten als Ressource in der Zero Trust-Umgebung konzentriert, die natürlich wie andere Ressourcen Schutz benötigt. Aus unserer Zero Trust-Perspektive bedeutet dies, dass Daten über PEPs zugegriffen werden müssen, die einen identitätszentrierten Sicherheitskontext durchsetzen. Datenlebenszyklusmanagement, Datensteuerung und DLP sind wichtige Elemente zur Gewährleistung der Datensicherheit und werden weiterhin existieren (und effektiv bleiben), auch außerhalb einer Zero Trust-Lösung. Die Verwendung einer identitätszentrierten Sicherheitslösung wird letztendlich eine Datensicherheitslösung verbessern. Dies ist jedoch definitiv ein fortgeschritteneres Szenario. Wir empfehlen, dass Ihre Zero Trust-Strategie zu einem bestimmten Zeitpunkt einen kontextsensitiven Datenschutz beinhaltet, obwohl dies in der Regel nicht der beste Anwendungsfall für ein frühes Projekt ist und von den Datenschutzfähigkeiten Ihrer ausgewählten Zero Trust-Plattform abhängt.

KAPITEL 14

Infrastruktur und Plattform als Dienst

Die Einführung von Cloud Computing war einer der größten und einflussreichsten Veränderungen in unserer Branche im letzten Jahrzehnt und zeigt keine Anzeichen einer Abschwächung. Die Leistungsfähigkeit und Allgegenwärtigkeit von Infrastructure as a Service (IaaS) und Platform as a Service (PaaS) Angeboten haben die Art und Weise, wie ein Großteil unserer Software erstellt, bereitgestellt und abgerufen wird, verändert. Wir glauben jedoch nicht, dass diese Plattformen bereits einen ähnlich breiten und bedeutenden Einfluss auf die Sicherheit hatten. Obwohl diese Plattformen über ausgeklügelte und leistungsstarke Zugriffskontrollmodelle verfügen, sind sie hauptsächlich darauf ausgelegt, Dienste innerhalb ihrer Cloud-Umgebungen zu schützen und nicht als umfassende Unternehmenssicherheitslösungen für alle Benutzer in mehreren heterogenen Umgebungen zu dienen.

Dieser breite Anwendungsbereich – der Zugriffsschutz für alle Benutzer auf alle Ressourcen – ist natürlich ein grundlegendes Prinzip von Zero Trust. Das bedeutet nicht, dass diese IaaS- und PaaS-Cloud-Plattformen nicht Teil (sogar ein bedeutender Teil) einer Zero Trust-Sicherheitsbereitstellung sein können. Immerhin hat Google viele dieser Prinzipien intern entwickelt und hat begonnen, Elemente davon kommerziell als Teil ihrer Cloud-Plattform verfügbar zu machen. Im Allgemeinen konzentrieren sich die Sicherheitslösungen der großen Cloud-Anbieter jedoch darauf, Sicherheit innerhalb ihrer Cloud-Plattformen zu bieten, anstatt als allgemeine Sicherheitslösungen für das gesamte Unternehmen. Die Ausnahme hiervon ist Microsoft, das seine Stärken in Identität, Desktop-Betriebssystem und Cloud-Computing auf innovative und interessante Weise nutzt.

Denken Sie daran, dass unser Ziel nicht darin besteht, Anbieter und ihre Angebote zu bewerten oder zu rangieren – das ist ein sehr dynamisches und bewegliches Ziel –

J. Garbis und J. W. Chapman, *Zero Trust Sicherheit*, https://doi.org/10.1007/979-8-8688-0105-1_14

unser Ziel ist es, Ihnen ein Framework und eine Reihe von Tools zur Verfügung zu stellen, damit Sie fundierte und informierte Entscheidungen darüber treffen können, wie Sie am besten mit Ihrer Zero Trust-Initiative fortfahren. Und in den heutigen Unternehmen sind IaaS und PaaS so wichtig, dass jede Zero Trust-Initiative sie sehr wahrscheinlich einschließen wird. Lassen Sie uns eintauchen.

Definitionen

Infrastructure as a Service ist gut verstanden und einfach zu definieren: dynamische Bereitstellung eines vollständigen Betriebssystems, bereitgestellt in einer Cloud Service Provider (CSP) Umgebung mit einem „Pay-as-you-go" Service-Modell. Unternehmenskunden sind verantwortlich für die Konfiguration und Wartung des vollständigen Betriebssystems und seines umgebenden Netzwerks sowie für die Bereitstellung jeder gewünschten Software auf dem virtuellen Server. Effektiv ist die Infrastruktur, die Unternehmen als Dienst nutzen, eine virtuelle „Bare-Metal"-Maschine, auf die sie ein Betriebssystem-Image ihrer Wahl bereitstellen und konfigurieren.

Platform as a Service hingegen umfasst eine Vielzahl von Funktionen und Modellen über die CSPs hinweg, mit einer potenziell verwirrenden Reihe von Fähigkeiten. Der Begriff *serverloses Computing* wird auch häufig verwendet, wenn über PaaS gesprochen wird, und bezieht sich auf die Möglichkeit, benutzerdefinierten Code bereitzustellen, der Funktionen implementiert, die Sie geschrieben haben, ohne dass ein vollständiges Serverbetriebssystem bereitgestellt werden muss. Serverlose Funktionen werden in eine PaaS-Umgebung bereitgestellt, die die umgebende Infrastruktur für den Zugriff, die Verwaltung und den Start bereitstellt.

Wir erkennen an, dass wir die sehr beträchtliche Breite der PaaS-Fähigkeiten, die bei den großen CSPs verfügbar sind, wie Cloud-Funktionen, containerisierte Workloads, Service-Meshes und alles dazwischen, übergehen. Wir werden einige davon später in diesem Kapitel untersuchen, wenn wir die Möglichkeiten kategorisieren und untersuchen, wie sie in eine Zero Trust-Umgebung integriert werden können.

Obwohl IaaS und PaaS erhebliche Unterschiede aufweisen, haben sie auch einige Gemeinsamkeiten. Vor allem werden sie beide als Mittel verwendet, um benutzerdefinierte Ressourcen zu beherbergen und auszuführen, die von dem Unternehmen entworfen und bereitgestellt wurden. Diese Ressourcen können benutzerdefinierter Code in einer Funktion, ein vollständiges ausführbares Programm

oder eine Webanwendung oder sogar nur eine unternehmensgestaltete Datenbank sein, zum Beispiel. In allen Fällen handelt es sich um Ressourcen (Code oder Daten), die das Unternehmen bestimmten Identitäten zugänglich machen möchte und die daher ein Zugriffskontrollmodell benötigen.

IaaS und PaaS sind für Zero Trust von großer Bedeutung, da diese Plattformen einen großen Anteil daran haben, wie Anwendungen heute erstellt und bereitgestellt werden. Natürlich haben CSPs ausgeklügelte und robuste Zugriffskontrollmechanismen, die Aspekte von Zero Trust bieten. Zum Beispiel bietet Googles GCP den Identity-Aware Proxy, der identitätszentrierte Fernzugriffsrichtlinien für GCP-Ressourcen durchsetzt. Die internen Sicherheitsmodelle der CSPs bringen jedoch einige Komplexität mit sich, wenn diese Ressourcen von externen Identitäten abgerufen werden. Insbesondere ist der Fernzugriff oft außerhalb des Geltungsbereichs des CSP und erfordert eine Koordination oder Abstimmung mit einer anderen Sicherheitslösung an den Stellen, an denen der Zugriff die Grenzen zwischen Sicherheitsdomänen überschreitet.

Hier kann eine Zero Trust-Plattform helfen, indem sie Sicherheit und Zugriffskontrollen über System- und Silogrenzen hinweg normalisiert. Beachten Sie, dass die Integration zwischen Zero Trust und der nativen CSP-Sicherheit gültig und wertvoll ist, wie zum Beispiel die Verwendung von Cloud-Metadaten-Tags als Eingabe in kontextbezogene Richtlinien. Sie sollten jedoch vorsichtig sein, nicht zu viel zu versuchen. Zum Beispiel mag es technisch machbar sein, aber es macht möglicherweise keinen Sinn, Ihr Zero Trust-System zur Verwaltung der Zugriffskontrolle für Dienste zu verwenden, die vollständig innerhalb einer IaaS- oder PaaS-Plattform bereitgestellt und aufgerufen werden. Die Entscheidung, wo und wann der Geltungsbereich Ihrer Zero Trust-Initiative eingeschränkt werden soll, wird ein wichtiger Faktor für den Erfolg sein.

Lassen Sie uns unsere Diskussion über IaaS- und PaaS-Dienste fortsetzen und die Möglichkeiten untersuchen, wie Zero Trust in diesen Umgebungen verwendet werden kann und sollte.

Zero Trust und Cloud-Dienste

Die Art und Weise, wie eine Zero Trust-Sicherheits plattform in eine IaaS- oder PaaS-Umgebung passt, hängt von Ihrem Zero Trust-Bereitstellungsmodell sowie von den Arten von Cloud-Plattformdiensten ab, die Sie gewählt haben. Insbesondere die Zero Trust-Enklaven-basierten und Cloud-gerouteten Bereitstellungsmodelle funktionieren

gut, da in beiden Fällen der PEP extern zu den Ressourcen ist, die sie schützen. Das heißt, sie fungieren als natürliche architektonische Komponente an der Grenze des CSP für den externen Zugriff, was dem Zero Trust-System ermöglicht, seine identitätszentrierten Richtlinien durchzusetzen, bevor es den Subjekten erlaubt, auf Ressourcen innerhalb der Cloud-Umgebung zuzugreifen.

Im Gegensatz dazu erfordern die ressourcenbasierten und Mikrosegmentierungsmodelle zwei Dinge, die in Cloud-Umgebungen eine Herausforderung sein können. Erstens muss der PEP auf der Ressource selbst laufen. Dies stellt kein Problem für IaaS-Ressourcen dar, ist aber in der Regel nicht mit PaaS-Ressourcen kompatibel. Zweitens bieten diese beiden Modelle in der Regel keine Mechanismen zur Durchsetzung der Zugriffskontrolle über Netzwerkgrenzen hinweg. Das heißt, sie erfordern, dass die Subjekte direkten Netzwerkzugriff auf die PEPs haben. Dies funktioniert für Dienste und Ressourcen in einem lokalen Netzwerk, erfordert jedoch einen separaten Zugriffsmechanismus für entfernte Subjekte, der nicht ein inhärenter Teil dieser beiden Modelle ist. Aus unserer Sicht machen diese Einschränkungen es, insbesondere für Cloud-Dienste, die wahrscheinlich von einer Vielzahl von Standorten aus zugegriffen werden, schwierig, diese Zero Trust-Modelle für IaaS- und PaaS-Ressourcen in vielen Situationen zu verwenden. Darüber hinaus haben CSPs ihre eigenen intern entwickelten (und normalerweise recht effektiven) Sicherheitsmodelle für den Dienst-zu-Dienst-Zugriff innerhalb der PaaS-Umgebung. In der Praxis ist es wahrscheinlich besser, das native Zugriffskontrollmodell des CSP für interne PaaS-Dienste zu akzeptieren, anstatt ein externes und möglicherweise inkompatibles aufzuzwingen. Wir untersuchen dies später im Kapitel, wo wir Service-Meshes diskutieren.

Bisher haben wir uns angesehen, wie wir das Zero Trust-Sicherheitsmodell auf IaaS- und PaaS-Ressourcen anwenden können, und was wir gesehen haben, ist, dass der PEP am effektivsten als Zugriffskontrollpunkt über die Cloud-Grenze hinweg (am Eingangspunkt in die Cloud-Umgebung) funktioniert. Lassen Sie uns untersuchen, wie genau das funktionieren kann, indem wir uns ansehen, wie Cloud-Dienste zugegriffen werden und wie der Zugriff entsprechend kontrolliert werden kann. Unsere Diskussion und Diagramme basieren auf dem Enklaven-basierten Zero Trust-Modell zur Vereinfachung, obwohl sie für ein Cloud-geroutetes Zero Trust-System weitgehend gleich funktionieren werden.

Im Gegensatz zu SaaS-Diensten, die wir im folgenden Kapitel besprechen, verfügen alle IaaS- und PaaS-Plattformen über integrierte Zugriffskontrollmethoden, die sie

universell leicht mit einem Zero Trust PEP integrierbar machen. Es gibt mehrere technische Methoden, mit denen Cloud-Plattformen diese Zugriffskontrolle durchsetzen; zur Vereinfachung bezeichnen wir sie hier allgemein als *Zugangsgateway*, das die Möglichkeit bietet, eine Quell-IP-Adressfilterung als logische Eingangsfirewall in eine IaaS- oder PaaS-Umgebung durchzuführen. Diese Fähigkeit, obwohl grundlegend, ist alles, was wir benötigen, um unser Ziel zu erreichen: Unser Zero Trust-System (durchgesetzt über den PEP) ist die Art und Weise, wie wir dynamische und identitätszentrierte Richtlinien anwenden.

Abb. 14-1 zeigt das Szenario, in dem ein PEP, der auf einer CSP-Plattform läuft, verwendet wird, um den Zugriff auf IaaS- oder PaaS-Ressourcen innerhalb der gleichen Cloud-Umgebung zu steuern. Zugriffskontrollen über dieses Modell fallen in eine von zwei allgemeinen Kategorien.[1] IaaS-Ressourcen wird eine IP-Adresse zugewiesen, und der Zugriff auf diese IP-Adresse wird innerhalb des Zugangsgateways des CSP so konfiguriert, dass *nur* der Verkehr, der vom PEP ausgeht, Zugriff auf die Ressource hat. Abb. 14-1 zeigt dies in dem Szenario, in dem die IaaS-Ressource eine private IP-Adresse von 10.5.3.1 hat (zu der Remote-Benutzer ihren Verkehr sowieso nicht routen könnten). Das Zugangsgateway ist so konfiguriert, dass es den Remote-Zugriff auf den PEP von jeder externen IP-Adresse, wie zum Beispiel von einem Remote-Benutzergerät, zulässt. Natürlich erzwingen der PEP (und der PDP, nicht gezeigt) die Zero Trust-Richtlinien; das Zugangsgateway wird ausschließlich dazu verwendet, sicherzustellen, dass der gesamte Ressourcen-gebundene Verkehr über den PEP geleitet wird und daher seinen Richtlinien unterliegt.

Beachten Sie, dass selbst wenn dieser IaaS-Ressource eine öffentliche IP-Adresse zugewiesen wäre, das Diagramm und das Endergebnis genau gleich sein könnten. Solange das CSP-Netzwerk so eingerichtet ist, dass der gesamte Ressourcen-gebundene Verkehr nur vom PEP ausgehen kann, kann das System sicherstellen, dass seine Zero Trust-Richtlinien durchgesetzt werden. Beachten Sie auch, dass diese Ressource, obwohl sie als einzelnes Objekt dargestellt wird, tatsächlich einem einzelnen Dienst (TCP-Port) auf einer IaaS-Instanz entsprechen könnte. Dieser Ansatz könnte beispielsweise für eine IaaS-Instanz nützlich sein, die einen öffentlich zugänglichen HTTPS-Webserver auf Port 443 betreibt, aber eine PEP-geschützte administrative SSH-Schnittstelle auf TCP-Port 22 aufrechterhält.

[1] Obwohl es natürlich zusätzliche Varianten und Fähigkeiten gibt. Wir können hier aufgrund von Platz- und Umfangsbeschränkungen keine erschöpfende Liste liefern.

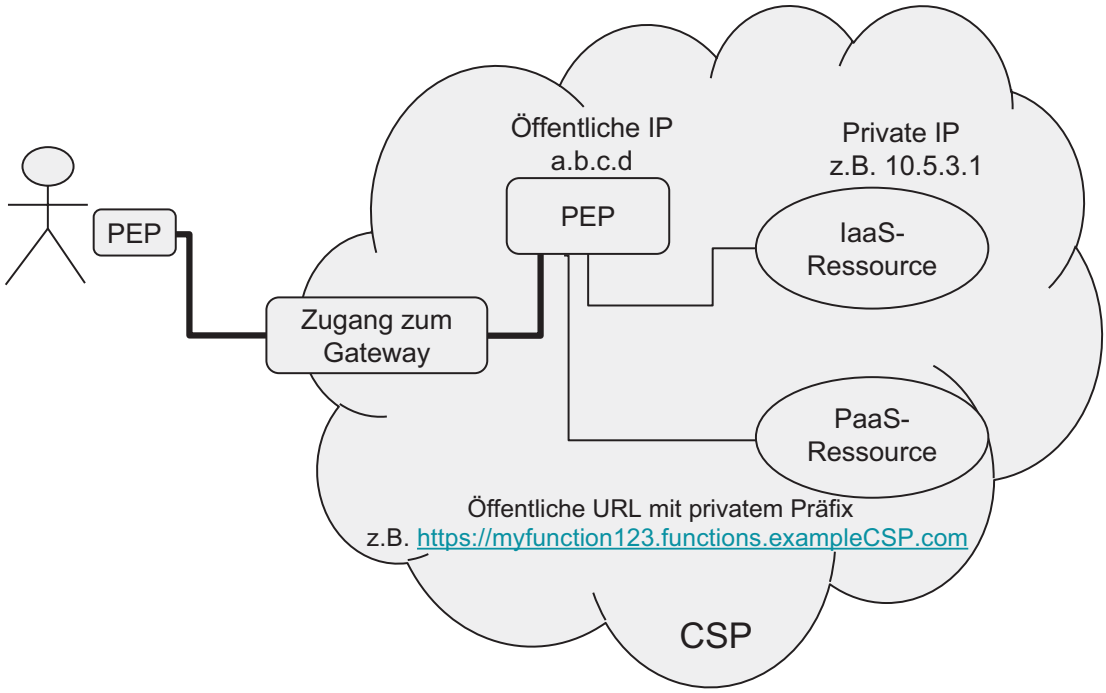

Abb. 14-1. *Cloud-Zugriffskontrolle über Co-located PEP*

Abb. 14-1 zeigt auch eine PaaS-Ressource, die über ein von Cloud-Plattformen häufig verwendetes Muster zugegriffen wird – eine öffentliche URL mit einer privaten Kennung als Präfix zur FQDN. Das Diagramm zeigt ein generisches Beispiel, https://myfunction123.functions.exampleCSP.com, während reale Beispiele aussehen wie https://abc123def.execute-api.us-east-1.amazonaws.com für eine AWS Lambda-Funktion, oder https://myapp1.azurewebsites.net/api/myfunction123 für eine Azure-Funktion.[2] In diesen Beispielen gibt es eine Reihe von öffentlichen IP-Adressen, die von vielen, vielen Funktionen geteilt werden, wobei die CSP-Infrastruktur das Load Balancing und die Zuordnung zu einem bestimmten Kundenkonto durchführt. Diese IP-Adressen und die Compute- und Netzwerkinfrastruktur, die sie bedienen, stehen unter Kontrolle des CSP und können von einem bestimmten Kunden nicht vorgeschaltet oder gestört werden. Aber das ist in Ordnung; tatsächlich steht es nicht im Widerspruch zu

[2]Obwohl diese ein bisschen wie „Sicherheit durch Obskurität“ wirken könnten, bedenken Sie, dass das Aufrufen dieser Dienste normalerweise auch einen API-Schlüssel erfordert, zusätzlich zur URL. Die Kombination mit einem PEP ist natürlich eine noch bessere Lösung.

unserem Zero Trust-Sicherheitsmodell. Dies liegt daran, dass, obwohl die IP-Adresse und der tatsächliche Netzwerkeinstiegspunkt öffentlich sind, CSPs die Möglichkeit bieten, die Quell-IP-Adressen einzuschränken, die berechtigt sind, eine bestimmte Funktion aufzurufen. Und natürlich würden wir in diesem Beispiel einfach konfigurieren, dass nur der Zugriff vom PEP erlaubt ist. Dies ist ein Beispiel dafür, wie man einige grundlegende Funktionen in einer Cloud-Umgebung – Einschränkungen der Quell-IP-Adresse – nutzen kann, um den Weg zum Zero Trust-Sicherheitsmodell zu öffnen.

Schließlich kann der PEP, da er lokal zur Cloud-Plattform gehört, API-Aufrufe machen, um Metadaten über die Ressourcen in der lokalen Cloud-Umgebung abzurufen, die verwendet werden, wenn der PEP Ziele (Ressourcen) für zugewiesene Richtlinien bestimmt. Ebenso kann der lokale PEP neu erstellte Dienstinstanzen über Unternehmens-Cloud-Konten erkennen und dynamisch (und automatisch) den richtigen Remote-Benutzern das richtige Zugriffslevel gewähren. Wie wir in unserem kommenden Kapitel über Richtlinien sehen werden, ist das Erkennen neuer Ressourcen und das Bewerten von Ressourcenattributen auf diese Weise eine wichtige Fähigkeit, die PEPs für Cloud-Umgebungen bereitstellen können.

Abb. 14-2 zeigt die Verwendung eines Remote-PEP – der in einer beliebigen Umgebung läuft (vor Ort oder in einer anderen Cloud-Umgebung, das spielt keine Rolle) – zur Durchsetzung der Zugriffskontrolle auf CSP-basierte Ressourcen. Diese Ressourcen könnten IaaS oder PaaS sein, wie in unseren vorherigen Beispielen, aber in jedem Fall müssen sie eine öffentliche IP-Adresse haben, weil sie (natürlich) remote zugegriffen werden. Wieder verwenden wir die grundlegende Funktionalität des CSP, um eine Einschränkung der Quell-IP-Adresse durchzusetzen, die verlangt, dass der gesamte Verkehr für diese Ressourcen von der öffentlichen IP-Adresse des PEP ausgeht. Wie im vorherigen Beispiel ermöglicht uns diese einfache Methode, die identitätszentrierten und dynamischen Zugriffskontrollen, die von unserem Zero Trust-Modell angetrieben werden, auf unsere CSP-basierten Ressourcen anzuwenden. Beachten Sie, dass das System mit dieser Topologie das native Anwendungsprotokoll vom PEP, durch das Zugangsgateway und zur Ressource verwendet, so dass es nur eine geeignete Wahl für verschlüsselte Protokolle ist.

Natürlich haben CSPs viele Netzwerk- und Sicherheitsfähigkeiten, die über das generische Zugangsgateway hinausgehen, das wir hier besprochen haben, wie Netzwerksicherheitsgruppen und IAM-Richtlinien. Mindestens können diese kombiniert werden, um Einschränkungen der Quell-IP-Adresse beim Zugriff auf

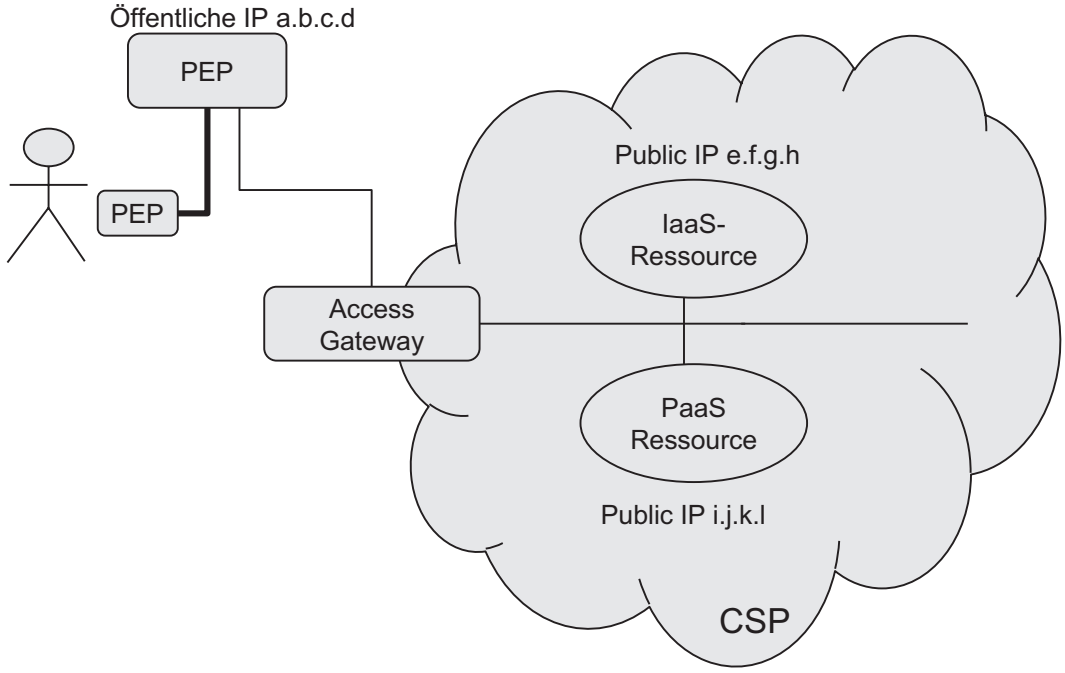

Abb. 14-2. *Cloud-Zugriffskontrolle über Remote PEP*

Ressourcen (Dienste) durchzusetzen, und sicherzustellen, dass sie nur von einem Zero Trust PEP aus zugegriffen werden können. Dies ist die grundlegende und ermöglichte Fähigkeit, um Cloud-Ressourcen in eine Zero Trust-Umgebung einzubeziehen.

In unserer vorherigen Diskussion haben wir (absichtlich) die Netzwerk-Topologie auf vereinfachte Weise dargestellt, um die Konzepte zu erklären; reale Cloud-Plattformen bieten mehrere Möglichkeiten, wie Sie Cloud-Ressourcen in Ihre Unternehmensnetzwerke integrieren können. Zum Beispiel bieten CSPs in der Regel ein „Direct Connect"-Modell für ein Site-to-Site-VPN an, das ein lokales Netzwerk logisch auf ein privates Cloud-Netzwerk über einen lokalen Telekommunikationsanbieter erweitert. CSPs bieten auch fortgeschrittenere Netzwerkverbindung- und Konfigurationsfähigkeiten, mit denen Sie komplexe Netzwerk-Topologien und ebenso komplexe Zugriffskontrollmechanismen erstellen können. Wir empfehlen jedoch, dass Sie die Dinge einfach halten und die dynamischen und identitätszentrierten Zugriffskontrollen auf Ihre Zero Trust-Plattform auslagern. Das ist es, was Zero Trust gut

kann, und es hilft Ihnen, die Erstellung dessen zu vermeiden, was sich wahrscheinlich als neues, komplexes und CSP-spezifisches Sicherheitsmodell herausstellen wird. Die CSP-Modelle, obwohl leistungsfähig, sind eher netzwerk- und IP-adressenzentriert als identitätszentriert. Und sie haben definitiv nicht die Fähigkeit, die Arten von Zero Trust-Richtlinien zu definieren und durchzusetzen, die wir in unseren heterogenen und vielfältigen Unternehmensumgebungen benötigen.

Natürlich gibt es Ausnahmen zu jedem Ratschlag, und wir erkennen an, dass es weder möglich noch angemessen ist, Ihr Zero Trust-System in jeden Teil Ihrer Umgebung zu zwingen. Tatsächlich ist ein Teil einer erfolgreichen Zero Trust-Reise zu wissen, wo man Grenzen zieht. Letztendlich müssen Sie sicherstellen, dass Sie die am besten geeignete und effektivste Sicherheitsplattform, Tools und Prozesse für jeden Teil Ihrer Umgebung auswählen.

Ein gutes Beispiel dafür ist das Service Mesh, das ein Mechanismus zur Bereitstellung und Verwaltung von containerisierten Arbeitslasten auf zuverlässige und skalierbare Weise ist. Service Meshes sind in gewisser Weise im Wesentlichen ein eigenständiges Zero Trust-Mikrosegmentierungsmodell und -system. Lassen Sie uns einen Blick darauf werfen, wie sie funktionieren und wie Sie sie in Ihr breiteres unternehmensweites Zero Trust-System einbinden könnten.

Service Meshes

Service Meshes sind ein neuer und schnell wachsender Ansatz zur Bereitstellung von containerisierten Arbeitslasten im großen Maßstab. Obwohl sie nicht grundsätzlich auf der Cloud basieren (die Open-Source-Meshes können absolut vor Ort bereitgestellt werden), haben wir sie am häufigsten in Cloud-Umgebungen gesehen. Service Meshes, wie zum Beispiel *Istio* und *Linkerd*, eignen sich sehr gut für die moderne DevOps-Stil Microservices-basierte Anwendungsentwicklung.

Service Meshes sind Plattformen für den Betrieb, die Steuerung und das Management von groß angelegten containerisierten (Microservices) Arbeitslasten, mit einem Schwerpunkt auf der Verwaltung der Kommunikation zwischen Microservices. Zum Beispiel besagt die Istio-Dokumentation: „Ohne Änderungen an den zugrunde liegenden Diensten bietet Istio automatisierte Basis-Verkehrsresilienz, Sammlung von Dienstmetriken, verteiltes Tracing, Verkehrsverschlüsselung, Protokoll-Upgrades und

erweiterte Routing-Funktionen für alle Dienst-zu-Dienst-Kommunikation.„[3] Die Linkerd-Dokumentation sagt

> *Es fügt Beobachtbarkeit, Zuverlässigkeit und Sicherheit zu Cloud-nativen Anwendungen hinzu, ohne Code-Änderungen zu erfordern. Zum Beispiel kann Linkerd Erfolgsraten und Latenzen pro Dienst überwachen und melden, kann fehlgeschlagene Anfragen automatisch erneut versuchen und kann Verbindungen zwischen Diensten verschlüsseln und validieren, alles ohne jegliche Modifikation der Anwendung selbst.*[4]

Was an diesen Ansätzen interessant ist, ist, wie sie eine reiche Auswahl an Bereitstellungs-, Kommunikations- und Laufzeitdiensten für Microservices durch eine konfigurationsbasierte Plattform bieten. Wie das Versprechen von Anwendungsservern (App Servern) aus den späten 1990er Jahren, befreit dies Entwickler dazu, sich auf die Geschäftslogik anstatt auf die Infrastruktur zu konzentrieren. Natürlich ist die heutige Technologie erheblich anders als die der 1990er Jahre, und auch der Service-Mesh-Ansatz zur Sicherheit hat sich weiterentwickelt. Lassen Sie uns nun einen Blick auf die interne Struktur eines Service-Mesh (wir haben Istio als Beispiel gewählt) werfen, um zu sehen, wie es gut mit dem Zero Trust Microsegmentation-Modell abgestimmt ist.

Die High-Level Istio Mesh-Architektur ist in Abb. 14-3 dargestellt, die wir aus einer Zero Trust Sicherheitsperspektive betrachten werden.

Das Erste, was zu beachten ist, ist die vertraute Trennung zwischen der Steuerungsebene und der Datenebene und eine Reihe von verteilten Proxies, einer vor jedem Dienst. Diese Proxies fungieren, wenig überraschend, als Policy Enforcement Points (PEPs). Die Istiod-Dienste sind der Policy Decision Point (PDP) in der Steuerungsebene und bieten Kernsicherheitsfunktionen, einschließlich der Funktion als systemeigene Zertifizierungsstelle, Dienstidentitätsmanagement und Speicherung und Bewertung von Authentifizierungs- und Autorisierungspolicen. Die Proxies stellen sicher, dass die Kommunikation von Dienst zu Dienst über einen mTLS-Kanal erfolgt, der Vertraulichkeit sowie Authentifizierung des Dienstanbieters und des Dienstnutzers bietet.

Das Istio Sicherheitsmodell basiert auf einem deklarativen Policymodus, der Dienstattribute (wie Namespaces und Labels) als Subjektkriterien verwendet, um zu bestimmen, welche Policen auf welche Dienste anzuwenden sind. Das

[3] https://istio.io/latest/faq/general/.
[4] https://linkerd.io/2/faq/#what-is-linkerd.

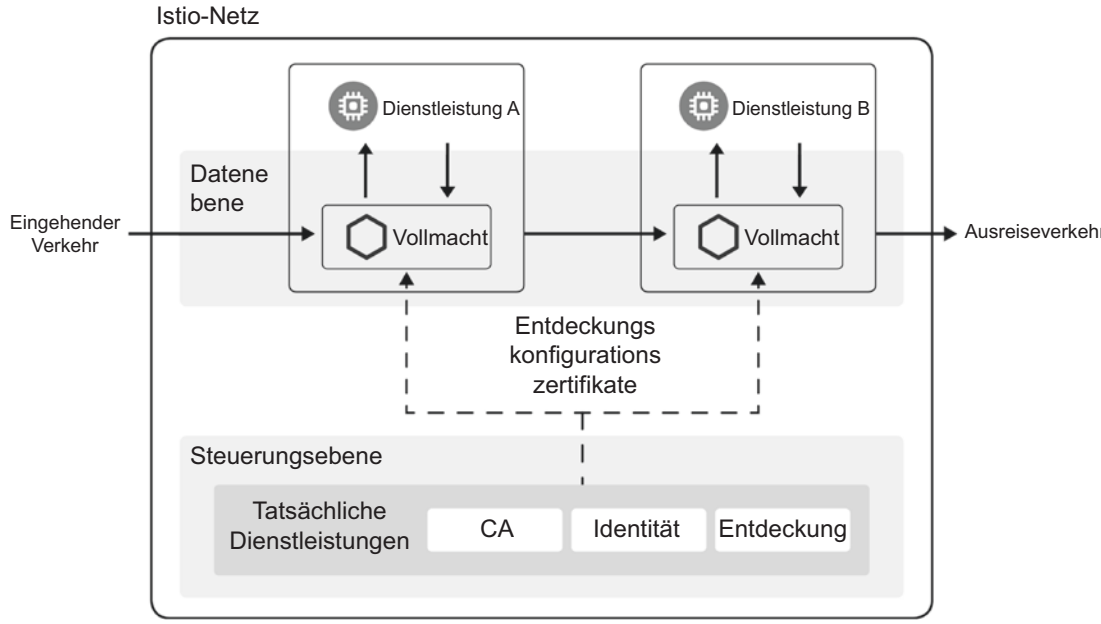

Abb. 14-3. *Istio Architektur*[5]

Autorisierungsmodell lässt den Proxy (PEP) Anfragen auf der Grundlage von Attributen des Anfragenden, des Zielservices und der Metadaten und Headerinformationen der Anfrage bewerten. Beachten Sie, dass innerhalb des Meshes Anfragende und Dienste durch Dienstidentifikatoren und nicht durch IP-Adressen angesprochen werden – tatsächlich teilen sich in vielen Fällen diese Dienste alle die gleichen IP-Adressen, die daher aufhören, ein bedeutendes Attribut zu sein, mit dem sie unterschieden werden können.

Wir haben hier nur eine kurze Einführung in Service Meshes und ihre Sicherheitsmodelle gegeben, aber es sollte ausreichen, um Sie davon zu überzeugen, dass es sich um gut durchdachte und kohärente Plattformen mit internen Sicherheitsrichtlinien und Durchsetzungsmodellen handelt (zugegeben, mit unterschiedlichen Grad an Unterstützung für identitätszentrierte und kontextbasierte Policen). Service Meshes sind gute Beispiele für Sicherheitssysteme, die genug eigenes „Schwerkraftzentrum“ haben, um ihren fortgesetzten Unternehmenseinsatz zu rechtfertigen, auch innerhalb eines breiteren Zero Trust-Programms. Dies sollte im

[5]Siehe https://istio.io/latest/docs/concepts/what-is-istio/ für weitere Informationen.

klaren Kontrast zu Diensten wie IaaS stehen, die im Allgemeinen grundlegende netzwerkzentrierte Sicherheitskontrollen haben und durch die Zero Trust-Plattform des Unternehmens geschützt werden müssen, anstatt durch das Cloud-native Modell.

Glücklicherweise definieren Service Meshes eine klare Grenze für ihren Anwendungsbereich – den Rand des Meshes – und können sehr einfach und effektiv eine umgebende Zero Trust-Plattform zur Durchsetzung von Ein- und Ausgangspolicen nutzen. Dies macht Service Meshes besonders gut geeignet für die Integration mit Zero Trust-Systemen, die externe PEPs verwenden, insbesondere die Enklaven-basierten und Cloud-gerouteten Modelle. In diesen Situationen wird das Mesh aus der Perspektive des Zero Trust-Systems zur impliziten Vertrauenszone.

Was wir beschrieben haben (und was heute vollständig erreichbar ist), ist im Wesentlichen eine Armlängen-Bereitstellung eines breiten unternehmensweiten Zero Trust-Systems Seite an Seite mit einem Service Mesh. Es wird interessant sein zu sehen, hoffentlich in naher Zukunft, eine Zero Trust-Lösung, bei der der PEP in der Lage ist, Policen auf der Grundlage von Arbeitslastattributen innerhalb der Containerumgebung zu rendern, und den externen Zugriff auf containerisierte Arbeitslasten zu steuern. Dies würde nur eine grundlegende Möglichkeit erfordern, die Container-Arbeitslastattribute im Zero Trust-Policymodell darzustellen und Zugriffskontrollentscheidungen zur Durchsetzung in das Mesh zu übertragen. Einige dieser Verbindungen existieren bereits; zum Beispiel ist es derzeit möglich, Zero Trust-Kontext in Istio über HTTP-Anforderungsheader zu übertragen. Diese Art von Integration wird interessant und wertvoll sein, wenn Organisationen in höhere Reifegrade mit ihren Zero Trust-Programmen voranschreiten.

Zusammenfassung

Es ist klar, dass IaaS und PaaS in ihrer Bedeutung und Auswirkung auf die Entwicklung und Bereitstellung von Unternehmensanwendungen weiterhin wachsen werden. Diese Plattformen haben die Breite und Tiefe ihrer Fähigkeiten dramatisch erweitert und tatsächlich sogar die Möglichkeit eingeführt, bestimmte Cloud-verwaltete Dienste vor Ort auszuführen. Dies ist hauptsächlich auf die allgegenwärtige Netzwerkkonnektivität und äußerst kostengünstige Rechen- und Speicherkapazitäten zurückzuführen. Dies, kombiniert mit ausgeklügelter Steuersoftware, hat zu einer Erweiterung dessen geführt, was wir in den letzten Jahren als „as a Service“-Angebote betrachten. Die Vorstellung,

servicebasierte (und Cloud-verwaltete) Rechen- oder Sensorknoten direkt in ein Unternehmensnetzwerk zu integrieren, wird immer häufiger, wobei große CSPs in diesem Bereich Innovationen vorantreiben. Dieser Trend wird etwas humorvoll als „Fog Computing“ bezeichnet.[6] Es wird sehr interessant sein zu sehen, wie sich diese Angebote und Architekturen aus Sicherheitsperspektive weiterentwickeln – klar ist, dass diese verteilten Rechenelemente eine verteilte Sicherheit benötigen und es wird die Möglichkeit geben, sie mit Unternehmens- und CSP-basierten Zero Trust-Plattformen zu integrieren.

Unternehmensanwendungsarchitekturen entwickeln sich ebenfalls schnell weiter, um die neuen IaaS- und PaaS-Fähigkeiten zu nutzen, und Sicherheitsteams müssen dies nicht nur verfolgen, sondern führen und ermöglichen. Wir glauben, dass eine Zero Trust-Architektur und -Plattform der beste Weg sind, dies zu erreichen.

Die in diesem Kapitel besprochenen Prinzipien und Konzepte sollten Ihnen ein klares Verständnis dafür vermitteln, wie Sie die Sicherung von IaaS- und PaaS-Bereitstellungen im Rahmen Ihrer Zero Trust-Initiative angehen und wie Sie serviceorientierte Anwendungen unterstützen können. Um unsere Analyse von Zero Trust und Cloud-basierten Systemen abzuschließen, untersucht das folgende Kapitel SaaS-Anwendungen.

[6] Weil es eine Wolke ist, die sehr nahe bei Ihnen ist. Machen Sie uns nicht für das Wortspiel verantwortlich, wir haben es nicht erfunden.

KAPITEL 15

Software als Dienst

Cloud-basierte Software, die als Dienst (SaaS) bereitgestellt wird, ist natürlich ein wichtiger Bestandteil der heutigen IT- und Geschäftsumgebung und hat einen tiefgreifenden Einfluss darauf, wie kommerzielle Software erstellt und genutzt wird. Diese Veränderung hat es bemerkenswert einfacher und leichter gemacht, anspruchsvolle Geschäftssoftware zu nutzen, da Unternehmen sich jetzt anmelden, ein Konto erstellen und innerhalb von Minuten einen Mehrwert erzielen können.

Wir definieren SaaS als eine öffentlich zugängliche Webanwendung,[1] bei der der Dienstanbieter (Verkäufer) die Infrastruktur hostet, verwaltet und wartet und mit der der Abonnent (und verwaltet) die zugewiesene Anwendungsfunktion über das Internet ausführt. SaaS-Anwendungen sind in der Regel aus Effizienzgründen mehrmandantenfähig, wobei jeder Abonnent nur auf seine privaten Daten zugreifen kann.

Aus der Perspektive der Zero Trust-Sicherheit können wir sofort einige wichtige Unterschiede zwischen SaaS und den IaaS/PaaS-Ressourcen erkennen, die wir im vorherigen Kapitel besprochen haben. Zunächst und vor allem sind SaaS-Anwendungen *öffentlich* zugänglich, und jeder Benutzer im Internet kann über eine HTTPS-Verbindung auf sie zugreifen. Das heißt, die Zugangspunkte zu einem SaaS-System sind per Definition öffentlich und nicht privat. Und sie sind nur über eine verschlüsselte Verbindung zugänglich. Das bedeutet, dass bei SaaS-Anwendungen keine Ressourcenverstecke durch einen PEP benötigt werden (da dies kein Ziel für SaaS ist) und keine Verschlüsselung des Netzwerkverkehrs erforderlich ist (da bereits HTTPS verwendet wird).

Dies wirft natürlich die Frage auf, ob und wie Zero Trust noch relevant für SaaS-Ressourcen ist. Wir glauben, dass die Verwendung von Zero Trust zur Verwaltung und

[1]Viele SaaS-Anwendungen können und bieten neben einer Browser-Benutzeroberfläche auch Nicht-Web-Schnittstellen, wie APIs, an.

J. Garbis und J. W. Chapman, *Zero Trust Sicherheit*, https://doi.org/10.1007/979-8-8688-0105-1_15

Kontrolle des Zugriffs auf SaaS-Anwendungen einen Wert hat, obwohl wir anerkennen, dass Zero Trust weniger Dinge für SaaS-Ressourcen im Vergleich zu privaten Ressourcen tut. Insbesondere kann Zero Trust auch für öffentlich zugängliche SaaS-Anwendungen identitätszentrierte und kontextsensitive Zugriffsrichtlinien durchsetzen. Da das PDP mit Identitätsanbietern und anderen Unternehmenssystemen integriert ist, kann es Gruppenmitgliedschaften sowie Identitäts-, Geräte- und Gesamtsystemattribute zur Zugriffskontrolle verwenden, genau wie es für private Ressourcen kann. Während viele (aber nicht alle) SaaS-Anwendungen sicherlich mit Identitätsanbietern für die Authentifizierung integrieren können, verwenden sie in der Regel noch keine Geräte-, Identitäts- oder Systemattribute zur Zugriffskontrolle.

Natürlich ist die Sicherheit von SaaS-Anwendungen breiter als nur Zugriffskontrolle, und die Sicherheitsbranche hat ein Ökosystem von Sicherheitsangeboten für SaaS entwickelt, einschließlich Secure Web Gateways (SWG) und Cloud Access Security Brokers (CASB), unter anderem. Lassen Sie uns diese betrachten und untersuchen, wie sie sich auf Zero Trust beziehen.

SaaS und Cloud-Sicherheit

Um über Zero Trust und SaaS zu sprechen, müssen wir die Hauptkomponenten der Cloud-Sicherheit untersuchen. Wir beginnen mit der Betrachtung der nativen SaaS-Sicherheitskontrollen und untersuchen dann die Bereiche Secure Web Gateway und Cloud Access Security Broker.

Native SaaS-Kontrollen

Obwohl sie öffentlich verfügbar sind, erkennen und bestätigen SaaS-Anbieter die Notwendigkeit, eine gewisse Zugriffs- und Netzwerksicherheit um ihre Lösung zu haben. Natürlich haben sie Mechanismen eingesetzt, um ihre Dienste vor Internet-Angriffen wie DDoS zu schützen, und haben interne Systeme, um die Integrität und Verfügbarkeit ihrer Plattform zu erhalten. Darüber hinaus bieten viele SaaS-Systeme Unternehmen zwei eingebaute Zugriffskontrollmechanismen. Der erste ist die gleiche grundlegende Netzwerkzugriffskontrollfähigkeit wie bei IaaS- und PaaS-Plattformen – die Möglichkeit, Quell-IP-Adressbeschränkungen durchzusetzen. Der zweite ist das föderierte Identitätsmanagement, bei dem das SaaS-System die Benutzerauthentifizierung an einen externen Identitätsanbieter delegiert. Lassen Sie uns jeden einzelnen besprechen.

In Bezug auf Quell-IP-Adressbeschränkungen implementieren SaaS-Plattformen dies notwendigerweise etwas anders als IaaS/PaaS, insofern sie die Quell-IP-Adressregel nur für Benutzer durchsetzen, die mit einem bestimmten Konto verbunden sind. Zum Beispiel kann jeder Benutzer auf dem Planeten die `https://MySaaSApp.com/login` Seite erreichen, aber die SaaS-Plattform wird nur Benutzern aus der mycompany.com-Domain erlauben sich anzumelden, wenn ihr Verkehr von der festgelegten IP-Adresse ausgeht. Dies ist im Wesentlichen eine Authentifizierungszugriffskontrollrichtlinie, die auf die Mietverhältnisse eines bestimmten Kunden innerhalb der SaaS-Plattform angewendet wird. Diese Fähigkeit kann verwendet werden, um den Zugriff über ein traditionelles VPN oder ein Zero Trust-System zu erfordern – beide leiten den Benutzerverkehr durch ein unternehmensgesteuertes Netzwerk mit einem bekannten IP-Adressausgangspunkt.

Beim föderierten Identitätsmanagement nutzt die Anwendung einen externen Identitätsanbieter für die Benutzer*authentifizierung,* durch standardisierte Mechanismen wie SAML und OpenID Connect. Effektiv ist dies eine weitere Möglichkeit, identitätszentrierte Aspekte von Zero Trust-Zugriffskontrollen durchzusetzen, die (interessanterweise) unabhängig von der Netzwerksicherheit sind. Aus technischer Sicht können Benutzer sich nicht direkt in die SaaS-Anwendung authentifizieren – die SaaS-App holt entweder ein aktuelles Authentifizierungstoken aus dem Browser des Benutzers oder leitet den Browser zur Authentifizierung an den Identitätsanbieter weiter. Dies verwendet natürlich die Authentifizierungsfaktoren und Kontextkontrollen, die im Identitätsanbieter konfiguriert sind. Beachten Sie, dass dies im Allgemeinen nur mit der Authentifizierung verbunden ist. SaaS-Anwendungen verlassen sich immer noch weitgehend auf interne *Autorisierungs*modelle, bei denen Benutzer verschiedenen Rollen zugewiesen werden, die ihre Berechtigungen innerhalb der Anwendung steuern. Die meisten SaaS-Anwendungen haben derzeit keine Mechanismen, um externe Kontextinformationen zu verbrauchen und Autorisierungsentscheidungen auf dieser Grundlage zu treffen – dies ist ein fortgeschrittenerer und zukunftsorientierter Anwendungsfall, auf den wir in der Zusammenfassung dieses Kapitels noch einmal eingehen werden. Beachten Sie schließlich, dass es keinen Grund gibt, warum diese beiden Ansätze nicht kombiniert werden können – zum Beispiel die Verwendung eines föderierten Identitätssystems zur Authentifizierung in Kombination mit einer Zero Trust-Netzwerklösung zur Durchführung tiefer Geräteposture-Checks.

Als nächstes werden wir uns CASBs und SWGs ansehen, zwei wichtige Bereiche innerhalb der Cloud-Sicherheit, die Unternehmen nutzen, um Sichtbarkeit und Kontrolle über den Benutzerzugriff auf SaaS-Anwendungen zu erhalten. Interessanterweise gibt es einen zunehmenden Grad an Überschneidung und Konvergenz zwischen diesen zuvor getrennten Markt Segmenten, und tatsächlich ist dies Teil eines größeren Trends zur Konsolidierung einer breiten Palette von Netzwerk- und Sicherheitsfunktionen in ein integriertes Serviceangebot (der Secure Access Service Edge).

Sichere Web-Gateways

Sichere Web-Gateways, die entweder vor Ort oder als Cloud-basierter Dienst bereitgestellt werden können, bieten Unternehmen eine Möglichkeit, zu kontrollieren, auf welche Websites ihre Benutzer zugreifen können, und einen gewissen Grad an Antimalware- und Bedrohungsschutz durchzuführen. SWGs führen in der Regel eine TLS-Beendigung durch und fungieren als Man-in-the-Middle-Web-Proxy, um den Inhalt des Verkehrs zu inspizieren. Einige SWGs verwenden Endpunkt-Agenten, um Internet-gebundenen Verkehr zu erfassen (und um zusätzliche Dienste bereitzustellen). Vor-Ort-Unternehmens-SWGs verlieren an Beliebtheit und werden in der Regel durch Cloud-basierte SWG-Dienste ersetzt.

Das SWG-Richtlinienmodell ist in gewisser Weise das Gegenteil des Zero Trust-Modells – es soll den Zugriff auf verbotene Internetziele blockieren, anstatt dem Zero Trust-Modell zu folgen, das nur den Zugriff auf ausdrücklich erlaubte Ziele zulässt. Das heißt, SWGs arbeiten in der Regel im „Standard Allow"-Modus, was in den meisten Fällen sinnvoll ist, da das Volumen und die Breite der Seiten im Internet nahezu unendlich ist.

SWG sind in der Regel mit Unternehmensidentitätsanbietern für die Benutzerauthentifizierung integriert und können Attribute wie Gruppenmitgliedschaften verwenden, um verschiedene Zugriffskontrollrichtlinien durchzusetzen. SWGs allein bieten jedoch keine Netzwerksicherheit oder Fernzugriff auf private Ressourcen – dies ist einfach nicht im Rahmen des Problems, das sie lösen sollen. Beachten Sie, wie wir im folgenden Text besprechen werden, dass einige der Cloud-basierten SWG-Anbieter ihr Serviceangebot erweitert haben, um auch Zero Trust-ähnliche Zugriffskontrollen für private Ressourcen zu umfassen.

Cloud Access Security Broker

CASBs werden in der Regel von Unternehmen verwendet, um das Problem des „Shadow IT“ zu lösen, bei dem Geschäftsteams SaaS-basierte Anwendungen außerhalb der Sichtbarkeit und Kontrolle der IT nutzen. CASBs lösen dieses Problem, indem sie die Nutzung von SaaS-Anwendungen entdecken und melden und eine entsprechende Reihe von Anwendungsrisiko- und Compliance-Bewertungsfähigkeiten bereitstellen. Sie bieten auch Wert, indem sie DLP-Kontrollen auf den SaaS-basierten Daten durchsetzen und oft einige Benutzeridentitäts- und gerätebasierte Zugriffsrichtlinien einbeziehen, in der Regel in Verbindung mit SAML- oder OpenID Connect-basierten Identitätsanbietern.

Es ist interessant, über CASBs nachzudenken, die adaptive und risikobasierte Authentifizierung und Autorisierung durchführen, indem sie Identitäts- und Geräteattribute verwenden. Aus dieser Perspektive scheinen sie definitiv als Zero Trust-Richtliniendurchsetzungspunkte zu agieren, obwohl natürlich ihr Durchsetzungsmodell auf SaaS-Anwendungen ausgerichtet ist, so dass sie keine Netzwerksicherheitsfunktionen bereitstellen. CASBs sind auch nicht dafür konzipiert oder implementiert, Zugriffskontrollen für private oder vor Ort befindliche Anwendungen bereitzustellen, so dass ihre Richtlinien- und Durchsetzungsmodelle diese Arten von Funktionen nicht enthalten. Wie die SWG-Anbieter, die wir zuvor erwähnt haben, haben auch Anbieter, die im CASB-Bereich begonnen haben, ihre Plattformfähigkeiten in andere Funktionsbereiche erweitert. Wir werden später auf die Branchenkonvergenz eingehen, nachdem wir Zero Trust und SaaS diskutiert haben.

Zero Trust und SaaS

Es sollte offensichtlich sein, dass Zero Trust-Sicherheit auf SaaS-Anwendungen angewendet werden kann und gut mit ihnen funktioniert, unabhängig davon, ob Ihre gewählte Sicherheitsarchitektur einen SWG, einen CASB oder keinen von beiden beinhaltet. Zero Trust-Sicherheitssysteme können identitäts- und kontextsensitive Zugriffskontrolle für SaaS-Anwendungen bereitstellen, solange die SaaS-Plattform IP-Adressbeschränkungen bietet und solange das Zero Trust-System kompatibel ist mit der Definition von SaaS-Anwendungen als Ziele innerhalb des Policy-Modells und der Erfassung des für sie bestimmten Verkehrs.

SWG und CASB werden weiterhin nützlich sein, auch in Verbindung mit einem Zero Trust-System, obwohl Unternehmen sich bewusst sein müssen, wie diese verschiedenen Systeme mit Verkehr und Netzwerkrouting arbeiten und sie manipulieren. Unternehmen könnten beispielsweise den Ansatz verfolgen, ihr Zero Trust-System nur zur Kontrolle des Zugriffs auf private Ressourcen zu verwenden, während sie einen SWG und/oder CASB für ihre SaaS-Anwendungen verwenden. Dies ist ein vernünftiger Ansatz.

Zero Trust und Edge Services

Derzeit gibt es einen Trend auf dem Markt hin zu einer konvergierten und cloudbasierten Netzwerk- und Sicherheitslösung, die viele dieser Funktionen zusammenfasst. Gartner nennt dies den *Secure Access Service Edge* (SASE), während Forrester's Variante als *Zero Trust Edge* bezeichnet wird. Effektiv beschreiben diese, wie cloudbasierte Sicherheits- und Netzwerkanbieter mehrere funktionale Angebote in eine einzige as-a-service Plattform integriert haben. Typische Funktionen innerhalb dieser Plattform umfassen Netzwerk (SD-WAN, WAN-Optimierung, QoS, unter anderem) und Sicherheit (Firewall, IDS/IPS, SWG, CASB, DNS-Filterung und Zero Trust Network Access).

Das Bewusstsein und Interesse von Unternehmen an SASE und ZTE hat zweifellos in jüngster Zeit erheblich zugenommen, und es gab entsprechende Aktivitäten mit erhöhter Unterstützung durch Anbietermarketing, Innovation und Branchenkonsolidierung (Übernahme). Einen Schritt zurückgehend bieten diese konvergierten Plattformen drei Hauptgruppen von Funktionen:

- Netzwerkkonnektivität
- Sicherheit für den Internetzugang (Ausgangszugang)
- Zugang zu privaten Ressourcen (Zero Trust Network Access oder Eingangszugang)

Aus unserer Sicht ist besonders interessant und anders der Zero Trust Network Access (ZTNA) Teil davon. Dies liegt daran, dass selbst wenn das Netzwerkmanagement und die Analyse und Sicherheit des Internetverkehrs in eine Cloud-Umgebung verlagert werden, ZTNA weiterhin erfordern wird, dass Elemente (PEPs) in von Unternehmen kontrollierten Umgebungen bereitgestellt werden, einschließlich On-Premises-Unternehmensnetzwerken, Rechenzentren und öffentlichen Cloud-basierten IaaS- und

PaaS-Umgebungen. Dies liegt an zwei Gründen. Erstens erfordern TCP/IP-Netzwerke einen lokalen Knoten, der als eines Ende des verschlüsselten Netzwerktunnels fungiert und entfernte Verbindungen zu privaten Ressourcen im privaten Netzwerk vermittelt oder proxyt. Zweitens ist der lokale Knoten erforderlich, um Kontext und Attribute von lokalen Ressourcen als Teil der Zugriffsrichtlinienentscheidungskriterien zu erhalten und zu verwenden (wir werden dies in Kap. 17 genauer behandeln, wo wir uns auf Policy-Modelle konzentrieren).

Die Anforderung an eine Reihe von Knoten in lokalen privaten Netzwerken – unsere Zero Trust PEPs – ist einer der Gründe, warum wir glauben, dass ZTNA nicht auf die gleiche Weise wie die anderen SASE Komponenten angegangen werden sollte. Der andere Grund ist, dass eines unserer Kernprinzipien darin besteht, dass das Zero Trust-Identitäts- und kontextsensitive Sicherheitsmodell für den Zugriff aller Identitäten auf alle Ressourcen durchgesetzt werden muss, unabhängig vom Standort der Identität oder Ressource. Obwohl Organisationen intensiv SaaS-Anwendungen nutzen und viele Benutzer auf Homeoffice umgestellt haben, haben sie immer noch Benutzer vor Ort und Ressourcen vor Ort. Sie müssen auch den Zugriff von Server zu Server vor Ort kontrollieren, was cloudbasierte Dienste oft schwer zu verwalten finden. Insgesamt sind all diese Gründe der Grund, warum Gartner beispielsweise „Ingress SASE“ von „Egress SASE“ unterscheidet, mit unterschiedlichen Anforderungssätzen.

In jedem Fall handelt es sich hierbei um einen sich schnell entwickelnden Bereich, und wir glauben, dass es eine Möglichkeit gibt, dass diese aufkommenden cloudbasierten Sicherheitsplattformen sich mit Zero Trust-Kontext integrieren und ihn nutzen, ob er von ihrer eigenen Plattform bereitgestellt wird oder durch Integration mit dem Angebot eines anderen Anbieters.

Zusammenfassung

Lassen Sie uns darüber nachdenken, wie SaaS und Zero Trust-Sicherheit in der nicht allzu fernen Zukunft aussehen könnten. Zuerst (und wir geben zu, dass dies keine besonders kühne Vorhersage ist), glauben wir, dass Identität und daher Identitätsanbieter im Zentrum von Zero Trust bleiben werden. Wir glauben jedoch, dass diese Anbieter nicht nur als autoritative Verzeichnisse und Authentifizierungspunkte dienen, sondern als „Zentren der Schwerkraft“ für den Benutzerzugriff auf Web-Apps und für Zugriffskontrollmodelle. Ein klares Beispiel dafür sind heute die Zugriffsportale,

die viele IdPs bereitstellen, mit Startsymbolen für den Zugriff auf SaaS-Anwendungen. Heute bieten diese Portale hauptsächlich nur Authentifizierung und Zugriff, aber wir glauben, dass es eine Möglichkeit für Identitätsanbieter gibt, die Breite und Leistungsfähigkeit ihrer Policy-Modelle über die Authentifizierung hinaus zu erweitern und die Autorisierung einzubeziehen.

Zum Beispiel könnten SaaS-Anwendungen beginnen, die Bereitstellung von Konten oder Rollen als Teil einer Just-in-Time (JIT) Zugriffsinitiative weitgehend zu unterstützen, unter Verwendung eines Standards wie SCIM.[2] SCIM ist jedoch nur ein erster Schritt, und es wird interessant sein zu sehen, ob und wie ein Standard (ob formell oder informell) entsteht, wie die Autorisierung dargestellt wird.[3] Wir glauben nicht, dass Anwendungen jemals ihre Autorisierung vollständig externalisieren werden, was tatsächlich einer der Gründe ist, warum XACML keine weit verbreitete Branchenakzeptanz erlangt hat. Wir glauben jedoch, dass wir eine allgemein akzeptierte Methode sehen werden, um authentifizierten (und daher vertrauenswürdigen) Identitätskontext an SaaS-Anwendungen zu definieren und zu kommunizieren, die sie in einer für ihre Umgebung geeigneten Weise konsumieren und verwenden können. JIT-Zugriffsprovisionierung ist tatsächlich ein enges Beispiel dafür.

Ohne Zweifel wird dies ein interessanter und dynamischer Bereich sein, den man beobachten sollte, wie Zero Trust-bewusste SaaS-Anwendungen sein können und welchen Sicherheits-, Betriebs- und Geschäftswert dies bringen wird. Im Laufe der Zeit glauben wir, dass diese Fähigkeiten auch auf Nicht-SaaS-Anwendungen „heruntertrickeln“ werden, aber angesichts ihrer ausgefeilten Föderationsfähigkeiten und Investitionen in ihre Plattformen erwarten wir, dass SaaS-Anbieter den Weg ebnen werden.

[2]SCIM ist das System für Cross-Domain Identity Management. Siehe https://tools.ietf.org/html/rfc7642.

[3]Oder, zum Beispiel, wenn Zero Trust, Identität und SaaS-Systeme beginnen, bestehende Standards wie XACML, die eXtensible Access Control Modeling Language, zu verwenden.

KAPITEL 16

IoT-Geräte und „Dinge“

In diesem Buch lag unser Hauptaugenmerk darauf, den Zugriff von authentifizierten Entitäten – nämlich Benutzern und Servern – zu kontrollieren. Was sie beide gemeinsam haben, ist, dass sie gegen ein Identitätssystem authentifiziert sind, Attribute oder Rollen für den Kontext haben und moderne Geräte mit voll funktionsfähigen Betriebssystemen verwenden, die die Installation von Drittanbietersoftware unterstützen. Dies macht diese Systeme gut geeignet für die Integration in die Art von Zero Trust-Architekturen, über die wir gesprochen haben. Natürlich sind dies nicht die einzigen Arten von Geräten – es gibt Milliarden von vernetzten Geräten völlig unterschiedlicher Art, die auf weniger leistungsfähiger und weniger erweiterbarer Hardware und Softwareplattformen laufen, oft als *Internet der Dinge* (IoT) Geräte bezeichnet. Diese Geräte existieren oft auf denselben Unternehmensnetzwerken wie die wertvollsten Ressourcen der Organisationen. Sie sind auch dafür bekannt, Sicherheitslücken aufzuweisen und eine einladende Angriffsfläche darzustellen, und sollten in jede Zero Trust-Sicherheitsarchitektur einbezogen werden.

Diese IoT-Geräte decken eine breite Palette von Funktionen, Fußabdrücken und Fähigkeiten ab, und wir schließen bewusst eine breite Palette in unsere Diskussion hier ein. Wir betrachten diese Kategorie von IoT-Geräten und „Dingen“ als neuere vernetzte Geräte sowie traditionellere Geräte, die in Unternehmensnetzwerken existieren. Zum Beispiel

- Drucker
- VOIP-Telefone
- IP-Kameras
- Ausweisleser
- „Intelligente“ Dinge, wie Tafeln, Glühbirnen, usw.

J. Garbis und J. W. Chapman, *Zero Trust Sicherheit*, https://doi.org/10.1007/979-8-8688-0105-1_16

- Medizinische oder diagnostische Geräte in Gesundheitsnetzwerken
- HVAC-Systeme

Wir möchten auch andere Arten von Geräten berücksichtigen, die möglicherweise an weit verteilten Standorten betrieben werden und sich in öffentlichen oder zellularen Netzwerken befinden, wie zum Beispiel

- Umweltsensoren
- Fernüberwachungskameras
- Maschinen- oder Fahrzeugsensoren oder Aktuatoren

Und schließlich gibt es Betriebstechnik (OT) Systeme, die sich auf industrielle Automatisierung und Management konzentrieren und in den letzten 10–15 Jahren auf standardisierte und interoperable TCP/IP-Netzwerke umgestiegen sind und häufiger mit Unternehmens-IT-Netzwerken verbunden werden. Zero Trust-Architekturen können auf OT-Umgebungen angewendet werden, obwohl sie einige Unterschiede und Herausforderungen im Vergleich zu IT-Umgebungen haben. Unser Fokus in diesem Kapitel liegt jedoch auf IT und Unternehmensnetzwerken.

Was all diese „Dinge“ gemeinsam haben, ist, dass sie eine IP-Adresse haben und Kommunikationen über das Netzwerk initiieren oder empfangen müssen. Wir betrachten diese Geräte auch als relativ geschlossene Systeme, was bedeutet, dass Unternehmen keine willkürliche Drittanbietersoftware auf sie installieren können. Dies gilt natürlich nicht für alle IoT-Geräte – es gibt eine wachsende Anzahl solcher Geräte, die auf voll funktionsfähigen Betriebssystemen basieren, typischerweise eine Variante von Linux, auf die Sie Drittanbietersoftware installieren können. Je nach Ihrer Umgebung und Architektur könnten Sie diese als Zero Trust-Subjekte behandeln (d. h., Rechengeräte mit Identitäten), in welchem Fall unser Standardansatz zur Zugriffskontrolle und Richtliniendurchsetzung gilt. Oder Sie können sie als IoT-Geräte behandeln, in welchem Fall die Prinzipien und Ansätze, die wir in diesem Kapitel diskutieren, gelten.

In jedem Fall werden diese Geräte häufig ohne das gleiche Maß an Sicherheitsbedenken entworfen, hergestellt und eingesetzt, das wir von Unternehmens-IT-Produkten erwarten. Es gibt Hunderte von Beispielen für Mängel in Verbraucherprodukten, und diese existieren auch in Produkten, die sich an Unternehmen richten, insbesondere bei spezialisierten vertikalen Produkten wie

medizinischen Geräten. Häufige Sicherheitslücken bei diesen Geräten sind die Verwendung von unverschlüsselten Netzwerkprotokollen, fest codierte Standardpasswörter, nicht entfernbarer Backdoors, Netzwerk- und Betriebssystemlücken, Schwierigkeiten oder Unmöglichkeit, Firmware zu aktualisieren, und bei physisch zugänglichen Geräten die Möglichkeit für einen Angreifer, diese Nähe zu nutzen, um Shell-Zugriff auf das Gerät zu erlangen.

Diese Geräte sind definitiv ein reifer Vektor für Angriffe und Datenexfiltration, und haben als Stützpunkte für Malware gedient, um Netzwerkaufklärung durchzuführen und sich seitlich zu bewegen (ganz zu schweigen davon, dass sie ein beliebter Schwachpunkt für rote Teams sind, um sie während Penetrationstests auszunutzen).

Beachten Sie, dass einige IoT-Geräte als Teil eines größeren, typischerweise cloudbasierten modernen Systems eingesetzt werden – die großen Cloud-Service-Anbieter haben jeweils ihre eigenen Plattformen, die sowohl Geräte- als auch Cloud-basierte Software nutzen, um Messaging, Sicherheit und Datenmanagement, unter anderem, zu ermöglichen. Diese Plattformen, wie Azure IoT, Google Cloud IoT Core und AWS Greengrass, haben jeweils ein gut konzipiertes Sicherheits- und Kommunikationsmodell, das in gewisser Weise selbstständig ist und eingebaute Unterstützung für sichere bidirektionale Kommunikation (oft sowohl synchron als auch asynchron) bietet. Daher kann es durchaus akzeptabel sein, sie getrennt von Ihrem allgemeinen Unternehmens-Zero Trust-Modell zu implementieren und zu betreiben. Das ist in Ordnung – wie wir im gesamten Buch erwähnt haben, muss nicht alles in den Geltungsbereich Ihres Zero Trust-Projekts einbezogen werden. Tatsächlich wird das bewusste Ausschließen bestimmter Komponenten Ihrer IT-Infrastruktur dazu beitragen, Ihren Fokus, Ihre Geschwindigkeit und Ihren Erfolg zu verbessern. Aber selbst wenn Sie eine moderne IoT-Plattform verwenden, ist es wichtig, ihre Netzwerk- und Kommunikationsarchitektur zu verstehen, damit Sie sicherstellen können, dass sie mit dem Rest Ihres Netzwerksicherheitsmodells koexistiert.

Natürlich sitzen die meisten IoT-Geräte außerhalb dieser Cloud-basierten Frameworks, und sollten unbedingt in Ihre Zero Trust-Sicherheitsarchitektur einbezogen werden. Im Rest dieses Kapitels werden wir zunächst einige der Sicherheits- und Netzwerkherausforderungen im Zusammenhang mit IoT-Geräten untersuchen und dann betrachten, wie Zero Trust-Systeme angewendet werden können, um diese Probleme zu lösen.

Netzwerk- und Sicherheitsherausforderungen von IoT-Geräten

Im Gegensatz zu Benutzergeräten oder Servern stellen IoT-Geräte oft komplexe Management-, Sicherheits- und Zugriffsherausforderungen dar, wenn sie in Unternehmensnetzwerke eingebunden werden, aufgrund ihrer geschlossenen Natur und oft eingeschränkten Kommunikationsarchitekturen. Abb. 16-1 zeigt eine vereinfachte Ansicht eines Unternehmensnetzwerks, um diese Punkte zu veranschaulichen. Das Netzwerk besteht aus verkabelten und drahtlosen Segmenten, an die eine Vielzahl von Gerätetypen angeschlossen ist. Das verkabelte Netzwerk im Unternehmen besteht aus einer Mischung von Benutzergeräten und Ethernet-verbundenen Dingen, einschließlich VOIP-Telefonen, IP-Kameras, Druckern und Zugangstür-Badge-Lesern. Das drahtlose Netzwerk wird von einigen Benutzergeräten, Druckern und anderem vernetzten Bürogerät wie drahtlosen Konferenzraummonitoren und digitalen Whiteboards genutzt.

Einige der Geräte in diesem Netzwerk kommunizieren nach oben zu privaten Servern, die in einem anderen Segment innerhalb des Unternehmensnetzwerks laufen, während andere sich mit Servern über das Internet verbinden. Es gibt auch eine Reihe von Systemadministratoren, die von Zeit zu Zeit eine Fernverbindung zu diesen Geräten herstellen müssen, um Firmware-Updates durchzuführen oder Konfigurationsänderungen vorzunehmen. Diese Administratoren können Mitarbeiter des Unternehmens sein oder für einen Gerätehersteller arbeiten.

Die in diesem Diagramm gezeigten Systeme weisen typischerweise eine Reihe von gemeinsamen Sicherheitsschwachstellen auf, die wir in der Einleitung angesprochen haben. Erstens verwenden viele dieser Geräte unverschlüsselte Netzwerkprotokolle, was sie anfällig für Verkehrsinspektionen oder Man-In-The-Middle (MITM) Angriffe macht, die die Vertraulichkeit, Integrität und Verfügbarkeit gefährden können. Zweitens haben viele dieser Geräte offene Listening-Ports. Während dies notwendig ist, um unseren Remote-Sysadmin den Zugriff auf sie zu ermöglichen, erlaubt es auch jedem anderen netzwerkverbundenen Gerät, eine TCP-Verbindung zu ihnen herzustellen. Drittens haben diese Geräte oft schwache (oder fest codierte) Authentifizierungsmechanismen und haben in der Regel auch Netzwerk-Stacks, die anfällig für eine Vielzahl von Angriffen sind. Schließlich können einige dieser Geräte, wie Außenumweltsensoren, Fernkameras oder Steuergeräte, für längere Zeit physisch für Angreifer zugänglich sein. Infolgedessen könnten Angreifer in der Lage sein, eine verkabelte Netzwerkverbindung

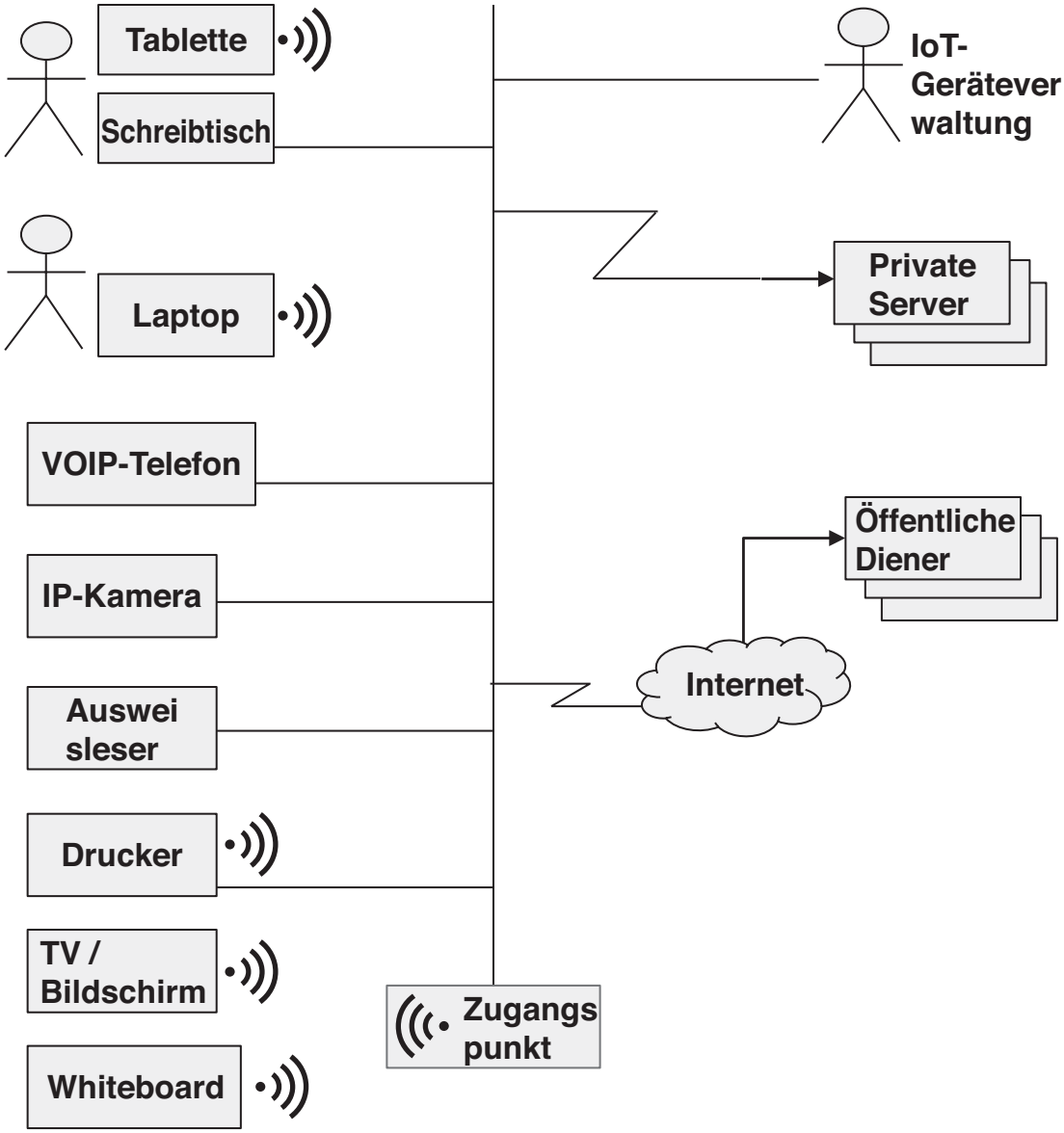

Abb. 16-1. *Unternehmens-IoT-Netzwerk*

zu kapern oder Zugang zum Gerät zu erlangen, indem sie es physisch kompromittieren (z. B. durch Neustarten mit einem bösartigen USB-Stick).

Wenn wir diese Geräte durch unsere Zero Trust-Sicherheitslinse betrachten, sollte klar sein, dass diese Systeme in vielerlei Hinsicht unseren Kernprinzipien nicht gerecht

werden. Idealerweise würde ein Zero Trust-System diese Geräte auf eine Weise absichern, die durchsetzt

- Prinzip der geringsten Privilegien: Minimieren Sie den Upstream-Zugriff, den diese Geräte haben, im Falle einer Geräte- oder Netzwerkkompromittierung.
- Geräteisolierung: Verhindern Sie, dass unbefugte Subjekte im Netzwerk eine Verbindung zu den Geräten herstellen.
- Verkehrverschlüsselung: Leiten Sie den nativen Geräteverkehr durch einen sicheren und verschlüsselten Tunnel.

Natürlich können einige dieser Geräte (wie Wandmontierte Badge-Leser) in einem isolierten verkabelten Netzwerk sein, und andere können bestimmten privaten VLANs zugewiesen werden, um ihren Verkehr zu isolieren. Das sind gute Praktiken, aber sie gelten nicht (und können nicht) für alle Geräte, und selbst wenn sie eingesetzt werden, machen sie die Geräte nicht unangreifbar für Angriffe.

Reale Netzwerke sind oft chaotisch, undurchsichtig und heterogen und sind oft organisch gewachsen, ohne einen kohärenten Plan. Dies ist in der Regel auf den Druck auf das technische Personal zurückzuführen, die Dinge so schnell wie möglich zum Laufen zu bringen, und nicht genügend Zeit oder Budget für Nacharbeiten oder Verbesserungen später einzuplanen. Infolgedessen können gemischte Unternehmensnetzwerke mit diesen Arten von Geräten eine Reihe von Herausforderungen aufweisen, die sie schwer zu sichern machen. Erstens neigen diese Netzwerke dazu, in der Praxis flach und offen zu sein, mit Hunderten (oder Tausenden) von unterschiedlichen Gerätesätzen. Dies ist oft auf die Schwierigkeit zurückzuführen, traditionelle (nicht-Zero Trust) ACLs über ein verteiltes Unternehmen zu verwalten und sie auf dem neuesten Stand und synchron mit täglichen Änderungen zu halten. Zweitens werden diese IoT-Geräte im Gegensatz zu Benutzergeräten, die in der Regel zentral verwaltet werden, typischerweise entweder als eigenständige Geräte verwaltet oder über ein Management-Software-System, das nur für Geräte eines bestimmten Typs gilt. Daher ist es oft schwierig und arbeitsintensiv, diese Geräte im großen Maßstab zu konfigurieren oder zu verwalten. Aber die größte Herausforderung bei diesen Geräten, angesichts der Unfähigkeit, Software auf sie zu installieren, ist die Kontrolle ihres Netzwerkverkehrs. Insbesondere, welche Upstream-Ressourcen dürfen sie sich verbinden, und welche anderen Systeme im Netzwerk dürfen sich mit ihnen verbinden. In einem Zero

Trust-System ist dies natürlich die Rolle des PEP – entweder ein Netzwerk-PEP, ein Benutzeragent-PEP oder beides. Als nächstes werden wir uns ansehen, wie wir diese Welten zusammenbringen können und welche technischen Herausforderungen oft auftreten.

Zero Trust und IoT-Geräte

Idealerweise würden IoT-Geräte auf ein isoliertes und einheitliches Netzwerk ausgerollt, wobei der gesamte Nord/Süd-Netzwerkzugriff in das isolierte Netzwerk durch einen Zero Trust PEP kontrolliert wird. Dieser idealisierte logische Zustand ist in Abb. 16-2 dargestellt.

Die Vorteile davon sollten klar sein, da dieses Modell jedes der zuvor aufgeführten drei Ziele erreicht. Erstens wird das Prinzip der geringsten Privilegien durchgesetzt – der gesamte Upstream-Netzwerkverkehr von jedem Gerätesatz wird vom PEP kontrolliert, was bedeutet, dass Zero Trust-Richtlinien auf ausgehenden Verkehr angewendet und durchgesetzt werden. Dies blockiert Versuche, ein kompromittiertes Gerät für Datenexfiltration, Aufklärung oder DDoS-Angriffe zu nutzen. Zweitens sind diese Geräte innerhalb ihrer eigenen einheitlichen impliziten Vertrauenszone isoliert, so dass eingehender Verkehr den PEP passieren muss, der Zugriffskontrollrichtlinien vor den offenen Listening-Ports der Geräte durchsetzt. Und schließlich wird der gesamte Verkehr zwischen den PEPs verschlüsselt, was alle nativen Klartextprotokolle, die von den Geräten verwendet werden, überwindet. Dies eliminiert einen Großteil des Risikos von MITM-Angriffen.

Natürlich ist selbst dieses idealisierte Modell unvollkommen, was ein Nebenprodukt der Natur dieser Geräte ist. Zum Beispiel können Geräte innerhalb jeder impliziten Vertrauenszone direkt über das LAN miteinander kommunizieren, so dass, wenn eine IP-Kamera kompromittiert wird, diese Malware möglicherweise lateral zwischen Peer-Kameras bewegen kann, obwohl sie auf diese isolierte Zone beschränkt ist, mit ausgehendem Verkehr, der durch den PEP eingeschränkt ist. Ein weiteres Beispiel – oft basiert die Geräteidentifikation auf schwachen Authentifizierungsmechanismen, so dass ein Angreifer sich als IP-Kamera ausgeben und die gleichen Netzwerkberechtigungen wie seine Peer-Kameras erhalten könnte. Es gibt Möglichkeiten, diese Schwächen zu kompensieren, auf die wir später eingehen werden.

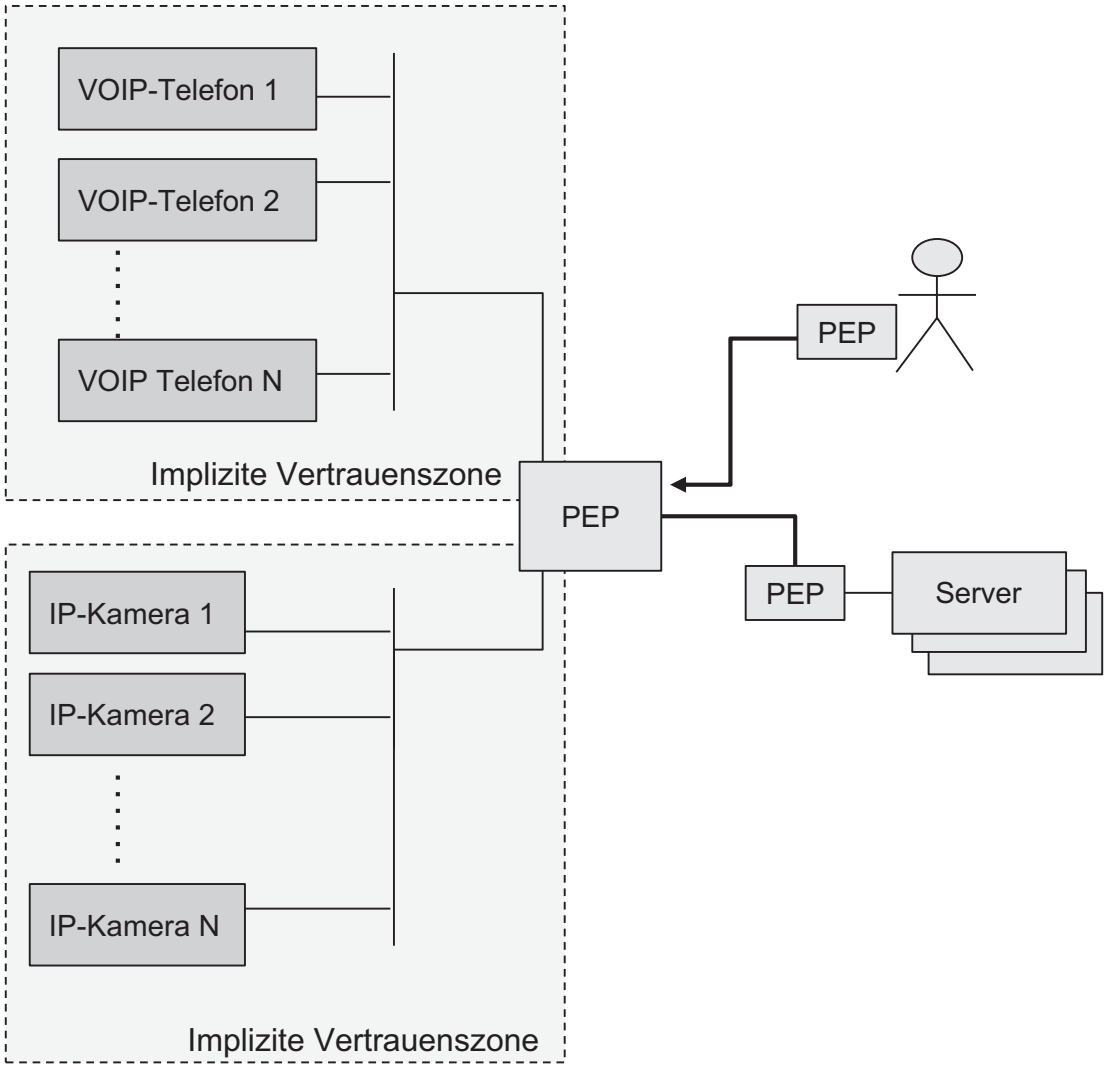

Abb. 16-2. *Idealisiertes Zero Trust IoT Netzwerkmodell*

Natürlich ist die in Abb. 16-2 dargestellte idealisierte Ansicht eine logische Ansicht, und reale Netzwerke verfügen über eine Vielzahl von technischen Mitteln, mit denen sie Geräte identifizieren und authentifizieren, Netzwerke und IP-Adressen zuweisen und den Verkehr leiten können. Dies sind die Schlüsselfunktionen, die jede Netzwerk- und Sicherheitsinfrastruktur bereitstellen muss, und sie können auf komplexe Weise kombiniert werden. Letztendlich muss ein Zero Trust-System, das IoT-Geräte sichert, in der Lage sein, folgende Funktionen auszuführen

- Erfassen, leiten und verschlüsseln des Verkehrs zu und von diesen Geräten
- Zentral verwalten von Zugriffsrichtlinien
- Durchsetzen von Zugriffskontrollen über eine verteilte Menge von Geräten

Dies ist schwierig in einer robusten Art und Weise auf flachen, gemischten Netzwerken wie dem in Abb. 16-1 dargestellten zu erreichen. Die Tab. 16-1 bis 16-3 zeigen Ansätze zu diesen Funktionen, zusammen mit den Vor- und Nachteilen jeder Methode.

Der einfachste und leichteste Ansatz ist in Abb. 16-3 dargestellt, die eine Reihe von IP-Kameras zeigt, die auf ein isoliertes und homogenes Netzwerk verteilt sind. Dies könnte ein physisch isoliertes, verkabeltes Netzwerk sein, ein VLAN, das von einem NAC zugewiesen wird, oder sogar ein kameraeigenes drahtloses Netzwerk mit einer isolierten SSID. Was wichtig ist (und was es einfach macht), ist, dass es homogen ist – alle Geräte in

Tab. 16-1. *Wie Geräte Netzwerken zugewiesen werden*

	Vorteile	**Nachteile**
Physisches Kabel/ Switch Port	Kann ein physisch isoliertes Netzwerk sein	Schwierig zu ändern Isolation kann durch Switch-Port-Kapazität begrenzt sein Schwierig, Netzwerkgeräte von Peers zu isolieren
Private VLAN	Logische Trennung innerhalb eines physischen Netzwerks	Zugang basiert auf physischem Netzwerk oder Switch-Port-Zugang
Wireless Access Point	Netzwerke sind in der Regel einfacher neu zu konfigurieren Eingebaute Geräteisolierung in vielen Wi-Fi-Systemen	Nicht alle Geräte sind Wi-Fi-fähig Einfache Passwortauthentifizierung ist nicht stark, und nicht alle Geräte unterstützen WPA-Enterprise
NAC/802.1x	Dynamische VLAN-Zuweisung kann Geräte nach Typ isolieren	Erfordert oft teure Hardware Schwierig, große Mengen von VLANs zu verwalten Nicht alle Geräte unterstützen 802.1x

Tab. 16-2. *Wie Geräte Identifiziert/Authentifiziert werden*

	Vorteile	**Nachteile**
IP-Adresse	Feste IPs können ein Gerät eindeutig identifizieren	Konfigurations- und Verwaltungsaufwand Schwache Form der Identifikation, leicht zu spoofen
MAC-Adresse	Unterstützt auf allen Geräten Nützlich zur Identifizierung von Geräteklassen in gemischten Netzwerken und zur Zuweisung zu Zonen (oft mit 802.1x)	Schwache Form der Identifikation, leicht zu spoofen
DHCP-Fingerprint	Unterstützt auf fast allen Geräten Mäßig nützlich zur Identifizierung von Geräteklassen in gemischten Netzwerken	Schwache Form der Identifikation, leicht zu spoofen
Zertifikat über 802.1x	Stark und zuverlässig	Verwaltungs- und PKI-Aufwand Viele Geräte können keine zertifikatsbasierte Authentifizierung oder Identifizierung verwenden

diesem Netzwerk sind vom gleichen Typ und haben daher den gleichen Satz von Netzwerkzugriffssteuerungen, die auf sie angewendet werden.

Der Schlüssel für dieses Szenario ist, dass die IP-Kameras im Netzwerk das PEP als ihr Standard-Netzwerk-Gateway konfiguriert haben, so dass aller nicht-LAN-Verkehr an das PEP gesendet wird, das Routing und Richtliniendurchsetzung durchführt. Das heißt, das PEP ist der einzige Ausgangspunkt aus der lokalen Zone. Die Zuweisung des Standard-Netzwerk-Gateways der Kameras könnte zentral über das IP-Kamera-Management-System oder über einen DHCP-Server für das Kamera-eigene Segment erfolgen.

In jedem Fall sollte klar sein, dass dies so nah wie möglich am idealen Szenario ist, was es einfach macht, es in ein Zero Trust-Modell zu integrieren. Unser nächstes Szenario, dargestellt in Abb. 16-4, ist typischer und schwieriger zu kontrollieren.

Dieses Diagramm zeigt ein gemischtes (heterogenes) Netzwerksegment, 192.168.112.0/20, bestehend aus Hunderten von Computern und Geräten in einem

Tab. 16-3. *Wie Netzwerk-Routing zugewiesen wird*

	Vorteile	**Nachteile**
Standard Netzwerk-Gateway	Automatisch über DHCP zugewiesen Fester und zentralisierter Ausgangspunkt vom LAN ist natürlicher Punkt zur Durchsetzung von Richtlinien	DHCP-Zuweisung kann nicht immer Gerätetypen in gemischten Netzwerken unterscheiden Konfiguration getrennt von DHCP ist möglich, aber möglicherweise aufwendig
Routeneinstellung für geschützte Ressourcen durch Netzwerk-Router	Einfach einzurichten und unabhängig von der Gerätekonfiguration	Sichert den Zugang zu Zielressourcen, filtert aber möglicherweise nicht nach Quelle Verhindert nicht den Gerätezugang zu anderen Ressourcen
Geräte manuell konfigurieren	Feinkörnige Kontrolle der Routen	Arbeitsintensiv und schwierig zu warten, wenn sich Netzwerke ändern

flachen Unternehmensnetzwerk in einem Bürogebäude. Die Geräte in diesem Netzwerk haben im Wesentlichen zufällige IP-Adressen, die ihnen aus dem Subnetzbereich über DHCP zugewiesen wurden, und die Organisation hat keine genaue CMDB. Dieses Szenario stellt eine Reihe von Herausforderungen dar, um unsere Ziele zu erreichen – nämlich sicherzustellen, dass nur die Testgeräte Zugang zum Testgeräteserver haben, dass keine anderen Geräte auf diesen Server zugreifen können und dass der Zugang zu den Testgeräten durch Richtlinien kontrolliert wird. Leider können wir in diesem realen Szenario all diese Ziele nicht erreichen, ohne Änderungen am Netzwerk vorzunehmen. Dies ist in vielen Unternehmensszenarien zu erwarten, auch außerhalb von IoT-Geräten – aber zumindest müssen Sie sich über die Mängel Ihres Netzwerks im Klaren sein und herausfinden, wie Sie diese Probleme lösen können, auch wenn Sie sie nicht sofort lösen können.

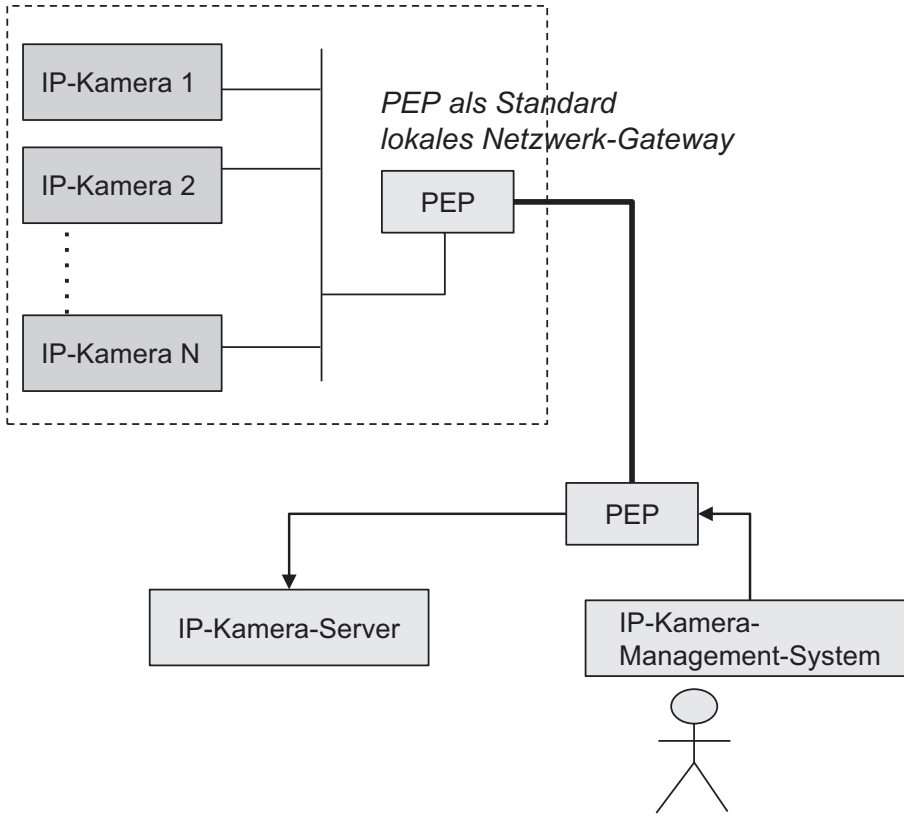

Abb. 16-3. *IP-Kameras auf isoliertem, homogenem Netzwerk*

Lassen Sie uns untersuchen, was hier erreicht werden kann (und was nicht), mit dem Fokus auf die Sicherung des Upstream-Netzwerkzugangs von den Testgeräten. Das heißt, das Unternehmen benötigt eine Möglichkeit, sicherzustellen, dass vom Testgerät initierter Verkehr, der für den Testgeräteserver (10.6.20.2) im entfernten Netzwerk bestimmt ist, zum lokalen PEP für Durchsetzung und Weiterleitung über den sicheren Tunnel geleitet wird. Dies kann auf drei mögliche Arten erreicht werden:

- Standard-Gateway direkt auf dem Testgerät konfiguriert
- Standard-Gateway über DHCP dem Testgerät zugewiesen
- Statisches oder dynamisches Routing im Netzwerk

Die Konfiguration des Standard-Netzwerk-Gateways direkt auf dem Testgerät kann möglich sein, abhängig davon, ob es dies technisch unterstützt. Es hängt auch davon ab,

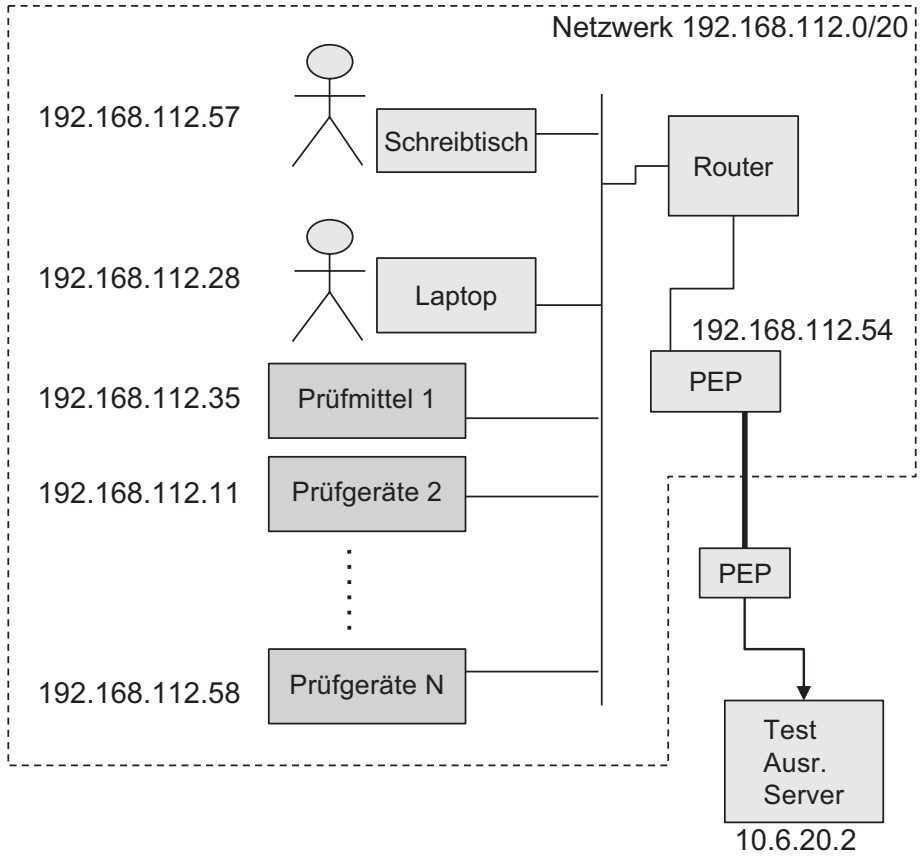

Abb. 16-4. *Heterogenes Unternehmensnetzwerk*

wie arbeitsintensiv dieser Prozess ist. Die Durchführung über ein zentralisiertes Management-System ist unkompliziert, während individuelle manuelle Änderungen an Hunderten von Geräten möglicherweise nicht in Frage kommen. Die Zuweisung des PEP als Standard-Netzwerk-Gateway über DHCP, für alle Geräte, kann in einigen Fällen ebenfalls ein gangbarer Ansatz sein. In einigen Fällen kann der DHCP-Server möglicherweise verschiedene Standard-Netzwerk-Gateways für verschiedene Geräte zuweisen, wenn die DHCP-Zuweisung genau zwischen DHCP-Anfragen, die vom Testgerät initiiert wurden, und solchen, die von anderen Geräten ausgegeben wurden, unterscheiden kann,[1] und unterschiedliche Werte zurückgeben.

[1]Zum Beispiel durch die Untersuchung von DHCP-Fingerabdrücken.

Schließlich ist es auch möglich, den Netzwerkrouter so zu konfigurieren, dass er den Netzwerkverkehr, der für den entfernten Testgeräteserver (10.6.20.2) bestimmt ist, an den lokalen PEP (192.168.112.54) sendet. Dies hat den Vorteil, dass keine weiteren Änderungen am Netzwerk erforderlich sind, erfordert jedoch, dass der PEP in der Lage ist, legitimen Verkehr (initiiert von einem Testgerät) von illegitimem Verkehr (z. B. initiiert von Malware auf einem Benutzergerät, das Netzwerkerkundungen durchführt) zu unterscheiden. Dies wird in unserem Szenario schwierig zu erreichen sein, da IP-Adressen zufällig zugewiesen werden und es keine CMDB gibt. Es ist möglich, dass der PEP MAC-Adressen zur Unterscheidung von Geräten verwendet, aber diese sind eine schwache Form der Identifikation, die trivial gefälscht werden kann und daher ein gewisses Risiko birgt, wenn sie auf diese Weise verwendet wird.

Zusammenfassung

Wie in vielen Bereichen unserer realen Netzwerke und Systeme sind IoT-Geräte oft komplex und schwer zu verwalten. Zero Trust kann in vielen (wenn nicht den meisten) Situationen helfen, bietet aber in der Regel nicht das gleiche Maß an Sicherheit wie bei Standard-Unternehmensgeräten (Benutzersystemen und Servern). Zero Trust PEPs können verwendet werden, um den Zugriff von Upstream-Geräten auf geschützte Ressourcen zu kontrollieren, um sicherzustellen, dass der Netzwerkverkehr verschlüsselt ist, und um den Downstream-Zugriff auf IoT-Geräte zu kontrollieren – mit unterschiedlichem Erfolg, abhängig von den vielen Faktoren, die wir in diesem Kapitel besprochen haben.

Wenn Sie Ihr Unternehmen betrachten, um Kandidaten-IoT-Systeme für die Aufnahme in Ihr Zero Trust-Projekt zu identifizieren, gibt es einige Merkmale, nach denen Sie suchen können, um Ihnen bei der Identifizierung gut geeigneter IoT-Systeme zu helfen. Erstens, verstehen Sie, wie die Netzwerkkonfiguration dieser Geräte konfiguriert ist, und bevorzugen Sie IoT-Geräte, die über einen zentral verwalteten Mechanismus verfügen, um diese leicht im großen Maßstab zu kontrollieren. Zweitens, suchen Sie nach Bereichen Ihres Netzwerks, die gut verstanden und angemessen gut dokumentiert sind. Vermeiden Sie es, IoT-Geräte in einem unverwalteten, vielfältigen und undurchsichtigen Netzwerk als frühes Projekt zu sichern – Sie müssen sicherstellen, dass Sie einige Erfahrungen und Erfolge bei der Anwendung Ihrer Zero Trust-Architektur auf IoT-Systeme in einfacheren und besser verstandenen Umgebungen haben. Und

schließlich, suchen Sie nach einigen „niedrig hängenden Früchten“ rund um die Sicherung des Fernzugriffs von Dritten auf interne Geräte. Die Fähigkeit von Zero Trust, einen Geschäftsprozess, wie die Erstellung eines Service Desk-Tickets, vor dem Zugriff zu verlangen, kann schnell echten Sicherheitswert liefern.

IoT-Geräte sind definitiv ein aufstrebender Bereich für Zero Trust und, wie wir hier untersucht haben, neigen dazu, komplex und hochtechnisch zu sein und können oft ein Minenfeld aus älterer und unflexibler Technologie sein. Aber es gibt viele Möglichkeiten zur Verbesserung, und wir haben dieses Thema nur an der Oberfläche gekratzt – dies könnte ein ganzes Buch für sich sein. Wenn dies ein primärer Anwendungsfall für Ihr Zero Trust-Projekt ist, erkunden Sie sorgfältig und führen Sie sicher ein Pilotprojekt in Ihrer beabsichtigten Umgebung durch, um die Kompatibilität der Technologie zu validieren. Einige wichtige Fragen, die Sie sich stellen sollten, beinhalten

- Wie komplex und ausgereift sind Ihre Gerätenetzwerke?
- Haben Sie ein genaues und zuverlässiges Inventar der Geräte und ihrer Kommunikationsmuster?
- Wie einfach oder schwierig ist es, den Netzwerkverkehr von Geräten für die Durchsetzung durch einen PEP zu erfassen?
- Welche Netzwerkänderungen werden erforderlich sein und welchen Einfluss werden sie auf andere vernetzte Geräte haben?
- Welche Netzwerkprotokolle verwenden diese Geräte? Handelt es sich um verbindungsorientierte oder verbindungslose Protokolle? Sind sie verschlüsselt?

Schließlich werden natürlich verschiedene Zero Trust-Implementierungen dies unterschiedlich angehen, und es ist wichtig, die Fähigkeiten Ihrer gewählten Zero Trust-Lösung und des Bereitstellungsmodells für diesen Anwendungsfall klar zu verstehen. Einige Produkte und Architekturen werden diese Szenarien gut unterstützen, während andere Schwierigkeiten haben werden. Mit all dem gesagt, glauben wir, dass Zero Trust-Systeme einen großen Wert für oft unsichere IoT-Ökosysteme bringen können, und wir ermutigen Sie, zu untersuchen, ob die Umgebung Ihrer Organisation ein guter Kandidat ist.

TEIL III

Alles Zusammenfügen

Im Teil II dieses Buches haben wir die Zero Trust-Prinzipien und -Architekturen aus Teil I genommen und sie als unsere Linse verwendet, um eine breite Palette von Komponenten in Unternehmens-IT- und Sicherheitsarchitekturen zu untersuchen. Von On-Premises- und Cloud-basierten Netzwerkinfrastrukturen bis hin zu Sicherheits- und Nicht-Sicherheitskomponenten hat diese Analyse Ihnen hoffentlich ein tiefes Verständnis für die Wege vermittelt, auf denen Zero Trust Ihr Unternehmen beeinflussen kann. Dies sollte Sie mit einem Satz von Werkzeugen, Mustern und Perspektiven ausgestattet haben, mit denen Sie beginnen können, die Reise Ihres Unternehmens zu Zero Trust zu gestalten.

Hier in Teil III werden wir unsere Reise abschließen, indem wir auf diesen Grundlagen aufbauen. Wir beginnen mit dem, was in vielerlei Hinsicht der Schlüsselstein des Zero Trust ist - das Policy-Modell, in Kap. 17. Erinnern Sie sich, dass unsere architektonische Prämisse ist, dass ein Zero Trust-System aus einer Reihe von verteilten Policy-Durchsetzungspunkten und einem zentralisierten Policy-Entscheidungspunkt besteht. Aus dieser Perspektive sind die definierten, bewerteten und letztendlich durchgesetzten Richtlinien wohl der wichtigste Teil des Systems. Was das bedeutet, ist, dass das Policy-Modell in Ihrer gewählten Zero Trust-Implementierung - seine Sprache und Struktur, die sich in den Bereitstellungsmodellen und Policy-Durchsetzungsfähigkeiten dieses Produkts widerspiegeln werden - einen großen Einfluss haben wird.

Nachdem wir das Policy-Modell besprochen haben, werden wir in Kap. 18 die Dinge wieder auf eine konkretere Realität zurückbringen, indem wir uns sieben der häufigsten Anwendungsfälle von Zero Trust ansehen und wie Ihre Organisation sie angehen sollte. Wir werden jeden einzelnen aus einer architektonischen Perspektive betrachten und dabei Überlegungen und Empfehlungen diskutieren.

Schließlich werden wir in Kap. 19 unsere Reise abschließen (und Ihnen helfen, Ihre zu beginnen) mit einer Diskussion und Anleitung, wie Sie erfolgreiche Zero Trust-

Implementierungen, Projekte und Initiativen planen können. Wir werden dies sowohl aus einer organisatorischen und programmatischen Top-Down-Perspektive als auch aus einer taktischen Bottom-Up-Projektperspektive betrachten. Wir werden uns auch häufige Hindernisse für Zero Trust-Initiativen ansehen und wie man sie am besten überwinden kann.

Lassen Sie uns eintauchen und beginnen, all diese Ideen zu einem kohärenten Ganzen zusammenzuführen.

KAPITEL 17

Ein Zero Trust Richtlinienmodell

Richtlinien sind das Herzstück von Zero Trust – schließlich sind seine primären architektonischen Komponenten *Richtlinien* Entscheidungspunkte und *Richtlinien* Durchsetzungspunkte. Der Begriff *Richtlinie* ist natürlich in der englischen Sprache stark überladen, mit Bedeutungen auf vielen verschiedenen Ebenen. In unserer Zero Trust-Welt sind Richtlinien die Strukturen, die von Organisationen geschaffen werden, um zu definieren, welche Identitäten Zugang zu welchen Ressourcen unter welchen Umständen erhalten dürfen. Denken Sie daran, dass in einer Zero Trust-Umgebung der Zugang nur durch die Bewertung und Zuweisung einer Richtlinie an eine Identität erlangt werden kann und dass der Zugang auf Netzwerk- oder Anwendungsebene durchgesetzt werden kann.

Die tatsächlichen, technischen Mittel, mit denen Richtlinien definiert und durchgesetzt werden, sind produkt- und implementierungsabhängig, aber die Konzepte und Komponenten sind universell und sollten in jedem Zero Trust-System allgegenwärtig sein. Das NIST Zero Trust-Dokument besagt, dass „eine Richtlinie die Menge an Zugriffsregeln auf der Grundlage von Attributen ist, die eine Organisation einem Subjekt, einem Datenasset oder einer Anwendung zuweist,“[1] und eines der NIST-Kernprinzipien ist, dass „der Zugang zu Ressourcen durch dynamische Richtlinien bestimmt wird – einschließlich des beobachtbaren Zustands der Client-Identität, der Anwendung/des Dienstes und des anfordernden Assets – und kann andere Verhaltens- und Umgebungsattribute einschließen.“[2] Erinnern Sie sich an unsere Arbeitsdefinition in Kap. 2, Zero Trust muss „die dynamische Durchsetzung von Sicherheitsrichtlinien ermöglichen.“

[1]NIST Zero Trust-Architektur, Seite 6
[2]Ebd

J. Garbis und J. W. Chapman, *Zero Trust Sicherheit*, https://doi.org/10.1007/979-8-8688-0105-1_17

Wie wir in Kap. 3 kurz eingeführt haben, fügen wir der Richtliniendiskussion Struktur und Spezifität hinzu, erweitern einige der Konzepte im NIST Zero Trust-Framework. Wir weben auch Industriekonzepte rund um Attribute-Based Access Control (ABAC) ein und interpretieren sie aus der Perspektive von Zero Trust.

Unser Ziel mit diesem Kapitel ist es, Ihnen ein Framework und eine Struktur zu bieten, mit denen Sie über den Umfang Ihres Zero Trust-Systems nachdenken können und mit denen Sie Anbieterplattformen bewerten können. Zero Trust-Systeme können nahezu unendlich in Breite und Tiefe sein, und es ist wichtig für Sie, ein starkes Gefühl dafür zu haben, was einbezogen werden sollte und was nicht, und was vernünftig in ein Richtlinienmodell aufgenommen werden kann. Dies ist erforderlich, um Ihre Richtlinienarchitektur und ihren Lebenszyklus sowie den entsprechenden Satz von Governance-Prozessen zu definieren. Das Verständnis der Fähigkeiten und Grenzen Ihres beabsichtigten Richtlinienmodells ist auch eine nützliche Möglichkeit, Anforderungen und Grenzen für Ihre geplante Zero Trust-Architektur festzulegen. Lassen Sie uns eintauchen, beginnend mit einer ausführlichen Diskussion der logischen Komponenten, die Richtlinien ausmachen.

Richtlinienkomponenten

In diesem Abschnitt führen wir die Richtlinienstruktur aus Kap. 3 erneut ein, diesmal mit zusätzlichen Kommentaren. Tab. 17-1 zeigt die Richtlinienstruktur, die die Komponenten *Subjektkriterien*, *Aktion*, *Ziel* und *Bedingung* definiert.

Beachten Sie, dass wir hier eine logische Struktur darstellen, die unserer Meinung nach eine solide Möglichkeit ist, über die Komponenten von Richtlinien nachzudenken. Tatsächliche Zero Trust-Implementierungen können ihr Richtlinienmodell durchaus anders strukturieren, sollten aber diese Elemente in sich enthalten. Lassen Sie uns jede der Komponenten des Richtlinienmodells nacheinander betrachten.

Subjektkriterien

Letztendlich wird ein Subjekt (eine authentifizierte Identität) die festgelegte Aktion auf das Ziel ausführen. Richtlinien werden von der PDP den Subjekten zugewiesen, die jedes Kriterium der Richtlinie zu verschiedenen Zeiten gegen das fragliche Subjekt bewertet (wir werden dies in diesem Kapitel weiter diskutieren). Beachten Sie, dass

Tab. 17-1. *Komponenten des Zero Trust-Richtlinienmodells*

Komponenten	Beschreibung
Subjektkriterien	Subjekte sind die Entitäten, die (initiierende) Aktionen durchführen Subjekte müssen authentifizierte Identitäten sein, und Richtlinien müssen *Subjektkriterien* enthalten, die die Subjekte bestimmen, auf die diese Richtlinie anwendbar ist
Aktion	Die Aktivität, die vom Subjekt durchgeführt wird Dies muss entweder eine Netzwerk- oder eine Anwendungskomponente enthalten und kann möglicherweise beide enthalten
Ziel	Das Objekt (Ressource), auf das die Aktion ausgeführt wird. Dies kann statisch oder dynamisch innerhalb der Richtlinie definiert sein und kann breit oder eng im Umfang sein, obwohl eng bevorzugt wird
Bedingung	Die Umstände, unter denen das Subjekt berechtigt ist, die Aktion auf das Ziel auszuführen Das Zero Trust-System muss die Definition von Bedingungen unterstützen, die auf mehrere Arten von Attributen zurückgreifen, einschließlich Subjekt-, Umgebungs- und Zielattributen

Richtlinien selbst normalerweise kein spezifisches Subjekt referenzieren, sondern stattdessen die *Kriterien* enthalten, die die PDP verwendet, um zu bestimmen, ob die Richtlinie einer gegebenen Identität zugewiesen wird. Einige Richtlinienkriterien können recht breit („Alle Mitarbeiter“) oder eng sein („Benutzer in der Gruppe *Marketing,* und zugewiesen zum Projekt *Bruin,* die Windows-Geräte verwenden“).

Typische Subjektkriterien umfassen die Mitgliedschaft in Verzeichnisgruppen, identitätsbezogene Attribute und relativ statische Geräteattribute wie Betriebssystemversion und Patch-Level oder Jailbreak-Status von Mobilgeräten. Beachten Sie, dass Subjekte, wie wir im gesamten Buch diskutiert haben, nicht unbedingt menschliche Benutzer sein müssen. Server (oder logischerweise die Dienstkonten, die in ihnen laufen) können auch Identitäten haben und daher authentifizierte Subjekte mit Richtlinien sein, die ihnen zugewiesen sind und ihnen spezifische Zugriffsrechte gewähren.

Beachten Sie, dass der Ansatz, den wir hier beschreiben, dem entspricht, was das NIST-Dokument als den *kriterienbasierten* Ansatz bezeichnet, mit dem der Vertrauensalgorithmus innerhalb der PDP Richtlinienzuweisungsentscheidungen trifft.

NIST diskutiert auch einen *punktebasierten* Ansatz, der ebenfalls akzeptabel ist. Wir bevorzugen nicht den einen vor dem anderen, obwohl wir für unsere Diskussion hier glauben, dass es einfacher ist, über einen Satz von Kriterien nachzudenken, die *alle* erfüllt sein müssen, damit eine Richtlinie einem gegebenen Subjekt zugewiesen wird.[3]

Schließlich beachten Sie, dass wir uns momentan Richtlinien und Subjekte aus der Perspektive von *subjektinitiierten Aktionen* ansehen, die aus dem bekannten Szenario stammen, in dem ein Benutzer oder ein Server (die authentifizierte Subjekte sind) sich über einen PEP mit einem Server verbindet, um auf eine Ressource zuzugreifen. Später werden wir das komplexere Szenario untersuchen, in dem diese Verbindung in umgekehrter Richtung erfolgt.

Aktion

Aktionen definieren die Art der Aktivität, die von der Richtlinie erlaubt wird. Die Einzelheiten der Aktivität hängen von den Fähigkeiten der Durchsetzungspunkte ab; während viele Aktionen mit dem Netzwerkzugriff zusammenhängen werden, ist es auch wahrscheinlich, dass einige Zero Trust-Systeme die Möglichkeit bieten, andere Arten von Aktionen durchzusetzen, wie zum Beispiel anwendungs- oder datenzentrierte Aktionen. Diese Unterscheidung entspricht den verschiedenen Arten von PEPs, die auf der Netzwerk- oder Anwendungsebene arbeiten können. Aus Netzwerksicht sollten Aktionen den erlaubten Satz von Netzwerkports und Protokollen spezifizieren. Aus einer Anwendungs- oder Datenperspektive könnten Aktionen an Rollen, Attribute, Anwendungsdienste oder Datenklassifizierungen gebunden sein (mehr zu diesem Thema in Kürze). Wir glauben, dass es die Dinge vereinfacht, Aktionen als unabhängig von den Zielen zu betrachten, auf die sie angewendet werden, obwohl in der Praxis einige Implementierungen möglicherweise kombinieren diese zusammen.

Hier sind einige Beispiele für Aktionen:

- Zugriff auf Ressource über HTTPS (TCP auf Port 443 mit TLS)
- Zugriff auf Ressource über TCP auf Port 3389 (RDP)
- Zugriff auf Ressource über UDP auf Port 53 (DNS) und Annahme einer Antwort

[3]Dies kann als punktebasierter Ansatz betrachtet werden, bei dem die Punktzahl 100 % betragen muss, wenn Sie es vorziehen.

- Zugriff auf Ressource über TCP-Port 445 (Windows SMB)
- Zugriff auf Web-App unter URL /app1 auf dem Ziel
- Zugriff auf Web-App unter URL /app1/adminUI auf dem Ziel
- Ausführen eines Linux *kill* Befehls über SSH
- Zugriff auf als „nicht klassifiziert“ gekennzeichnete Daten mit Lese-/Schreibberechtigungen
- Zugriff auf als „Kunden-PII“ gekennzeichnete Daten mit nur Leseberechtigungen

Sie werden bemerken, dass unsere Beispiele TCP- und UDP-Zugriff (die von einem Netzwerk-PEP durchgesetzt werden) sowie einige Beispiele, die auf Anwendungsebene-Konzepten basieren (und Anwendungsebene-PEP-Durchsetzung), beinhalten. Diese letzteren sind interessant und definitiv eher eine „Spitzenfähigkeit“. Anwendungsebene-Aktionen (Anwendungsfunktionen) sind im Allgemeinen nicht im Rahmen von Zero Trust-Richtlinien von heute. Dies liegt daran, dass Anwendungen in der Regel ein undurchsichtiges, internes Autorisierungsmodell haben, das nicht geeignet ist, von einem externen System gesteuert zu werden. Mit dem Aufkommen moderner Webanwendungen, die über HTTP zugegriffen werden, sehen wir jedoch eine häufigere Korrelation zwischen Anwendungsfunktionen und URLs, was die Tür für diese Arten von PEP-durchgesetzten Aktionen in einer Weise öffnet, die zuvor nicht möglich war.

Zum Beispiel haben wir möglicherweise eine wichtige interne Bankanwendung, die sich unter `https://fundmgmt.internal.example.com/main/` befindet und von Hunderten von Mitarbeitern genutzt wird. Diese App hat eine administrative UI, die unter `https://fundmgmt.internal.example.com/adminUI/` nur von den wenigen autorisierten Systemadministratoren aufgerufen wird. Während normale Benutzer keine administrativen Funktionen ausführen können, weil ihre Kontorolle es nicht erlaubt, können sie zur Admin-URL navigieren und versuchen, sie anzugreifen. Angesichts der Tatsache, dass dies ein finanziell lohnendes Ziel für Kriminelle ist, können wir uns leicht vorstellen, dass einige aus der Ferne direkt Malware auf der Workstation eines regulären Benutzers versuchen würden, dies zu tun. Indem wir eine Richtlinie erstellen, die eine Mitgliedschaft in der Admin-Verzeichnisgruppe erfordert, um auf die Admin-URL zuzugreifen, erreichen wir unser Prinzip der geringsten Privilegien und halten unsere Benutzer voll produktiv.

Dies ist möglich, weil es einen sichtbaren Aspekt der Anwendung gibt – die URL – die verwendet wird, um verschiedene Funktionen zu unterscheiden. Wenn die Anwendung ein undurchsichtiges Netzwerkprotokoll oder ein anderes URL-Schema verwenden würde, wäre dies nicht möglich. Es gibt einige bekannte Anwendungsprotokolle, für die diese Art der Durchsetzung von Zero Trust-Richtlinien möglich ist, zusätzlich zu HTTP. Zum Beispiel gibt es keinen Grund, dass Systeme, die bekannte Anwendungsprotokolle wie SSH proxyen, nicht dasselbe tun könnten. Schließlich machen PAM-Anbieter bereits einen guten Job bei der Durchsetzung von Kontrollen um spezifische SSH-Befehle, so dass es nicht weit hergeholt ist, sich ein Zero Trust-System (vielleicht von einem PAM-Anbieter) vorzustellen, das etwas Ähnliches bietet.

Die Datenbeispiele sowie mögliche Aktionen auf anderen Anwendungen sind ein bisschen anders und sind eher zukunftsorientierte Konzepte. Die Idee ist, dass ein Zero Trust-System ein offenes Sicherheitsframework verwenden würde, das es dem PEP und der Anwendung ermöglicht, Informationen auszutauschen, die ihre Fähigkeit zur Durchsetzung von Richtlinien verbessern. Wir können uns zum Beispiel eine Anwendung vorstellen, die in Zusammenarbeit mit einem PEP arbeitet, entweder über ein Plug-in oder über eine Konfiguration, und Anwendungsprotokollkomponenten mit Anwendungsaktionen verknüpft, so dass der PEP Kontrollen durchsetzen oder sogar eine Art von Just-In-Time-Anwendungsrollenbereitstellung für das Subjekt durchführen kann. Oder in die andere Richtung, eine strukturierte Möglichkeit für den PEP, zusätzliche Identitäts- oder Kontextinformationen an die Anwendung zu senden, so dass die Anwendung die Zero Trust-Kontrollen durchsetzen kann. Sie erinnern sich vielleicht daran, dass Google diesen letzteren Ansatz in ihrer BeyondCorp-Initiative verfolgt hat, die wir in Kap. 4 erwähnt haben. Ihr Access Proxy (effektiv ihr PEP) hat zusätzliche Kontextinformationen in HTTP-Headern für Benutzeraktionen eingefügt, und die Zielanwendungen konnten diese zusätzlichen Informationen entweder ignorieren oder verwenden.

Wir glauben, dass dies ein aufkommender Bereich ist und dass es in den nächsten Jahren interessante Entwicklungen in diesem Bereich geben wird. Idealerweise würden wir ein offenes Framework sehen, mit dem Anwendungsentwickler und Zero Trust-Systeme interagieren und integrieren können. Auch ohne diese technische Integration sollten Sie jedoch daran denken, dass Ihr Unternehmen Zugriffssteuerungsprozesse durchführen sollte, um sicherzustellen, dass Benutzer nur angemessene Anwendungsrollen und -fähigkeiten haben. Dies ist ein großartiges Beispiel dafür, wie verschiedene Arten von Systemen und verschiedene Teile der Organisation in Harmonie zusammenarbeiten können.

Ziel

Ziele definieren den Host, das System oder die Komponente, auf die eingewirkt wird. Richtlinien können Ziele statisch oder dynamisch definieren (was eine Aktion des PEP erfordert, um das Ziel vollständig zu rendern). Dynamische Richtlinien sind besonders leistungsfähig – eines der Schlüsselprinzipien von Zero Trust und warum es so überzeugend ist. Diese Richtlinien bieten die Möglichkeit, den Zugriff auf Attribute zu definieren und durchzusetzen, die bis zur Laufzeit unbekannt und nicht erkennbar sind.

Schauen wir uns einige Beispiele für Ziele an, die eine nützliche Bandbreite verschiedener Typen veranschaulichen.

Zugang zum Host 10.6.1.34

Dies ist ein einfaches, statisches und vollständig gerendertes Ziel – das Netzwerk-PEP muss keine weitere Arbeit leisten, um dies durchzusetzen. Ziele, die eine einzelne IP-Adresse angeben, sind zwar nützlich, aber normalerweise keine gute Wahl, um sie in eine Richtlinie aufzunehmen. IP-Adressen ändern sich natürlich und in vielen Fällen ist der logisch beabsichtigte Zugriff nicht auf den Host mit dieser IP-Adresse, sondern auf die Anwendung oder den Dienst, der auf dieser IP-Adresse läuft. In solchen Fällen könnte ein Hostname eine bessere Wahl für ein Ziel sein als eine IP-Adresse. Wir diskutieren dies in unserem nächsten Beispiel.

Ein letzter Kommentar – es gibt natürlich Fälle, in denen es sinnvoll ist, feste IP-Adressen in Zielen anzugeben, insbesondere wenn der Zugriff IT- oder Netzwerkadministratoren gewährt wird, die auf Infrastrukturelemente wie Netzwerkgeräte zugreifen müssen. Sie kennen Ihre Umgebung am besten und müssen letztendlich die effektivste Vorgehensweise entscheiden.

Zugang zum Host appserver1.internal.example.com

Ziele, die Hostnamen angeben, werden sehr häufig verwendet und sind eine sehr effektive Möglichkeit, Richtlinien zu definieren. Hostnamen werden natürlich über DNS in IP-Adressen umgewandelt. Richtlinien, die einen einzelnen Hostnamen als Ziel angeben, ermöglichen es Ihnen, feinkörnige Zugriffskontrollen zu erstellen, und werden oft mit einer begrenzten Menge von Aktionen kombiniert, meistens einem einzigen Netzwerkprotokoll und Port.

Zero Trust-Richtlinien müssen in der Lage sein, das Verhalten der internen DNS-Systeme, Teams und Prozesse einer Organisation zu nutzen und mit (anstatt gegen) seinem Verhalten zu arbeiten. Betrachten Sie zum Beispiel eine interne benutzerorientierte Anwendung mit einer IP-Adresse, die sich regelmäßig ändert. Dies ist zum Beispiel für ein virtualisiertes System mit einer Reihe von Anwendungsaktualisierungen, das möglicherweise einen gestaffelten Ansatz für Produktionsrollouts verwendet, völlig angemessen. DNS wird auch häufig für Lastausgleichszwecke verwendet, für geografische Verteilung über einen Satz von replizierten Anwendungsservern oder einfach als Standard-Best-Practice, um IT-Teams die Möglichkeit zu geben, notwendige Netzwerkänderungen unabhängig von Anwendungen vorzunehmen.

In allen Fällen ist es wichtig, dass das Zero Trust-System in der Lage ist, Hosts aufzulösen, indem die verteilten PEPs den entsprechenden DNS-Server verwenden. In einer verteilten Zero Trust-Umgebung, die über mehrere disparate Netzwerke läuft, ist es oft der Fall, dass ein zentralisiertes PDP nicht alle Hostnamen auflösen kann, da sie sich in getrennten Domänen und/oder in getrennten Netzwerken befinden.

Zugang zu Hosts im Subnetz 10.5.1.0/24

Dieses Beispiel zeigt ein statisches Ziel, das mehreren Hosts innerhalb des Subnetzes entspricht – tatsächlich gewährt dieses Ziel Zugang zu allen Hosts in diesem Subnetz. Diese Art von breitem Zugang ist nicht ideal und steht im Allgemeinen im Widerspruch zum Prinzip der geringsten Privilegien. Es gibt jedoch immer Ausnahmen. Dieses Ziel könnte sinnvoll in einer Richtlinie verwendet werden, wenn es zum Beispiel IT-Administratoren gewährt würde, die einen legitimen Bedarf haben, auf alle Hosts in diesem Netzwerk zuzugreifen[4] . Oder, wenn das Netzwerk so segmentiert war, dass alle Geräte in diesem Netzwerk von ähnlicher Art waren und es daher sinnvoll war, allen Zugang zu gewähren. Höchstwahrscheinlich würde dieses Ziel während eines Übergangszustands verwendet, wenn eine Organisation mitten in ihrer Reise zu Zero Trust ist und noch nicht bereit ist, feinere Zugriffsbeschränkungen durchzusetzen. Dies könnte als Enklaven-basiertes Modell mit der impliziten Vertrauenszone hinter dem PEP eingesetzt werden.

[4]In diesem Fall würden wir die Verwendung einer Bedingung empfehlen, die wir als nächstes diskutieren, damit IT-Administratoren nicht kontinuierlich und fortlaufend Zugang zum gesamten Netzwerk haben.

Zugang zu Systemen, die als „Abteilung=Marketing“ gekennzeichnet sind

Dieses Beispiel veranschaulicht einige der wirklichen Stärken eines Zero Trust-Systems, da es sich auf das PEP verlässt, um die Hosts tatsächlich aufzulösen, nachdem die Richtlinie dem Subjekt vom PDP gewährt wurde. Wir werden diesen Ablauf später in diesem Kapitel besprechen, aber vorerst ist dies ein Beispiel dafür, wie das Zero Trust-System das PEP verwendet, um die Richtlinie vollständig zu rendern, basierend auf seiner Fähigkeit, seine Umgebung zu befragen. Das heißt, der Ersteller der Richtlinie verlässt sich auf die Verwendung von Metadaten innerhalb des Laufzeitsystems der Organisation, um den Inhalt der Arbeitslast anzugeben, der letztendlich bestimmt, wer darauf zugreifen kann.

Die tatsächlichen Mechanismen, wie ein „Tag“ (in einigen Systemen als *Label* bezeichnet) angewendet und aufgelöst wird, werden implementierungsabhängig sein, aber die Details sind hier nicht relevant. Was zählt, ist das Konzept – dass Organisationen einen Mechanismus außerhalb der Standard-IT und Netzwerksteuerung verwenden können, um den Zugriff zu steuern, der Geschäfts- oder technische Prozesse und Sicherheit oft zum ersten Mal zusammenbindet. Zum Beispiel könnte eine Organisation ein Attribut innerhalb ihrer Configuration Management Database (CMDB) als Quelle für diese Informationen verwenden oder ein Metadatenattribut wie ein Tag innerhalb einer IaaS-Umgebung. In beiden Fällen ermöglicht dies IT- und Sicherheitsteams die Zusammenarbeit, wobei der Zero Trust-Verbrauch dieser Metadaten als leistungsstarker und automatisierter Integrationspunkt dient. Jeder Host, der auf diese Weise getaggt wird, würde automatisch vom Zero Trust-System erkannt und die entsprechende Menge an Zugriffsrichtlinien angewendet bekommen – was bedeutet, dass die richtige Menge an Benutzern automatisch das richtige Zugriffslevel erhält, einfach basierend auf der Verwendung dieses Tags.

Was an diesem Beispiel auch interessant zu bemerken ist, ist, dass es das Richtlinienmodell für Arten von Ressourcen öffnet, die nicht ausschließlich hostbasiert sind. Die modernen Anwendungen von heute sind häufiger als nicht containerisiert und/oder auf Mikrodiensten basierend und nicht direkt an ihren zugrunde liegenden Host gebunden. In diesen Fällen muss das Zero Trust-Richtlinienmodell in der Lage sein, zwischen verschiedenen Diensten zu unterscheiden und unterschiedliche Zugriffsstufen durchzusetzen, unabhängig davon, ob mehrere Dienste auf demselben physischen oder virtuellen Host laufen oder eine gemeinsame IP-Adresse teilen.

Zum Beispiel bieten Service-Mesh-Systeme wie **Istio** ein Richtlinienmodell, das dem Ansatz folgt, den wir hier beschreiben. Das Service-Mesh besteht aus einem verteilten Satz von PEPs, und ihre Autorisierungsrichtlinien beinhalten einen tag-basierten Mechanismus zur Auswahl von Richtlinienzielen und einen Mechanismus zur Angabe von Bedingungen.[5]

Zugang zu Systemen, die als „Stufe=Test“ gekennzeichnet sind

Dies ähnelt unserem vorherigen Beispiel, hat aber einen wichtigen Unterschied – die Verwendung eines Tags, der eine Bereitstellungsstufe anzeigt. Die Auswirkungen davon sind tiefgreifend, insbesondere in einer DevOps-Umgebung, wenn sie mit einer automatisierten Toolchain gekoppelt ist, die neue Versionen von Anwendungen oder Diensten kontinuierlich bereitstellt. In diesem Beispiel würde die Toolchain den Tag verwenden, um die entsprechende Entwicklungslebenszyklusstufe anzugeben, und das Zero Trust-System würde automatisch den richtigen Satz von Subjekten (entweder menschlich oder System) Zugang zu diesen Zielen gewähren. Das bedeutet, dass Subjekte automatisch und transparent den notwendigen Zugang als Nebenprodukt der Bereitstellungsprozesse erhalten. Wenn sich die Stufe einer Arbeitslast oder eines Dienstes ändert, folgen ihre Zugriffskontrollen automatisch, abgeleitet von diesem geänderten Status.

Aus unserer Sicht veranschaulicht dies schön die Stärke eines Zero Trust-Systems. Es nutzt technische Arbeit, die bereits durchgeführt wird (die Toolchain-getriebene Bereitstellung), und verwendet ein Attribut, um automatisch Zugriffsberechtigungen anzupassen. Die Nettoeffekt ist, dass Arbeitslasten genau den richtigen Satz von minimalen Zugriffskontrollen beibehalten, während sie durch ihren Lebenszyklus fortschreiten, ohne dass eine manuelle Intervention erforderlich ist. Dieser Ansatz kann sehr gut in eine DevOps-Organisation integriert werden, ihre Geschwindigkeit beibehalten und dabei Zero Trust-Sicherheitsprinzipien erreichen.

[5]Die eingebauten Bedingungen von Istio konzentrieren sich mehr auf Dienste und Netzwerke als auf Identitäten, aber sie enthalten einige experimentelle Erweiterungsfunktionen und könnten in zukünftigen Versionen in diese Richtung erweitern. Für weitere Informationen siehe `https://istio.io/latest/docs/concepts/security/`.

Zustand

Bedingungen spezifizieren die Umstände, unter denen das Subjekt tatsächlich die Aktion auf das Ziel ausführen darf. Beachten Sie, dass Richtlinienmodelle die Überprüfung einer sehr breiten Vielfalt von Bedingungen unterstützen sollten; tatsächlich sollte Ihre Zero Trust-Implementierung eine erweiterbare Reihe von Bedingungen unterstützen, damit Sie benutzerdefinierte Überprüfungen hinzufügen können. Bedingungen werden in der Regel gegen Geräte-, Authentifizierungs- oder Systemebenenattribute ausgewertet, obwohl einige Zero Trust-Implementierungen zusätzliche Typen unterstützen können.

Werfen wir einen Blick auf einige Beispiele für Bedingungen, die erfüllt sein müssen, damit der Zugriff erlaubt wird.

Die Uhrzeit liegt zwischen 08:00 und 18:00 Uhr

Zeitliche Einschränkungen sind eine bequeme und fokussierte Methode zur Zugriffskontrolle, effektiv für Benutzer mit gut definierten Rollen und regelmäßigen Arbeitszeiten. Diese Bedingung hilft, gegen gestohlene Anmeldeinformationen und Malware zu verteidigen, die versuchen könnten, außerhalb der Arbeitszeiten auf Ressourcen zuzugreifen. Diese Bedingung ist auch nützlich für geplante Wartungsfenster für immer aktive Geräte; stellen Sie sich eine Reihe von Einzelhandelsgeräten vor, die jede Nacht zwischen 01:00 und 03:00 Uhr eine Verbindung zu einem IT-Backend herstellen müssen. Es gibt keinen Grund, diese Netzwerkverbindung außerhalb dieses erlaubten Zeitfensters zu erlauben.

Diese Bedingung gibt uns ein klares Beispiel dafür, warum es notwendig ist, dass das PEP in der Lage sein muss, die Darstellung der Richtlinie abzuschließen. Eine Identität darf sich nur einmal pro Tag beim PDP authentifizieren, aber das PEP muss in der Lage sein, die aktuelle Zeit mit den erlaubten Zeitfenstern während des Tages zu vergleichen.

Der Benutzer hat innerhalb der letzten 90 Minuten eine gültige MFA oder Step-Up-Authentifizierung durchgeführt

Wir sind große Fans der angemessenen Verwendung von MFA, und diese Art von Bedingung sollte eine obligatorische (und häufige) Zutat in jeder Zero Trust-Implementierung sein. Wann und wie eine Step-Up-Authentifizierung erforderlich ist,

ist natürlich ein Balanceakt, und Sie müssen sowohl das Benutzererlebnis als auch das Bedrohungsmodell, gegen das Sie sich verteidigen, berücksichtigen. Bestimmte hochriskante oder hochwertige Anwendungen können es rechtfertigen, bei jeder Sitzungsinitiierung eines Benutzers nach MFA zu fragen, aber in vielen Fällen ist es ebenso effektiv und weniger aufdringlich, MFA einmal für eine gesamte Gruppe von Ressourcen zu verlangen und diese für einen bestimmten Zeitraum gültig zu halten. Auch diese Art von Bedingung muss vom PEP ausgewertet und durchgesetzt werden; die Step-Up-Authentifizierung kann zu einer beliebigen Zeit aufgrund des Benutzerzugriffs durch das PEP ausgelöst werden, und das PDP wird höchstwahrscheinlich nicht in diesen Ablauf eingebunden sein.

Beachten Sie, dass es eine Vielzahl von Ansätzen und Lösungen als zweite Faktoren gibt, einschließlich FIDO2, Smartphone-Apps, Push-Benachrichtigungen und Biometrie. Zero Trust-Plattformen sollten alle oder einige davon über standardisierte APIs unterstützen, um Ihnen die Möglichkeit zu geben, diejenigen auszuwählen, die am besten für Ihre Umgebung geeignet sind.

Gerätehaltung erfüllt Anforderungen: Anti-Malware-Dienst läuft

Diese Bedingung wird verwendet, um zu validieren, dass das Gerät des Subjekts die Sicherheitsanforderungen erfüllt. Beachten Sie, dass in diesem Beispiel auf Informationen zurückgegriffen wird, die vom Gerät selbst abgerufen wurden. Die Überprüfung, ob der Anti-Malware-Dienst derzeit ausgeführt wird, kann vom Benutzeragenten PEP oder von einer anderen Softwarekomponente auf dem Gerät durchgeführt werden, aber bedenken Sie, dass alle Informationen, die von einem Gerät gesendet werden, nur teilweise vertrauenswürdig sein sollten.

Obwohl viele IT- und Sicherheitsorganisationen eine ordnungsgemäße Sicherheitshygiene auf Benutzergeräten durchführen, wie zum Beispiel durch die Einschränkung von Administrationsrechten, ist es natürlich möglich, dass Malware auf dem Gerät falsche Informationen zurückgibt. Daher ist eine Anzeige, dass ein Anti-Malware-Dienst auf einem Gerät läuft, nützliche Information und durchaus gültig, um sie als Bedingung durchzusetzen, sie sollte jedoch nur als eine Komponente der Verteidigung in der Tiefe betrachtet werden.

Gerätehaltung erfüllt Anforderungen: Sicherheitsscan des Endpunkts wurde vor weniger als 48 Stunden abgeschlossen

Diese Bedingung verwendet Gerätehaltungsinformationen, die von einem Sicherheitsscanning-Tool, wie einer Endpunktverwaltungs- oder Schwachstellenscanning-Lösung, abgerufen wurden. Da das PEP diese Informationen von einem Server und nicht von einem Gerät abruft, kann es als vertrauenswürdiger behandelt werden.[6] Beachten Sie, dass in diesem Beispiel die Bedingung zufällig erfordert, dass ein Sicherheitsscan kürzlich abgeschlossen wurde. Ein anderer Ansatz könnte darin bestehen, aktuellere Informationen zu nutzen, wie zum Beispiel das PEP dazu zu bringen, einen Anruf bei einem Überwachungssystem wie einem SIEM oder UEBA zu tätigen, und nahezu Echtzeitinformationen über das Risikoniveau des betreffenden Geräts zu erhalten.

Ein Service Desk Ticket ist in einem *Offenen* Zustand für diese Ressource

Diese Bedingung ist eines der interessantesten und überzeugendsten Beispiele dafür, wie Zero Trust-Systeme Sicherheitsdurchsetzung und Geschäftsprozesse verbinden können. Wie das Metadaten-Tag-Beispiel, das wir für Ziele besprochen haben, ermöglicht dies Organisationen, ihre gewünschten Geschäftsprozesse zu nutzen. Indem der Zugriff – durch das Netzwerk oder die Anwendung durchgesetzt – ein Nebenprodukt eines ordnungsgemäß ausgeführten Geschäftsprozesses ist, garantiert es, dass die Benutzer den Prozess befolgen. Dies kann enorme Vorteile in Bezug auf Nachvollziehbarkeit, Wiederholbarkeit und Qualität haben, ganz zu schweigen von der Sicherheit.

In diesem Beispiel möchte die Organisation sicherstellen, dass der IT-Admin-Zugriff auf eine bestimmte Ressource nur erlaubt (und nur möglich) ist, wenn es ein Service Desk-Ticket im *offenen* Zustand gibt, das dieser Ressource entspricht. Das Ergebnis dieser Richtlinie ist, dass Stakeholder gezwungen sein werden, ein Service Desk-Ticket zu erstellen, damit ein IT-Admin auf die Ressource zugreifen und die notwendige

[6]Natürlich ist kein System perfekt, und das Sicherheitssystem könnte es versäumt haben, Malware auf dem Gerät zu erkennen, oder es könnte selbst kompromittiert sein und falsche Informationen zurückgeben.

Aufgabe ausführen kann. Und sobald das Ticket geschlossen ist, wird der Admin-Zugriff auf diese Ressource widerrufen. Dies beseitigt die Notwendigkeit, dass Admins und ihre Geräte einen breiten und kontinuierlichen Netzwerkzugriff haben, während sie voll produktiv bleiben. Es stellt auch sicher, dass alle Admin-Zugriffe aus Compliance-Gründen verfolgt werden.

Dieses Service Desk-Ticket ist nur ein Beispiel; Zero Trust-Systeme können im Grunde genommen mit jedem Geschäftsprozess auf ähnliche Weise integriert werden, was erhebliche Vorteile für die gesamte Organisation bringt.

Sowohl das Subjekt als auch das Ziel müssen als Server gekennzeichnet sein, die sich in einem „Produktions"-Zustand befinden

In diesem Beispiel sind sowohl das Subjekt als auch die Ziele Server und haben ein Tag, das zur Kennzeichnung ihres Zustands verwendet wird. Diese Bedingung ist eine Möglichkeit, zu verhindern, dass Entwicklungs- oder Test-Apps (oder Entwickler, die an Nicht-Produktionssystemen arbeiten) versehentlich mit einem Produktionsservice verbinden. Natürlich sollte es zusätzliche Kontrollschichten über die Authentifizierung geben – zum Beispiel könnten Anwendungsanmeldeinformationen oder ein Zertifikat benötigt werden, abhängig vom Service-zu-Service-Authentifizierungsmodell. Aber besonders in Umgebungen mit manuellen Tests oder Freigabeschritten ist es zu einfach für Entwickler, einen Fehler zu machen; oft wird diese Arbeit über die Befehlszeile durchgeführt, wo es einfach ist, einen einfachen Kopier- und Einfüge- oder Tippfehler zu machen, der erhebliche Auswirkungen haben kann.

Diese Art von Kontrolle – unter Verwendung von Metadaten sowohl des Subjekts als auch des Zielservices – könnte erweitert werden, um weitere Einschränkungen zu definieren, zum Beispiel nach Anwendungs- oder Projektname. Während es unwahrscheinlich ist, dass ein Anwendungsservice, der Teil des Projekts *oriole* ist, versehentlich versucht, eine Verbindung zu einem Service innerhalb des Projekts *bluejay* herzustellen, ist es sicherlich möglich, dass ein bösartiger Benutzer oder Malware mit Zugriff auf den Host dieser Anwendung versuchen könnte, Netzwerkerkundungen oder seitliche Bewegungen durchzuführen. Unser Prinzip der geringsten Privilegien sollte uns dazu veranlassen, diese Art von Richtlinien zu haben, sobald unsere Zero Trust-Infrastruktur und Sicherheitsreife dafür bereit sind.

Subjektkriterien vs. Bedingungen

Während wir diese Beispiele durchgegangen sind, haben Sie wahrscheinlich bemerkt, dass es einige Überprüfungen gibt, die entweder in die Subjektkriterien oder in die Bedingungen passen könnten. Das ist in Ordnung – es gibt nicht unbedingt feste Regeln dafür, und Sie müssen einige Urteilsentscheidungen darüber treffen, basierend auf den Besonderheiten Ihrer Organisation und Ihrer gewählten Plattform. Mit zunehmender Erfahrung sollte Ihnen klar werden, welcher Ansatz am besten funktioniert.

Im Allgemeinen sollten Sie in Betracht ziehen, dass einige Arten von Überprüfungen besser geeignet sind, um sie in der PDP zum Zeitpunkt der ersten Sitzungseinrichtung durchzuführen (wie zum Beispiel während der Identitätsauthentifizierung), auch wenn die PEP technisch in der Lage ist, sie durchzuführen. Diese Überprüfungen beziehen sich in der Regel auf Attribute, die sich langsam ändern und daher wahrscheinlich für die Dauer einer Benutzersitzung fest bleiben. Natürlich hängt es davon ab, wie die spezifische Zero Trust-Plattform implementiert ist, aber zum Beispiel sind Betriebssystemversion und Geolokalisierung unwahrscheinlich, dass sie sich ändern, während eine aktive Sitzung aufrechterhalten wird. Wir werden später in diesem Kapitel untersuchen, welche Attribute wo bewertet werden sollten.

Beispielrichtlinien

Jetzt, da wir uns angesehen haben, wie Richtlinien erstellt werden und einige Beispiele für ihre Komponenten überprüft haben, lassen Sie uns sie in einigen Beispielrichtlinien zusammenstellen, die einige der Möglichkeiten aufzeigen, wie diese Komponenten miteinander verknüpft werden können.

Unsere erste Beispielrichtlinie ist die, die wir in Kap. 3 vorgestellt haben, als wir das Richtlinienmodell erstmals erklärten, dargestellt in Tab. 17-2.

In diesem Fall werden die Subjektkriterien diese Richtlinie Benutzern zuweisen, die Mitglieder der angegebenen Identitätsanbietergruppe, Dept_Billing, sind. Beachten Sie, dass in dieser Organisation nur Mitarbeiter in ihrem Identitätsanbieter gespeichert sind, so dass es keinen Grund gibt, eine zusätzliche Überprüfung für diese Rolle innerhalb der Kriterien durchzuführen, da sie implizit ist. Beachten Sie auch, dass in diesem Beispiel nicht überprüft wurde, ob der Benutzer tatsächlich ein aktives Konto in der Abrechnungsanwendung hat. Dies hätte nützlich sein können, falls *einige* aber nicht *alle* Mitglieder der Abrechnungsabteilung aktive Benutzer dieser Anwendung sind. Dies ist

Tab. 17-2. *Beispiel Richtlinie – Benutzerzugriff auf die Abrechnungsanwendung*

Richtlinie: Benutzer in der Abrechnungsabteilung müssen in der Lage sein, die Webanwendung für die Abrechnung zu nutzen	
Subjektkriterien	Benutzer, die Mitglieder der Gruppe Dept_Billing im Identity Provider sind
Aktion	Benutzer müssen in der Lage sein, auf die Web-UI über Port 443 über HTTPS zuzugreifen
Ziel	Die Abrechnungsanwendung mit dem FQDN billing.internal.company.com
Bedingung	Benutzer können vor Ort oder remote sein Remote-Benutzer müssen vor dem Zugriff (zum Zeitpunkt der Authentifizierung) oder einmal in jedem 4-Stunden-Fenster zur MFA aufgefordert werden Benutzer müssen diese Anwendung von einem firmeneigenen Gerät mit laufender Endpunktsicherheitssoftware aus zugreifen

ein interessanter Punkt und zeigt ein ziemlich häufiges Vorkommen – wo eine Organisation keine Identitätsgruppe hat, die perfekt zu der Gruppe von Benutzern passt, die eine bestimmte Aktion erhalten sollten.

Das ideale Szenario für Zero Trust-Richtlinien besteht natürlich darin, das Prinzip der geringsten Privilegien durchzusetzen und nur genau dem richtigen Satz von Benutzern Zugriff zu gewähren. Eine unvollkommene Zero Trust-Implementierung ist jedoch besser als keine, und wir glauben, dass es besser ist, mit einer Richtlinie voranzukommen, die einigen zusätzlichen Benutzern Zugriff gewährt, anstatt auf Änderungen in einem Identitätsmanagementprogramm und -prozess warten zu müssen, um eine „perfekte“ Gruppenzuordnung zu erreichen. Denken Sie daran, dass wir dies in Kap. 5 angesprochen haben – dies ist ein großartiges Beispiel dafür, wie ein Zero Trust-Projekt voranschreiten und Wert liefern kann, während das Identitätsteam auf einem separaten parallelen Weg fortschreitet.

Zurück zu unserem Beispiel, die Aktion in diesem Fall ist einfach – nur die Fähigkeit, auf die Web-UI über HTTPS zuzugreifen – und das Ziel ist ein einfacher vollqualifizierter Domainname. Die Bedingungen, die zur Durchsetzung einiger Kontrollen verwendet werden, sind jedoch interessanter. Zunächst müssen Remote-Benutzer eine MFA-Aufforderung eingeben, wenn sie auf diese Anwendung zugreifen, und 4 Stunden später erneut. Benutzer, die im (vertrauenswürdigeren) internen Firmennetzwerk arbeiten, müssen keine MFA eingeben, da ihre physische Präsenz im Gebäude als zusätzlicher

Faktor betrachtet werden kann. Die Bedingungen erfordern auch, dass das Gerät firmeneigen ist (validiert durch das Vorhandensein eines gültigen Zertifikats, das von der Firmen-CA ausgestellt wurde) und dass die Endpunktsicherheitslösung des Unternehmens auf diesem Gerät läuft.

Dies ist eine vernünftige und ausgewogene Reihe von Bedingungen nach unserer Einschätzung, die es entfernten Benutzern ermöglicht, produktiv zu sein, während sie nur ein minimales Maß an Ärger verursacht und den Zugriff nur von gültigen, vom Unternehmen verwalteten Geräten erzwingt. Werfen wir einen Blick auf ein weiteres Beispiel, das in gewisser Weise sogar einfacher ist, basierend auf einigen Einschränkungen in ihrer Umgebung.

Im Beispiel in Tab. 17-3 verwendet die Organisation die Richtlinie, um den Sysadmin-Zugriff auf Produktionsserver zu steuern. Ihre Sysadmins benötigen Remote-Zugriff (SSH, SFTP, Web und RDP) auf Server oder Netzwerkgeräte in ihrem großen Produktions-Subnetz, das Tausende von Hosts enthält. Jeden Arbeitstag müssen diese Sysadmins sich mit einigen dieser Systeme verbinden, um sie zu aktualisieren, neu zu konfigurieren oder Fehler zu beheben. Die Organisation möchte nicht, dass ihre Admins einen weit offenen und dauerhaften Zugriff auf dieses Netzwerk haben, aber sie müssen auch ihre Admins in die Lage versetzen, ihre Arbeit zu erledigen, was bedeutet, dass sie jeden Tag Zugriff auf eine willkürliche und unvorhersehbare Menge von Hosts benötigen.

Diese Beispielrichtlinie löst dieses Problem für sie, indem sie die Zugriffskontrolle an einen Geschäftsprozess bindet – die Nutzung ihres Service-Desk- (Ticketing-) Systems. Mit dieser Richtlinie hält die Organisation ihre Admins produktiv und stellt sicher, dass alle Zugriffe auf diese Produktionssysteme protokolliert werden.

Beachten Sie, dass unsere Beispielorganisation, wie viele reale Unternehmen, in einigen Bereichen reifer und in anderen weniger reif ist. In diesem Beispiel zeigt die

Tab. 17-3. *Beispiel Richtlinie – Admin-Zugriff auf Produktions-Subnetz*

Richtlinie: Sysadmin-Zugriff auf Produktions-Subnetz	
Subjektkriterien	Benutzer, die Mitglieder der Gruppe Sysadmins im Identitätsanbieter sind
Aktion	Benutzer können auf TCP-Ports 22, 3389 und 443 zugreifen und ICMP-Ping verwenden
Ziel	Jeder Host im Subnetz 10.0.0.0/8
Bedingung	Es muss ein Service-Desk-Ticket im „offenen“ Zustand vorliegen, das den Hostnamen oder die IP-Adresse angibt, auf die zugegriffen wird

Nutzung des Service-Desks als zuverlässigen und regelmäßigen Prozess zur Steuerung von Sysadmin-Aufgaben ein beträchtliches Maß an Reife. Andererseits deutet die Gewährung sowohl von SSH- als auch von RDP-Zugriff für jeden Server darauf hin, dass sie kein genaues Asset-Management-System haben, auf das sie sich verlassen können, um Hosts auf Betriebssystemtypen abzubilden. Diese Beispielrichtlinie hat auch keine MFA damit verbunden. Vielleicht gibt es in dieser fiktiven Organisation eine kulturelle Widerstand gegen die Nutzung davon, oder vielleicht verwendet die Organisation eine Art von ausgleichender Kontrolle, wie einen Credential Vault.

Die in Tab. 17-4 gezeigte Beispielrichtlinie veranschaulicht die Verwendung eines dynamisch gerenderten Ziels, bei dem das PEP die Metadaten für Ziele in einer IaaS-Umgebung bewertet. Obwohl die Aktionen weit offen sind, ist dies angemessen, da es sich um eine Entwicklungs-Umgebung handelt. Diese Richtlinie gibt den Entwicklern die volle Möglichkeit, in ihrer IaaS-Umgebung zu arbeiten, während sichergestellt wird, dass sie nicht auf die Ressourcen anderer Projekte zugreifen können.

Unsere letzte Beispielrichtlinie, in Tab. 17-5, veranschaulicht ein Server-zu-Server-Szenario und zeigt, wie ein Unternehmen eine Richtlinie definieren könnte, die es einem

Tab. 17-4. *Beispiel Richtlinie – Entwicklerzugriff*

Richtlinie: Entwicklerzugriff auf Projekt „Everest“ Ressourcen	
Subjektkriterien	Das Subjekt muss Mitglied der Project_Everest Verzeichnisgruppe sein
Aktion	Alle TCP-, UDP- und ICMP-Aktionen
Ziel	Jede Ressource in der IaaS-Entwicklungsumgebung, die als „project=Everest“ gekennzeichnet ist
Bedingung	Keine (der Zugriff ist immer erlaubt)

Tab. 17-5. *Beispiel Richtlinie – Server-zu-Server-Zugriff*

Richtlinie: Webserver in DMZ greift auf Datenbankserver zu	
Subjektkriterien	Das Subjekt muss den Hostnamen ws1.company.com oder ws2.company.com haben
Aktion	Zugriff auf TCP-Port 3306
Ziel	Host app1database.internal.company.com
Bedingung	Keine (der Zugriff ist immer erlaubt)

Webserver, der in der DMZ läuft, erlaubt, auf seinen zugehörigen Datenbankserver im privaten internen Netzwerk zuzugreifen. Man kann sich leicht vorstellen, dass diese Webanwendung die Frontend für eine E-Commerce-Site bereitstellt, mit einer Vielzahl von Backend-Diensten, die mit der Kern-Datenbank interagieren (zum Beispiel zur Aktualisierung des Inventars oder zur Bearbeitung von Bestellungen). In diesem Beispiel gibt es mehrere Instanzen des Webservers für Lastverteilung und HA-Zwecke, und ihre internen IP-Adressen ändern sich regelmäßig aufgrund der zugrunde liegenden virtuellen Infrastruktur, wobei neue Versionen häufig bereitgestellt werden. Diese einfache Richtlinie hilft der Organisation, den Zugriff automatisch anzupassen, auch auf ihrer sich ändernden Infrastruktur, während sie eine strenge Sicherheit beibehält.

Richtlinien, angewendet

Dieses Richtlinienmodell sollte Ihnen eine Struktur bieten, mit der Sie über Zugriffsregeln nachdenken und diese erstellen können, auf eine Weise, die sowohl für technische als auch für nicht-technische Stakeholder sinnvoll ist. Es sollte auch hilfreich sein, wenn Sie potenzielle Zero Trust-Produkte analysieren, um Ihnen ein Gefühl für die Arten von Fähigkeiten zu geben, die Sie benötigen.

Natürlich existieren diese Richtlinien nicht im Vakuum – sie erfordern Attribute (kontextuelle Eingaben), um bewertet zu werden, sie müssen erstellt werden, um spezifische Szenarien zu erfüllen, und sie haben einen Fluss in Bezug auf wann und warum sie bewertet werden. In diesem Abschnitt werden wir uns mit jedem dieser Aspekte von Richtlinien befassen, beginnend mit Attributen.

Attribute

Zero Trust-Richtlinien basieren auf den Attributen, die mit Identitäten, Geräten, Zielen und dem gesamten Unternehmenssystem verbunden sind. Wie im Richtlinienmodell dargestellt, werden diese Attribute in Subjektkriterien, in Zielen und in Bedingungen referenziert. Attribute sind der Schlüssel zur Erreichung der Kontextsensitivität von Richtlinien und zur Erlangung der für Zero Trust benötigten Skalierung und Dynamik und fallen in drei Kategorien.

Identitätsattribute werden in der Regel vom Identitätsanbieter abgerufen, der die Identität authentifiziert, obwohl sie natürlich mit Attributen aus anderen Quellen

ergänzt werden können. Identitätsattribute umfassen Verzeichnisgruppenmitgliedschaften sowie direkt zugewiesene Attribute wie Rollen. Jede Organisation wird wahrscheinlich benutzerdefinierte Gruppen erstellen und ihren Identitäten benutzerdefinierte Attribute zuweisen, und die Verwendung dieser Attribute in Richtlinien durch Zero Trust-Systeme ist eine Kernfähigkeit, die unbedingt vorhanden sein muss.

Geräteattribute können direkt vom Gerät abgerufen werden (typischerweise über einen lokalen Agenten) oder von einem externen System wie einem CMDB oder einem Endpunkt-Management-System. Einige Geräteattribute, insbesondere solche, die von einem lokalen Prozess auf dem Gerät erhalten werden, können sich recht häufig ändern. Die relative Beständigkeit von Attributen ist etwas, das wir im folgenden Text diskutieren, und sollte definitiv ein Faktor sein, wenn Sie entscheiden, wo, wann und wie Sie sie bewerten.

Es gibt eine weitere Reihe von Attributen zu berücksichtigen, die wir als *Systemattribute*. Diese Kategorie ist ein bisschen ein Sammelsurium und bezieht sich auf die Attribute, die mit dem breiteren Unternehmensnetzwerk und Ökosystem verbunden sind. Dies kann Dinge wie das allgemeine Netzwerkbedrohungs- oder Risikoniveau (vielleicht von einem SIEM erhalten), System- oder Netzwerklast oder sogar Attribute, die mit Geschäftsprozessen oder IT-Funktionen verbunden sind, wie zum Beispiel, ob dies ein genehmigtes Wartungsfenster ist oder ob es eine Notfall-IT-„Breakglass“-Situation gibt.

Schließlich werden *Zielattribute* verwendet, um Ziele für Aktionen zu bestimmen, wie wir zuvor besprochen haben. Diese können abgerufen werden, indem das PEP seine lokale Umgebung abfragt, oder vielleicht von einer zentralisierten und autoritativen Quelle wie einem CMDB.

Beachten Sie, dass wir in unserer Diskussion über Attribute dies aus der Sicht betrachtet haben, dass das Zero Trust-System Attribute von externen Quellen abruft. Während dies definitiv ein häufiges Szenario sein wird, ist es nicht die einzige Möglichkeit. Es ist durchaus sinnvoll, dass das Zero Trust-System selbst ein Repository für Attribute ist. In diesem Fall muss es natürlich eine Reihe von Mechanismen geben, um die Attribute zu bevölkern und zu aktualisieren – denken Sie daran, dass wir dies in Kap. 11 abgedeckt haben, wo wir die Sicherheitsorchestrierung diskutiert haben.

Angesichts all dessen werfen wir einen Blick auf die Änderungsrate verschiedener Typen von Attributen. Die Tabelle der Attributbeständigkeit ist in Tab. 17-6 dargestellt,

Tab. 17.6 *Attributbeständigkeit*

Attributbeständigkeit	Identitätsattribute (Benutzer)	Geräteattribute	Systemattribute	Zielattribute
Permanent (niemals ändern)	Biometrie (z. B. Fingerabdrücke, Iris-Scan)	Betriebssystem	*Keine*	Betriebssystem
Halbpermanent (weniger als eine Änderung pro Jahr)	Staatsbürgerschaft Wohnsitzland Zertifizierungen Sicherheitsfreigaben	Hostname	Domain	Identifikator Hostname URL
Selten (monatliche oder jährliche Änderungen)	Gruppenmitgliedschaften Rollen Projektzuweisungen	OS-Version oder Patch-Level Komponenten-Patch-Level (z. B. AV-Signaturdatei)	DNS-Server-Einstellungen	IP-Adresse Zertifikatsinformationen Netzwerkinformationen (z. B. TLS-Parameter) Ressourcen-Version
Regelmäßig (wöchentliche Änderungen)	Keine	Geräte-Posture-Check Registry-Schlüssel Werte	*Keine*	Ziel-Posture-Check
Häufig (stündliche oder tägliche Änderungen)	Geolokalisierung Netzwerkattribute	Prozessstatus Geräte-IP-Adresse	Netzwerk-Risikolevel Netzwerklast Notfall-Situation	Ressourcenlast Ressourcenverfügbarkeit

zusammen mit Beispielen für Attribute und ihrer allgemeinen Häufigkeit der Änderung. Betrachten Sie diese nicht als feste Regeln, sondern eher als eine Reihe von Richtlinien. Selbst „permanente“ biometrische Attribute könnten sich tatsächlich ändern, zum Beispiel aufgrund von Verletzungen oder Transplantationen. Und Ihre Organisation

könnte einige Richtlinien zur Vermögensverwaltung haben, die zum Beispiel die relative Beständigkeit bestimmter Geräteattribute beeinflussen könnten.

Insgesamt glauben wir, dass diese Tabelle nützlich sein wird, weil sie Ihnen helfen kann, die Arten von Attributen zu verstehen, die existieren, und zu entscheiden, wo und wie oft Sie in Betracht ziehen sollten, sie zu bewerten (z. B. zur Authentifizierungszeit vs. zur Zugriffszeit).

In der Praxis macht es Sinn, häufig wechselnde Attribute in den PEPs zu validieren, wahrscheinlich als Teil einer Bedingung. Dies liegt daran, dass diese Attribute innerhalb einer aktiven Sitzung ändern können, und die PEPs sind der Mechanismus für diese Art von Zugriffszeit-Durchsetzung. Längerlebige Attribute könnten sinnvoll sein, als Teil der Subjektkriterien in der PDP zu bewerten. Natürlich sollten Sie diese als Richtlinien behandeln, da Ihre gewählte Zero Trust-Plattform die Dinge möglicherweise anders angeht.

Richtlinienszenarien

Jetzt, da wir die Struktur der Richtlinien und die Menge der Attribute, die als Eingabe in sie verwendet werden, untersucht haben, ist es an der Zeit, dass wir uns die häufigsten Szenarien ansehen. Damit meinen wir die Muster und Zugriffsmethoden, mit denen Subjekte auf Ziele zugreifen. Aber zuerst wollen wir sicherstellen, dass wir unsere Richtlinien und Annahmen gut verstehen.

Zuerst (mit Ausnahme von IoT-Systemen, die wir in Kap. 16 besprochen haben), muss es immer mindestens ein Subjekt in jeder Zero Trust-Aktion geben, die durchgeführt wird, wobei Subjekte authentifizierte Identitäten sind. Das heißt, nicht authentifizierte Identitäten können keine Subjekte sein, obwohl sie sicherlich Ziele sein können. Zweitens wird wahrscheinlich ein gewisses Maß an Kommunikation auf einem Netzwerk außerhalb der Kontrolle des Zero Trust-Systems innerhalb der impliziten Vertrauenszone stattfinden. Sie müssen über die Grenzen Ihrer impliziten Vertrauenszone nachdenken und explizite Entscheidungen darüber treffen, und sie sollte im Laufe der Zeit schrumpfen, während Sie Fortschritte auf Ihrer Zero Trust-Reise machen. Während Ihrer Reise wird es oft eine gemischte Menge an Kommunikation zu Zero Trust-Ressourcen geben, wobei ein Teil der Kommunikation durch PEPs erfolgt

(und den Zero Trust-Richtlinien unterliegt), während es eine gewisse Kommunikation, sogar zu den gleichen Ressourcen, geben wird, die die Zero Trust PEP umgeht.

Schließlich beachten Sie, dass Ressourcen, auf die nicht autorisierte Benutzer zugreifen können (wie öffentliche Webserver), außerhalb des Geltungsbereichs von Zero Trust-Richtlinienmodellen liegen. Diese Systeme gewähren bewusst einem *jedem* entfernten System ein gewisses Vertrauen, indem sie es erlauben, sich mit der Ressource zu verbinden und diese zu nutzen. Natürlich können auch auf einem öffentlich zugänglichen Webserver andere Dienste wie der administrative Zugriff auf diesen Host im Geltungsbereich eines Zero Trust-Systems liegen (und sollten es wahrscheinlich auch). Das heißt, die Anforderung von Zero Trust, dass alle Subjekte authentifizierte Identitäten sein müssen, wird Ihnen helfen, klare Grenzen für Ihr System zu ziehen. Beachten Sie, dass einige Ressourcen in Ihrer Umgebung zwar außerhalb des Geltungsbereichs von Zero Trust liegen, sie aber definitiv immer noch im Geltungsbereich Ihres Sicherheitsteams liegen und durch einen angemessenen Satz von Kontrollen geschützt werden müssen.

Betrachten wir nun mehrere Szenarien, die unsere Diskussionen über das Richtlinienmodell mit den Zero Trust-Bereitstellungsmodellen verbinden. Beachten Sie, dass wir in all diesen Diagrammen den PDP zur Klarheit weggelassen haben.

Dieses erste Szenario, in Abb. 17-1, zeigt eine einfache Bereitstellung, die das Enklaven-basierte Zero Trust-Bereitstellungsmodell verwendet. In diesem Beispiel ist das einzige Richtlinienziel der Webserver, der den Zugriff des Benutzers darauf kontrolliert. Alle drei dargestellten Server befinden sich innerhalb der impliziten Vertrauenszone von Zero Trust, so dass ihr Zugriff aufeinander nicht vom PEP kontrolliert wird. Das heißt, der PEP kontrolliert nur den Zugriff des Subjekts auf den Webserver.

In dem in Abb. 17-2 gezeigten Szenario wurde der Datenbankserver teilweise hinter einem PEP platziert, so dass er ein Ziel innerhalb einer Richtlinie sein kann. In diesem

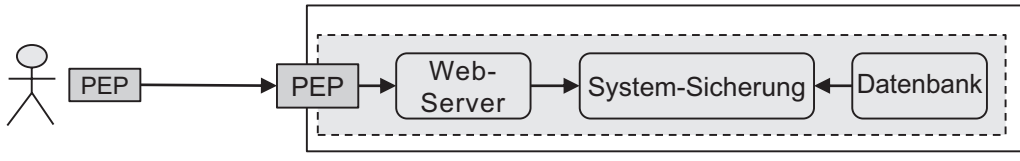

Abb. 17-1. *Richtlinienszenario – Webserver als Ziel*

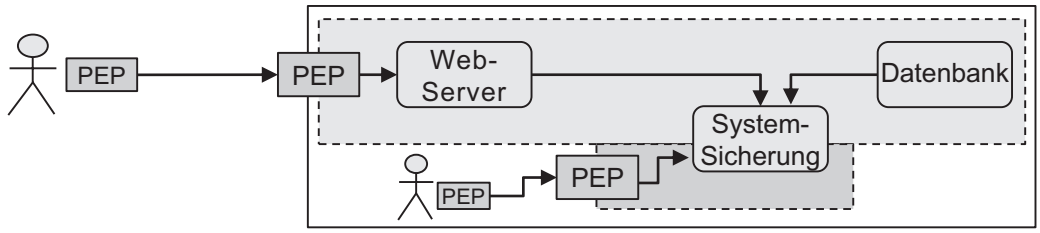

Abb. 17-2. *Richtlinienszenario – Datenbankserver als Ziel*

Beispiel hat die Organisation den IT-Administratorzugriff auf den Datenbankserver eingeschränkt, so dass er nur von einer authentifizierten Identität über eine zugewiesene Richtlinie zugegriffen werden kann. Der Webserver und das Backup-System haben jedoch weiterhin direkten Zugriff auf den Datenbankserver, da sie sich innerhalb der impliziten Vertrauenszone befinden. In der Praxis würde dies durch Firewall-Einstellungen erreicht werden, so dass der Admin-Zugriff (über Port 22) nur über den PEP erreichbar ist, während der Datenbankzugriff (z. B. Port 3306) für jeden anderen Server innerhalb der größeren impliziten Vertrauenszone zugänglich ist.

Dies dient als gutes Beispiel aus der Praxis, wie eine Organisation schrittweise zu Zero Trust übergehen kann – indem sie die verschiedenen Dienste, die auf dem Datenbankserver laufen, als unterschiedliche logische Ziele behandelt, können sie ihre Sicherheit verbessern, indem sie den Admin-Zugriff streng kontrollieren, ohne ihre Anwendungs- oder Geschäftsbetrieb überhaupt zu beeinträchtigen. Dies kann eine vorübergehende Phase sein oder auch nicht; Abb. 17-3 zeigt einen möglichen nächsten Schritt auf diesem Weg.

Abb. 17-3 zeigt, wo die Organisation auch den Datenbankserver hinter einen PEP gestellt hat, so dass nur authentifizierte Subjekte darauf zugreifen können.[7] Die Auswirkungen davon sind, dass der Webserver nun ein Subjekt sein muss, mit einer Identität und einer Möglichkeit zur Authentifizierung. Die Ergebnisse sind eine reduzierte implizite Vertrauenszone (Verbesserung der Sicherheit) sowie verbesserte Bereitstellungsflexibilität.

Dieses letztere Ergebnis ist ein interessanter und oft übersehener Vorteil von Zero Trust. Da der Zugriff des Webservers auf den Datenbankserver nun über das Zero Trust-System erfolgt, kann die Datenbank überall in der Infrastruktur des Unternehmens

[7]In diesem Beispiel kann der System-Backup-Server weiterhin direkt auf die Datenbank zugreifen, zum Beispiel über Firewall-Regeln und/oder einen bestimmten TCP-Port.

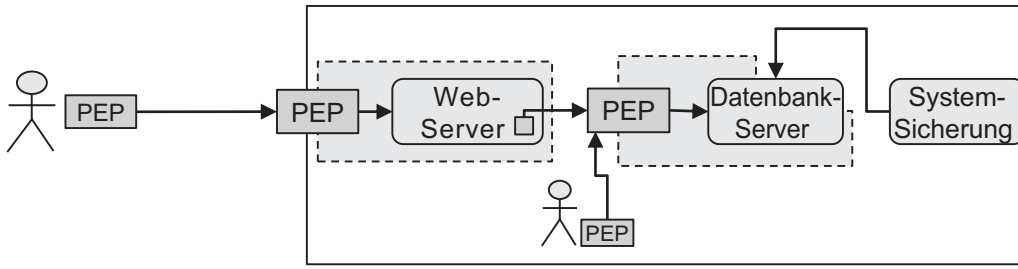

Abb. 17-3. *Richtlinienszenario – Webserver als Subjekt*

verschoben werden, ohne dass dies Auswirkungen auf den Webserver hat, außer vielleicht für eine zusätzliche Latenz. Das heißt, der Bereitstellungsort des Datenbankservers wird im Grunde genommen irrelevant für den Webserver und kann transparent an einen entfernten oder cloudbasierten Ort verlegt werden. Ohne Zero Trust könnte die Organisation dies nicht erreichen, ohne irgendeine Art von Remote-Zugriffsmechanismus bereitzustellen, typischerweise über eine WAN-Verbindung. Das bringt eine ganze Reihe von Sicherheits- und Netzwerküberlegungen mit sich, sowie wahrscheinlich zusätzliche Kosten. Der Einsatz eines PEP und einer Richtlinie zur Bereitstellung des Zugriffs ist weitaus einfacher, schneller und sicherer.

Zielinitiierter Zugriff

Unser nächstes Szenario führt das Konzept einer *zielinitiierten* Aktion ein. Bisher wurde unser Diskurs und unser Richtlinienmodell aus der Perspektive eines authentifizierten Subjekts betrachtet, das auf eine Ressource zugreift, über einen PEP. Das heißt, das Gerät des Subjekts initiiert die Verbindung (bei Verwendung eines verbindungsorientierten Protokolls wie TCP) oder initiiert den Netzwerkverkehr (bei Verwendung eines verbindungslosen Protokolls wie UDP). Die vorherigen Szenarien, in denen ein Benutzer auf einen Webserver zugreift und ein Webserver auf eine Datenbank zugreift, sind gute Beispiele für dieses Muster.

Einige Anwendungen und Netzwerke nutzen jedoch eine umgekehrte Art der Kommunikation, was bedeutet, dass unser Zero Trust-System dies ebenfalls unterstützen muss, um unsere Ziele der Sicherung aller Kommunikationen über Richtlinien zu erreichen. Dieses Muster nennen wir *zielinitiiert:* Wir haben immer noch ein authentifiziertes Subjekt und einen Zugriff, der von einem PEP kontrolliert wird, aber der Netzwerkverkehr wird vom Ziel der Richtlinie initiiert und der Verkehr oder die

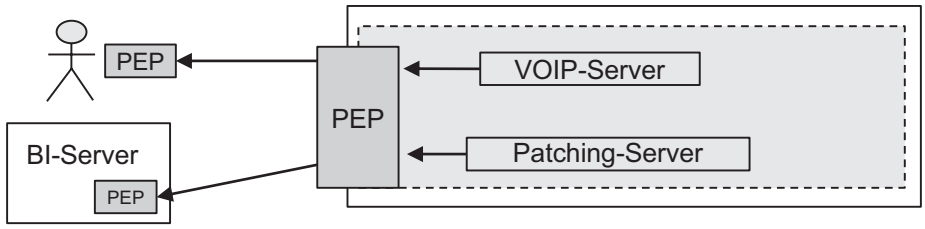

Abb. 17-4. *Richtlinienszenario – Zielinitiiert, Enklavenbasiert*

Verbindung wird zum Subjekt gesendet. Lassen Sie uns ein Beispiel untersuchen, das dies konkret macht.

In Abb. 17-4 verwendet das Zero Trust-System das enklavenbasierte Bereitstellungsmodell, wobei der PEP ihr On-Premises-Datencenter-Netzwerk sichert. Die Organisation verwendet Softphones auf Benutzergeräten für Sprachanrufe, und das Protokoll erfordert, dass Anrufe vom VOIP-Server zum Benutzergerät (das einen lokalen Benutzeragenten PEP ausführt) initiiert werden. Die Organisation hat auch einen Business Intelligence (BI) Analyse-Server in einer entfernten Umgebung laufen, der wiederum ein authentifiziertes Subjekt mit einem lokalen PEP ist. Ihre Infrastrukturprozesse erfordern, dass ihr interner Patch-Server periodisch eine Verbindung zum entfernten BI-Server herstellt, um OS-Updates durchzuführen.

In beiden in Abb. 17-4 dargestellten Fällen muss der Netzwerkverkehr durch (und kontrolliert von) den PEP geleitet werden, basierend auf Richtlinien. Aus technischer Sicht stellt dies bestimmte Anforderungen an die Zero Trust-Plattform und ihr Richtlinienmodell. Einige Zero Trust-Bereitstellungsmodelle, wie das enklavenbasierte und ressourcenbasierte Modell, die typischerweise eine direkte Verbindung zwischen Benutzergeräten und PEPs nutzen, können dieses Szenario problemlos unterstützen. Lösungen, die auf dem Cloud-Routing-Bereitstellungsmodell basieren, kämpfen in der Regel darum, dies zu unterstützen. Wir werden uns das Mikrosegmentierungs-Bereitstellungsmodell in unserem nächsten Szenario ansehen.

Mikrosegmentierung

Erinnern Sie sich, dass im Mikrosegmentierungs-Bereitstellungsmodell die aufgerufenen Ressourcen authentifizierte Identitäten sind, genau wie die Subjekte. Infolgedessen werden die Zugriffs- und Richtlinienmodelle symmetrischer sein. Dies wird in Abb. 17-5 dargestellt, wo sowohl der Webserver als auch der Benutzer Verbindungen zum

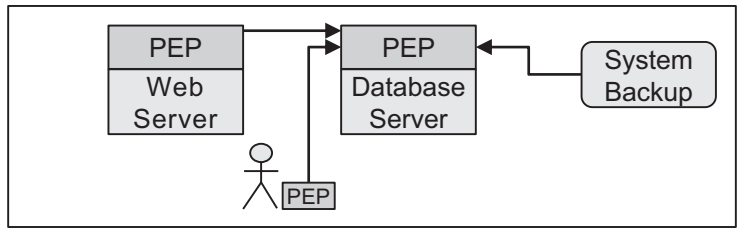

Abb. 17-5. *Richtlinienszenario – Mikrosegmentierung*

Datenbankserver initiieren und alle drei authentifizierte Entitäten sind (beachten Sie, dass wir gleich auf den System Backup-Server eingehen werden).

Die Implikationen davon sind, dass, während die Konzepte von *Subjektkriterien* und *Zielen* existieren werden, das Richtlinienmodell in einem solchen System leicht anders sein muss. In Abb. 17-5, weil sowohl der Webserver als auch der Datenbankserver Identitäten sind, sind sie beide authentifiziert und haben ähnliche Attribute-Sets. Daher wird es möglich sein, sie mit der gleichen Art von Kriterien zu spezifizieren, im Gegensatz zu unseren vorherigen Szenarien, in denen Subjekte und Ziele auf unterschiedliche Weise spezifiziert wurden.

Natürlich müssen selbst im Mikrosegmentierungsmodell Ihre Identitäten mit Nicht-Identitätssystemen interagieren können. Wie zuvor gezeigt, muss der PEP dem Backup-System den Zugriff auf den Datenbankserver ermöglichen. Beachten Sie, dass wir eine weitere Besonderheit im Zusammenhang mit dem Service-to-Service-Szenario in Kap. 18 untersuchen werden.

Jetzt, da wir gesehen haben, wie verschiedene Arten von Richtlinien in verschiedenen Szenarien eingesetzt werden können, wollen wir uns die Flüsse ansehen, die mit ihnen verbunden sind.

Richtlinienbewertung und -durchsetzungsflüsse

Abb. 17-6 zeigt den logischen System Fluss von Richtlinien durch ein Zero Trust-System. Der PDP nimmt als Eingabe die Attribute für die Identität, das Gerät und das System und verwendet sie zur Bewertung der Richtlinien im Richtlinienspeicher. Das Ergebnis dieser Bewertung sind Richtlinien, die diesem Subjekt für die Dauer dieser Sitzung gewährt werden. Diese Ergebnisse, die an die PEPs übermittelt werden, enthalten Informationen über das Subjekt, dem dies gewährt wurde, sowie Informationen über die Aktion, das

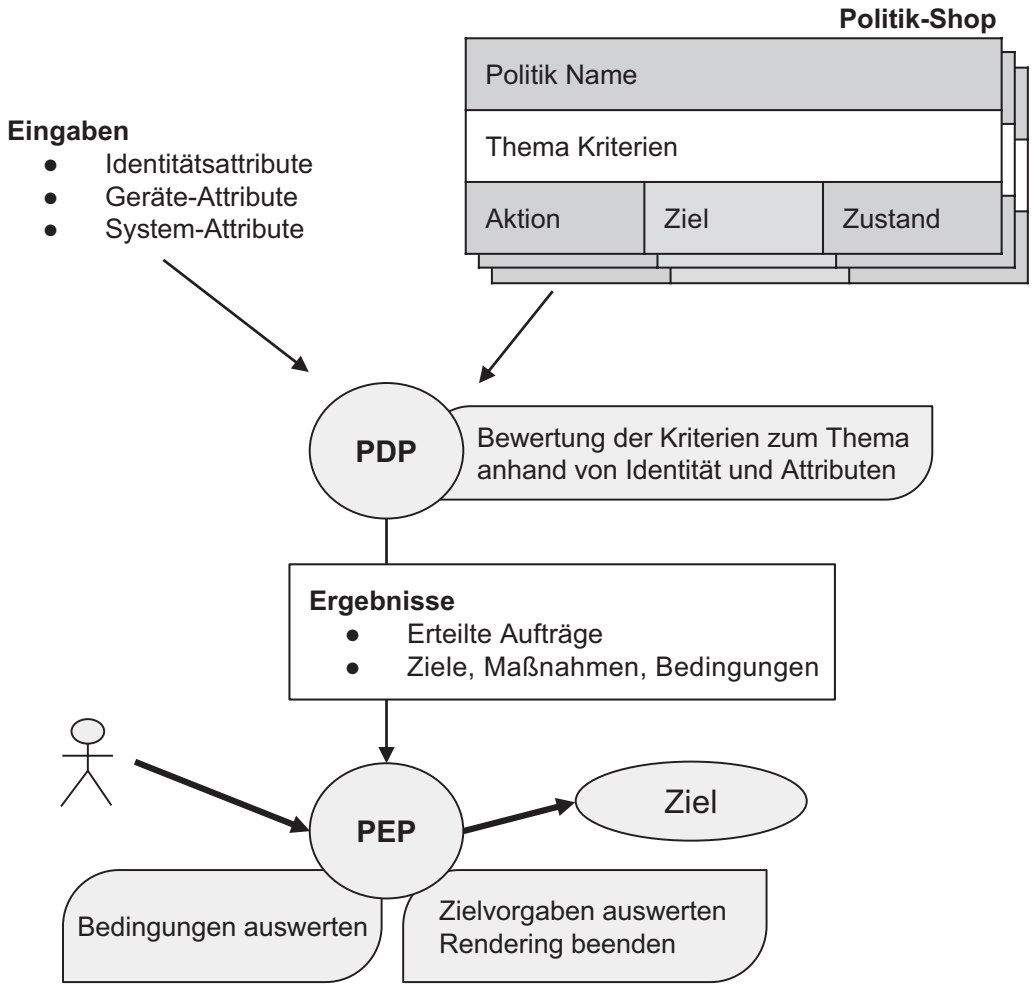

Abb. 17-6. *Richtlinienbewertung und Durchsetzung*

Ziel und den Zustand. Die gewährten Richtlinien müssen möglicherweise durch den PEP weiter gerendert werden, durch die Untersuchung der Metadaten, die mit potenziellen Zielen verbunden sind, um zu bestimmen, welche übereinstimmen. Und der PEP ist verantwortlich für die Durchsetzung von Zugriffszeitbedingungen in den gewährten Richtlinien.

Abb. 17-6 zeigt die Aktionen, die das Zero Trust-System mit den Richtlinien durchführt, während sie durch das PDP und PEP fließen. Während dies zeigt, *was* das System tut, müssen wir auch auf das *wann* eingehen. Wir haben dies in unserem früheren Kapitel über Sicherheitsorchestrierung angesprochen, in dem wir die primären

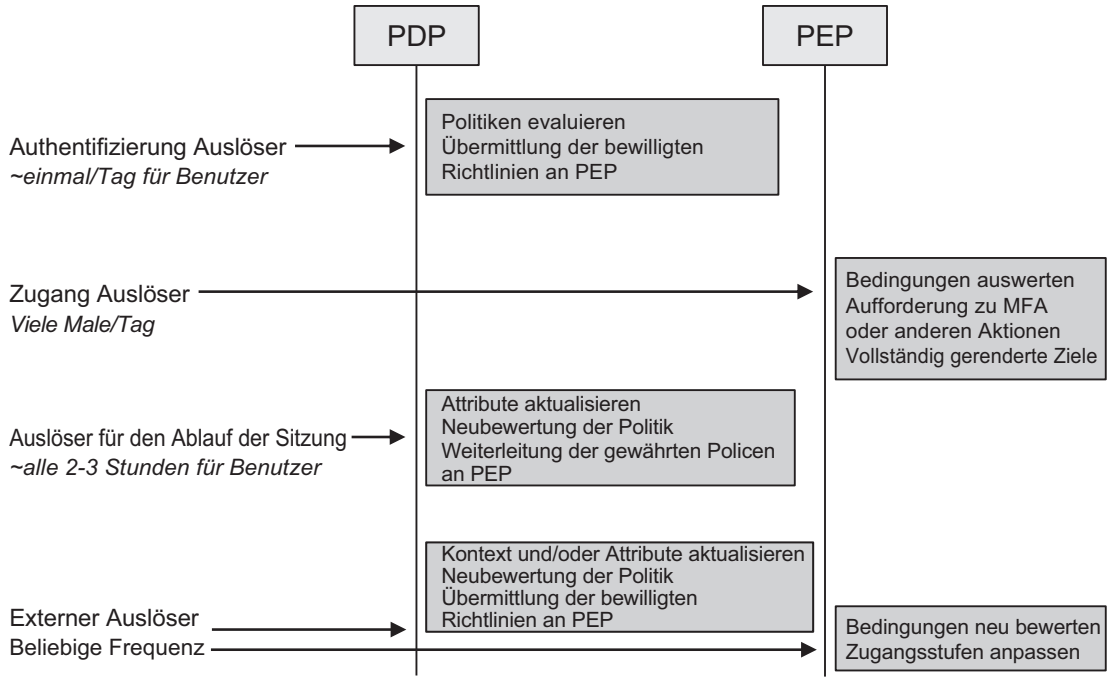

Abb. 17-7. *PDP und PEP Auslöser*

Auslöser vorgestellt haben, die Aktionen innerhalb eines Zero Trust-Systems initiieren. Abb. 17-7 zeigt diese Auslöser und was sie im PDP und PEP auslösen, wenn sie aufgerufen werden.

Authentifizierungsauslöser

Identitäten müssen sich natürlich beim PDP authentifizieren, um Zugang zu erhalten. Die meisten Zero Trust-Systeme werden mit dem Identitätsanbieter einer Organisation integriert sein (anstatt als eigener IdP zu fungieren), und der Authentifizierungsauslöser wird den in Abb. 17-6 gezeigten Richtlinienbewertungsfluss auslösen. Ihre Organisation wird in der Lage sein zu konfigurieren, wie häufig Identitäten in Ihr Zero Trust-System authentifiziert werden, und inwieweit dies für Endbenutzer transparent ist.

Bei dieser Entscheidung spielen viele Faktoren eine Rolle, einschließlich Ihres beabsichtigten Anwendungsfalls und der Authentifizierungsmethoden. Wir werden dies in Kap. 18 weiter diskutieren, aber zum Beispiel möchten Sie möglicherweise, dass die Geräte der Benutzer sofort authentifiziert werden, wenn sie sich zu Beginn ihres

Arbeitstages an ihren Desktops anmelden, wenn Ihr System ihren gesamten Zugang sichert und für ihre Produktivität erforderlich ist. Alternativ können einige Organisationen beschließen, ihre Zero Trust-Reise mit einem VPN-Ersatzszenario zu beginnen; in diesem Szenario könnten Benutzer sich nur dann explizit in ihre Systeme authentifizieren, wenn sie auf spezifische entfernte Ressourcen zugreifen müssen.

Systemidentitäten (nicht-personenbezogene Entitäten) haben natürlich einen anderen Authentifizierungslebenszyklus. Diese Arten von Identitäten laufen oft kontinuierlich, so dass es keinen natürlichen Fluss geben kann, der zu einer regelmäßigen Authentifizierung führt. In diesen Fällen wird der im folgenden Text besprochene Sitzungsablaufauslöser von größerer Bedeutung sein.

Zugriffsauslöser

Der Zugriffsauslöser jeder Richtlinie wird aufgerufen, wenn Identitäten auf ein Ziel zugreifen. Verschiedene Zero Trust-Implementierungen werden dies je nach Bereitstellungsarchitektur, den Fähigkeiten des PEP und der Art des Netzwerkprotokolls (z. B. verbindungsorientiert oder verbindungslos) leicht unterschiedlich handhaben.

Einige Implementierungen können Bedingungen für jedes Netzwerkpaket, bei jeder neuen Verbindung zu einem Ziel (falls zutreffend) oder periodisch (z. B. alle 5 Minuten) bewerten. Unabhängig von der Häufigkeit muss das PEP in der Lage sein, Bedingungen zu bewerten und durchzusetzen, einschließlich Tageszeit, externe Faktoren wie den Status eines Service Desk-Tickets und das Auffordern der Benutzer zu allen notwendigen Interaktionen wie einer gesteigerten Authentifizierung.

Das PEP ist auch dafür verantwortlich, alle Ziele vollständig zu rendern, womit wir meinen, dass das PEP seine Umgebung abfragen und Ressourcen entdecken muss, die den zugehörigen Metadatenanforderungen entsprechen, wie z. B. ein spezifisches Label Wert zu haben.

Sitzungsablaufauslöser

In diesem Buch haben wir eine *Sitzung* nicht formal definiert, was absichtlich war. Verschiedene Zero Trust-Bereitstellungsmodelle und -Plattformen können sehr unterschiedliche Konzepte von Sitzungen haben, und diese Variabilität macht es schwierig, diesen Begriff präzise zu verwenden. Wichtig ist, dass Ihr Zero Trust-System

ein logisches Konzept einer Sitzung haben muss, das ein Zeitraum ist, nachdem eine Identität authentifiziert wurde und währenddessen sie aktiv auf geschützte Ressourcen zugreifen kann.

Sitzungen müssen eine begrenzte Lebensdauer haben, und am Ende der Sitzungslebensdauer muss das System eine Aktualisierung durchführen, bei der es aktualisierte Attribute erhält, Richtlinien erneut bewertet und alle geänderten Zugriffe an die PEPs kommuniziert. Diese Aktualisierung kann für Benutzer sichtbar sein oder nicht; dies sollte als Teil des Richtlinienmodells Ihrer Plattform konfigurierbar sein. Denken Sie daran, dass verschiedene Arten von Attributen unterschiedliche Änderungsraten haben, so dass es einige geben wird, die natürlicherweise mit einer Aktualisierung verbunden sind, wenn die Sitzung erneuert wird.

Über die Dauer der Sitzungen sollten Sie nachdenken und sie auf der Grundlage von Faktoren wie Risikostufe, Anwendungsfall und Identitätspopulation festlegen. Für Benutzer erscheint uns eine Sitzungsdauer von etwa 2–3 Stunden angemessen, abhängig davon, wie dynamisch die Umgebung und die Benutzerpopulation ist. Das ist auch etwa die maximale Häufigkeit, die Benutzer für die Aufforderung zur MFA akzeptieren werden, obwohl in einigen Umgebungen einmal pro Tag angemessener sein könnte. Für nicht-personenbezogene Entitäten sind die Sitzungsdauern stark vom Anwendungsfall und dem Grad abhängig, in dem sich Ihre Dienste und Umgebung ändern. In einigen Situationen könnte eine Sitzungsdauer von 24 Stunden durchaus angemessen sein, während in dynamischeren Systemumgebungen etwas im Bereich von 2-3 Stunden besser wäre. Bedenken Sie, dass viel von den Fähigkeiten Ihrer Zero Trust-Plattform und dem Overhead, der mit einer Sitzungsaktualisierung verbunden ist, abhängen wird. Denken Sie auch daran, dass die dynamischsten Attribute am besten als Bedingungen bewertet werden, die die PEPs mehrmals (sogar fast kontinuierlich) innerhalb einer aktiven Sitzung aktualisieren sollten.

Externer Auslöser

Nach unserer Erfahrung ist einer der Schlüsselfaktoren, die den Erfolg eines Zero Trust-Programms bestimmen, das Ausmaß, in dem die zugrunde liegende Technologieplattform Integrationen ermöglicht und unterstützt. Wir haben darüber im Kapitel über Sicherheitsorchestrierung gesprochen, aber es lohnt sich, dies hier zu wiederholen. Insbesondere müssen Zero Trust-Plattformen eine Art von API

bereitstellen, damit externe Systeme eine Aktualisierung initiieren können. Der Umfang der Aktualisierung wird von der Implementierung abhängen, aber wichtig ist, dass die Aktualisierung die Attribute einschließen muss, die für das externe System relevant sind, das die Aktualisierung initiiert. Denken Sie daran, dass wir ein Beispiel dafür in Kap. 11 ausführlich untersucht haben.

Zusammenfassung

In diesem Kapitel haben wir uns zunächst die logischen Komponenten von Zero Trust-Richtlinien angesehen – *Subjektkriterien, Aktionen, Ziele und Bedingungen.* Wir haben uns auch Attribute angesehen und ihre Rolle in Richtlinien untersucht. Dann haben wir die Dinge aus einer Bereitstellungs- und Flussperspektive betrachtet, mehrere Richtlinienszenarien untersucht sowie den Lebenszyklus der Richtlinienbewertung und Auslöser.

Es sollte klar sein, dass das Bild, das wir zeichnen, eines eines wirklich dynamischen und reaktiven Systems ist, das auf eine kooperative Laufzeitintegration zwischen IT- und Sicherheitskomponenten angewiesen ist. Dies kann eine kulturelle oder technische Veränderung für Unternehmen sein, und es ist wichtig, dies als Teil Ihrer Zero Trust-Reise anzuerkennen. Es ist auch wichtig zu verstehen, dass die Konzepte und Empfehlungen, die wir in diesem Kapitel diskutiert haben, allgemein auf Zero Trust-Plattformen und -Architekturen anwendbar sind, es jedoch in der Praxis eine Vielzahl von Fähigkeiten auf verschiedenen Zero Trust-Plattformen geben wird. Insbesondere gibt es viele verschiedene Arten von PEPs mit unterschiedlichen Durchsetzungsfähigkeiten in Netzwerken, Anwendungen und Benutzeragenten. Angesichts dessen, wenn Sie eine spezifische Zero Trust-Plattform auswählen, stellen Sie sicher, dass Sie ein tiefes Verständnis für ihre Architektur und Fähigkeiten haben, damit Sie Ihre Richtlinien und ihren Lebenszyklus und Flüsse so gestalten können, dass sie am besten mit den Fähigkeiten (und Stärken und Schwächen) Ihrer ausgewählten Plattform übereinstimmen.

Letztendlich möchten Sie eine Zero Trust-Plattform, die sowohl interne als auch externe Attribute nahtlos nutzen kann, mit internen und externen Mechanismen zur Erlangung aktualisierter Kontextinformationen, um Zugangsentscheidungen auf der Grundlage von aussagekräftigen und beschreibenden Richtlinien zu treffen.

KAPITEL 18

Zero Trust Szenarien

In diesem Buch haben wir viele verschiedene Aspekte der Unternehmenssicherheit und der IT-Infrastruktur untersucht. Wir haben die Dinge aus technischer und architektonischer Sicht betrachtet und verschiedene Anwendungsfälle erwähnt. In diesem Kapitel werden wir sieben verschiedene Szenarien untersuchen und diskutieren, wie Sie sie für die Aufnahme in Ihr Zero Trust-Programm bewerten und angehen können. Dies ist kein erschöpfender Satz von Anwendungsfällen, deckt aber die meisten der großen Szenarien ab.

Unsere Ziele für dieses Kapitel sind, Sie mit einem Verständnis dafür auszustatten, wie und wann diese verschiedenen Szenarien in Ihrer Umgebung anwendbar wären, und Ihnen relevante Empfehlungen zu geben, wie Sie sie angehen sollten. Natürlich müssen diese Szenarien auch aus einer Bereitstellungs- und Betriebsperspektive betrachtet werden, was Teil unserer Diskussion in Kap. 19 sein wird. Schließlich werden wir aus Gründen der Kürze hier nicht viel Zeit damit verbringen, diese Szenarien zu rechtfertigen – hoffentlich haben wir Sie davon überzeugt, wenn Sie es bis zum Kap. 18 geschafft haben. Lassen Sie uns eintauchen, beginnend mit einem der häufigsten Zero Trust-Anwendungsfälle, nämlich dem Ersetzen eines VPN.

VPN-Ersatz/VPN-Alternative

Wir haben über VPNs, ihre Schwächen und die vergleichbaren Vorteile, die Zero Trust bietet, bereits in Kap. 9 gesprochen. In diesem Abschnitt werden wir diesen Anwendungsfall kurz wiederholen, um eine Diskussion darüber zu eröffnen, wie Sie ein Zero Trust-Projekt angehen sollten, das auf einen Unternehmens-VPN (Remote User Access) Anwendungsfall ausgerichtet ist. Beachten Sie, dass wir zwei verwandte Szenarien untersuchen:

J. Garbis und J. W. Chapman, *Zero Trust Sicherheit*, https://doi.org/10.1007/979-8-8688-0105-1_18

- Ersetzen eines bestehenden, in Gebrauch befindlichen VPN durch eine Zero Trust-Lösung
- Einführung von Zero Trust für ein neues Remote Access-Szenario

Obwohl diese beiden Szenarien ähnliche technische Überlegungen haben, sollten sie eindeutig aus unterschiedlichen Perspektiven in Bezug auf Rechtfertigung und Entscheidungsfindung angegangen werden. Neue Projekte stellen oft einfachere und leichtere Entscheidungen dar, da es nicht so viele Einschränkungen oder Abhängigkeiten gibt. Dies steht im Gegensatz zu einem VPN-Ersatzszenario, bei dem eine Rechtfertigung für den Ersatz einer bestehenden und betriebsbereiten VPN-Lösung erforderlich sein wird. Das bedeutet nicht, dass dies eine bedeutende Hürde ist – wir haben viele, viele VPN-Ersatzprojekte gesehen – nur dass Sicherheitsleiter bereit sein müssen, die Entscheidung und das Projekt aus möglicherweise mehreren Perspektiven, einschließlich Sicherheit, Technik, Betrieb und Finanzen, zu diskutieren und zu rechtfertigen. Beachten Sie, dass wir dringend empfehlen, dass Organisationen ihre VPNs durch einen Zero Trust-Ansatz ersetzen; es gibt viele gute Gründe dafür.

Lassen Sie uns kurz die architektonischen Unterschiede zwischen traditionellen VPNs und einem Zero Trust-Modell überprüfen, die in Kap. 9 eingeführt und in Abb. 18-1 zusammengefasst wurden. Beachten Sie, dass dieses Szenario nur darauf abzielt, Remote-Benutzern einen sicheren Zugang zu Diensten zu bieten.

Traditionelle VPNs können nur einen einzigen sicheren Netzwerktunnel vom Gerät des Benutzers zu einem VPN-Server herstellen, der den sicheren Tunnel beendet und den Netzwerkverkehr in den privaten Netzwerkbereich zulässt. VPNs perpetuieren ein perimeterbasiertes Netzwerkmodell, das erfordert, dass alle verteilten Ressourcen über ein WAN mit dem Kernnetzwerk des Unternehmens verbunden werden. Alternativ erfordern sie, dass Benutzer manuell VPN-Verbindungen wechseln, wenn sie auf Ressourcen an verschiedenen Standorten zugreifen müssen. Im Gegensatz dazu werden Zero Trust-Systeme mehrere sichere Verbindungen zu verteilten PEPs herstellen, so dass Benutzer sie transparent zugreifen können. (Beachten Sie, dass dies für die Cloud-gerouteten und Enklaven-basierten Modelle zutrifft. Es muss nicht unbedingt für die Mikrosegmentierungs- oder Ressourcen-basierten Modelle zutreffen, abhängig von den Details der Implementierung.)

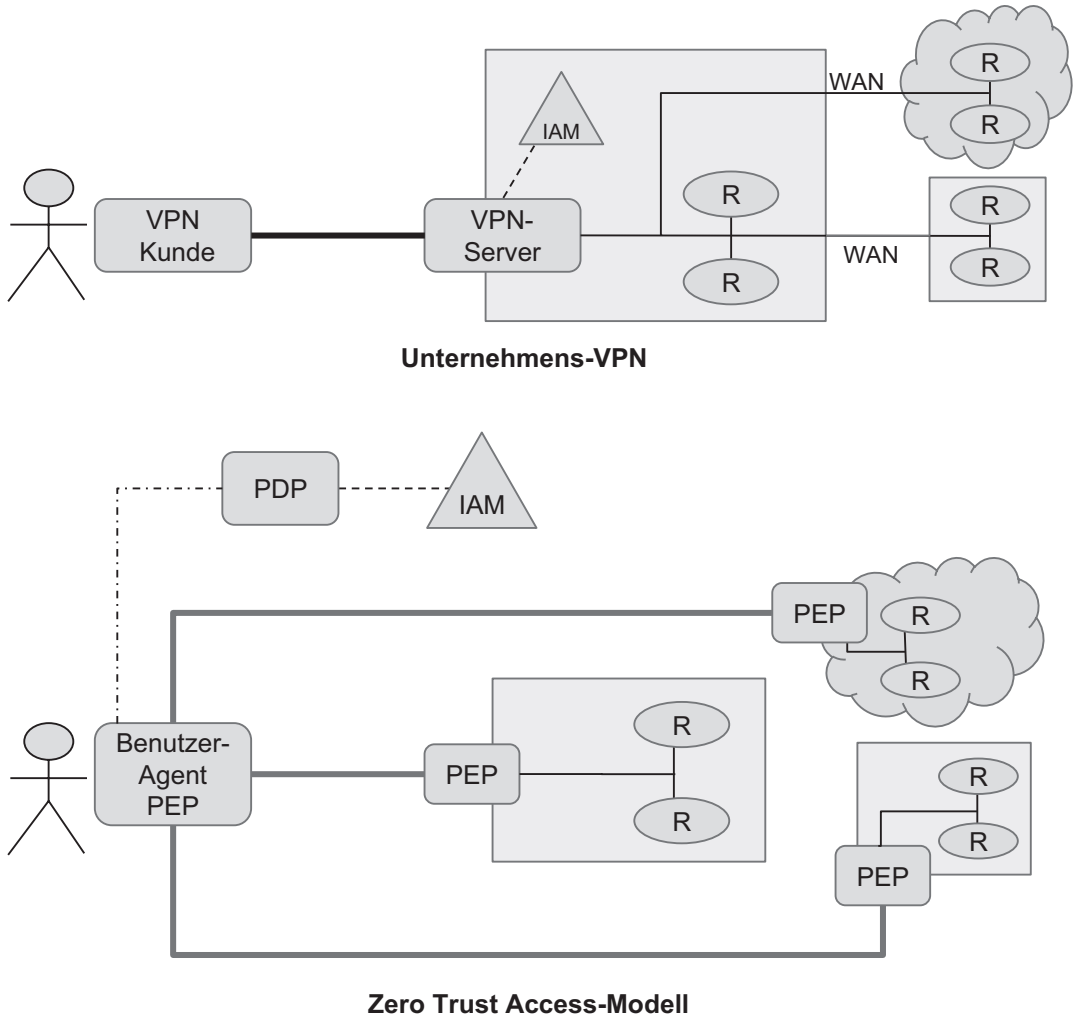

Abb. 18-1. *Unternehmen VPN und Zero Trust-Architekturen*

Überlegungen

In diesem Abschnitt werden wir einige verschiedene Aspekte betrachten, um Ihnen zu helfen, potenzielle VPN-Projekte für Zero Trust zu identifizieren.

Ressourcen

Betrachten Sie die Anzahl, Art, Standort und Wert der zu berücksichtigenden Ressourcen. Wie geschäftskritisch sind sie? Wenn es sich um einen Ersatz handelt, wie werden sie heute genutzt und welche Probleme oder Schmerzpunkte sind mit dem aktuellen VPN verbunden?

Im Allgemeinen bieten Zero Trust-Lösungen eine bessere Leistung als VPNs, insbesondere für verteilte Ressourcen. Sie können oft auch zum Schutz von Ressourcen in Standorten oder Umgebungen eingesetzt werden, in denen das Unternehmen keinen VPN-Zugangspunkt einrichten kann, zum Beispiel in einem Drittanbieternetzwerk. Wenn Sie über ein stark verteiltes oder dynamisches Ressourcen-Set verfügen, sind diese wahrscheinlich gute Kandidaten für einen Zero Trust-Ansatz – denken Sie an die dynamische Zielrendering aus unserem Policy-Modell-Kapitel.

Benutzer und Benutzererfahrung

Wer sind die Benutzer, die das VPN derzeit nutzen, oder die auf diese neuen Ressourcen zugreifen müssen? Sind alle Benutzer remote? Wurde diese Remote-Benutzerzugriffslösung schnell (und möglicherweise mit einigen bekannten Problemen oder Kompromissen) eingesetzt, zum Beispiel als Reaktion auf die COVID-19-Arbeit-von-Zuhause-Verschiebung? Greifen On-Premises-Benutzer auf diese Ressourcen über ein separates Sicherheitsmodell zu – zum Beispiel über Firewall-ACLs?

In diesen Fällen gibt es oft gute Gründe, Zero Trust zu übernehmen, zum Beispiel um Sicherheits- oder Betriebsprobleme zu überwinden, die durch ein schnell eingesetztes VPN verursacht wurden. Wenn es Ressourcen gibt, die kürzlich bereitgestellt wurden, könnte es sein, dass nur Remote-VPN-Benutzer einen sicheren Zugangsweg haben und dass Ihre Organisation eine Lösung für On-Premises-Benutzer benötigt. Und schließlich können Zero Trust-Lösungen, die darauf ausgelegt sind, den Zugang für alle Benutzer zu allen Ressourcen zu sichern, isolierte Lösungen eliminieren, wie separate Regeln und Zugangsmechanismen für Remote- gegenüber On-Premises-Benutzern.

Zero Trust kann schrittweise, Gruppe für Gruppe oder Anwendung für Anwendung, angewendet werden, obwohl die Benutzererfahrung definitiv eine Überlegung sein sollte. Das heißt, seien Sie sich der verschiedenen Zugriffswerkzeuge bewusst, die Ihre ersten Benutzergruppen nutzen, um unnötige Reibung zu vermeiden. Zum Beispiel

sollten Sie wahrscheinlich nicht verlangen, dass eine Gruppe von Endbenutzern im Laufe ihres Arbeitstages zwischen ihrem aktuellen VPN und Ihrer Zero Trust-Lösung hin und her wechselt. Es wäre viel besser, eine Gruppe von Benutzern auf Ihre Zero Trust-Lösung für *alle* ihre Zugriffsbedürfnisse umzustellen, indem sie ihren aktuellen breiten VPN-Zugang mit präziseren Zero Trust-Richtlinien für spezifische Ressourcen kombinieren. Auf diese Weise beginnen sie, verbesserte Sicherheit zu erlangen, während sie auch eine verbesserte Benutzererfahrung erhalten. Wir werden dies weiter in Kap. 19 diskutieren.

Identitätsanbieter

Einige VPN-Implementierungen sind nicht mit Unternehmensidentitätsanbietern integriert; in diesen Fällen kann eine Zero Trust-Bereitstellung schnell erheblichen Wert liefern. Indem die Authentifizierung von Remote-Zugriffsbenutzern an ihren Unternehmensidentitätsanbieter gebunden wird, beseitigen Sicherheitsteams eine Identitätssilo, das innerhalb ihres VPN existierte. Dies beseitigt jegliche Arbeit, die notwendig ist, um dieses Silo mit ihrem primären Anbieter synchron zu halten, zum Beispiel um auf Identitätslebenszyklusereignisse von Join, Move und Leave zu reagieren. Selbst wenn ein VPN einen Unternehmens-IdP verwendet, wird eine Zero Trust-Lösung es verbessern, indem sie feinkörnige und kontextsensitive Zugriffsrichtlinien durchsetzt. Viele Zero Trust-Lösungen unterstützen auch mehrere Identitätsanbieter verschiedener Typen, so dass verschiedene Benutzergruppen sich gegen verschiedene IdPs authentifizieren können, oder so dass Legacy-Systeme durch moderne Authentifizierungs-Protokolle geschützt werden können.

Netzwerk

Es ist entscheidend, dass Sie ein klares Verständnis für die Netzwerk-Topologie Ihres Unternehmens, die Datenflüsse und den Standort der geschützten Ressourcen erhalten. Dieses Wissen ermöglicht es Ihnen, gut informierte Entscheidungen und Empfehlungen über den Übergang vom VPN-Zugang zu Zero Trust zu treffen. Beginnen Sie mit der Frage, wo VPN-Konzentratoren (Zugangspunkte) sich befinden, welche Netzwerke sie zugänglich machen und wie verteilte Ressourcen aus Netzwerksicht zugegriffen werden.

Wie wir im einleitenden Teil dieses Kapitels erwähnt haben, bestimmen Sie, ob Benutzer einfach nur auf Ressourcen über einen einzigen Zugangspunkt in ein Unternehmensnetzwerk zugreifen. Selbst in diesem einfachen Fall kann Zero Trust einen Mehrwert bieten, wie verbesserte Leistung und Stabilität, bessere Integration mit Identitätsanbietern und MFA und natürlich feinkörnige Zugriffskontrollen.

Teams oder Projekte, die Zugang zu verteilten Ressourcen benötigen, haben typischerweise Probleme mit VPNs, und das ist eine Situation, in der Zero Trust glänzt (solange Ihr gewähltes Implementierungs- und Bereitstellungsmodell mehrere gleichzeitige Verbindungen zu verteilten PEPs unterstützt). Betrachten Sie dies als eine Gelegenheit, „Was-wäre-wenn"-Fragen an die Netzwerk- oder Anwendungsteams zu stellen. „Was wäre, wenn Benutzer gleichzeitig auf beide Ressourcen zugreifen könnten?" „Was würde es bedeuten, wenn wir den Zugang an einen Geschäftsprozess binden könnten, wie zum Beispiel ein Service Desk-Ticket?" „Was wäre, wenn wir tiefere Geräte-Posture-Checks durchführen könnten, bevor Benutzern der Zugang erlaubt wird?" Dies sind ausgezeichnete Fragen, um Gespräche mit diesen Teams zu entfachen und sie als Unterstützer Ihres Zero Trust-Projekts zu gewinnen.

Es gibt auch andere Fragen, die Sie Ihrem Netzwerkteam stellen sollten, die Ihnen helfen werden, besser für Ihre Zero Trust-Implementierung zu planen und dafür einzutreten. Zum Beispiel, finden Sie heraus, welche Arten von Remote-Zugriffsrichtlinien (ACLs) Ihr aktuelles VPN implementiert. Wie breit oder eng sind sie? Wenn sie sehr breiten Netzwerkzugang gewähren, was ziemlich häufig ist, kann Ihr Zero Trust-Projekt verbesserte Sicherheit und reduziertes Risiko liefern, indem es den Netzwerkzugang stark reduziert, ohne die Benutzerproduktivität zu beeinträchtigen. Bestimmen Sie, ob es ausstehende Compliance-Probleme oder Prüfungsergebnisse gibt, die Ihr Projekt adressieren kann.

Wenn Ihr VPN restriktiven Netzwerkzugang durchsetzt, finden Sie heraus, wie gut das aus betrieblicher und Benutzerproduktivitätssicht funktioniert. Es ist wahrscheinlich, dass dies in allen, außer den statischsten Umgebungen, betrieblichen Aufwand sowie Benutzerreibung verursacht. Ihre Zero Trust-Lösung sollte in der Lage sein, ebenso strenge (wenn nicht strengere) Zugangskontrollbeschränkungen durch automatisierte Richtlinien durchzusetzen, wodurch Ihre IT- und Betriebsteams von manuellem Aufwand entlastet werden.

Finden Sie schließlich heraus, wie Ihre Organisation Wide Area Networks nutzt. Diese verursachen typischerweise erhebliche Kosten für Organisationen, und Zero Trust-Lösungen können die Nutzung von WANs reduzieren (und in einigen Situationen eliminieren).

Empfehlungen

Der Ersatz von VPNs und die Alternative zu VPNs sind oft das erste Zero Trust-Projekt und oft ein gutes, um damit zu beginnen. Die Vorteile sind klar und die Funktionalität eines traditionellen VPN ist im Allgemeinen recht einfach durch eine Zero Trust-Lösung zu ersetzen. Wir empfehlen eine schrittweise Einführung, unter Berücksichtigung der Benutzergruppen, die möglicherweise für eine gewisse Zeit sowohl Zero Trust als auch VPN-Zugang beibehalten müssen. Diese Lösungen können in der Regel harmonisch auf einem Endbenutzergerät koexistieren, sie können jedoch in der Regel *nicht* gleichzeitig ausgeführt werden, da sie auf Netzwerkebene in Konflikt geraten. Dies könnte ein Problem sein, wenn Sie beispielsweise ein „immer aktives" VPN haben oder Zero Trust in einem ähnlichen Modell einführen möchten.

Eine letzte Empfehlung für das Szenario des VPN-Ersatzes besteht darin, sorgfältig auf die Reihe von Tools und Prozessen zu schauen, die um den Umfang und die Funktionalität des VPN-Tools herum aufgebaut wurden. Einige Organisationen, insbesondere solche mit älteren VPNs und älterer Infrastruktur, haben möglicherweise ein „Netz" von voneinander abhängigen Tools aufgebaut. Dies kann ein komplexes Hindernis für eine schrittweise Einführung von Zero Trust darstellen. Zum Beispiel hatte ein Unternehmen, mit dem wir gearbeitet haben, ein traditionelles VPN, das bestimmte Ereignisse in das Windows-Ereignisprotokoll des Benutzers protokollierte. Sie hatten eine Reihe von „Klebstoff"-Tools erstellt, die das Windows-Ereignisprotokoll überwachten und auf diese Ereignisse reagierten, indem sie einige Netzwerkkonfigurationsaufgaben durchführten. Die Modifikation dieser Tools war eine zusätzliche Aufgabe und verursachte eine Verzögerung des Projekts, da diese Komponente von einem anderen Team innerhalb der Organisation gewartet und verwaltet wurde. Seien Sie also bewusst, wie Ihre Unternehmens-IT-Umgebung funktioniert, und stellen Sie viele Fragen auf und ab dem IT-Stack und in Ihrem IT- und Geschäftsprozess-Ökosystem. Sie könnten überrascht sein über Bereiche und Wege, auf denen die Organisation Abhängigkeiten von bestimmten Tools oder Arbeitsabläufen aufgebaut hat. Einige davon könnten Hindernisse für die Einführung von Zero Trust sein, aber einige könnten aktuelle Schmerzpunkte sein, die Ihr Projekt beseitigen kann. Es gibt oft eine erhebliche Menge an Kopfschmerzen rund um VPNs, weshalb sie oft ein sinnvolles erstes Zero Trust Projekt darstellen.

Zugang von Dritten

Der Zugang von Dritten ist auch ein gutes Kandidatenszenario für Zero Trust, da er typischerweise eine Quelle von Kopfschmerzen und Risiken für Unternehmen ist und es einen klaren Unterschied und Vorteil gibt, wenn man einen Zero Trust-Ansatz gegenüber traditionellem Remote-Zugang von Dritten wählt. Beginnen wir mit einer Definition – für unsere Diskussion hier ist ein Dritter eine nicht angestellte Person, mit der das Unternehmen eine rechtliche Beziehung hat und die legitimen Zugang zu den Netzwerk- und privaten Ressourcen des Unternehmens benötigt. Insbesondere

- Die Personen können identifiziert werden.
- Die Ressourcen, auf die sie Zugriff benötigen, sind bekannt und identifizierbar.
- Sie benötigen Zugang zu privaten Unternehmensressourcen (wenn sie nur Internetzugang benötigen, könnten sie einfach das Gästenetzwerk nutzen, wenn sie vor Ort sind).

Beachten Sie, dass wir Vollzeit-Vertragsarbeiter (nicht Mitarbeiter) von diesem Szenario ausschließen; nach unserer Erfahrung werden diese Leute aus IT-Sicht viel mehr wie reguläre, Vollzeit-Mitarbeiter behandelt. Das heißt, ein Vertragsprogrammierer auf einer 6-monatigen Aufgabe ist vielleicht kein Firmenmitarbeiter, wird aber in der Regel ein firmenverwaltetes Gerät erhalten und Teil des Identitätsmanagementsystems des Unternehmens sein. Aus Sicherheitssicht sollten sie auf die gleiche Weise wie Mitarbeiter verwaltet werden, wenn auch mit viel eingeschränkterem Netzwerkzugang.

Schauen wir uns einige Beispiele für die Art von Dritten an, die für dieses Szenario relevant sind. Diese sind oft an externe Firmen gebunden, die spezialisiertes Fachwissen in einem bestimmten Bereich haben, das es nicht sinnvoll ist, intern im Unternehmen zu haben. Ein klassisches Risiko beim Zugang von Dritten ist beispielsweise eine Firma, die für die Überwachung, Wartung und Instandhaltung von Gebäude-HVAC-Systemen verantwortlich ist. Diese Systeme sind in der Regel im Unternehmensnetzwerk und die HVAC-Anbieter benötigen periodischen Zugang zu diesen Systemen, um sie effizient laufen zu lassen. Ein weiteres Beispiel ist eine Firma, die externe Finanzprüfer hat, die Zugang zu einem vor Ort befindlichen Finanzverwaltungssystem benötigen.

Diese Arten von Drittanwendern sind genau diejenigen, die zusätzliche Sicherheitskontrollen benötigen. Wie das NIST Zero Trust-Dokument feststellt, „kann

eine Organisation keine internen Richtlinien auf externe Akteure (z. B. Kunden oder allgemeine Internetnutzer) anwenden, aber sie kann einige auf Zero Trust basierende Richtlinien auf Nicht-Unternehmensnutzer anwenden, die eine besondere Beziehung zur Organisation haben".

Unsere Zero Trust-Prinzipien erfordern, dass diese Benutzer authentifiziert werden und ihr Netzwerkzugang auf das Minimum beschränkt wird. Traditionell haben Organisationen VPNs verwendet, um Dritten einen Remote-Zugang zu ermöglichen, und natürlich zeigen VPNs alle ihre Schwächen beim Zugang von Dritten. Darüber hinaus sind diese Drittanwender keine Mitarbeiter, so dass sie per Definition keine Geräte verwenden, die von diesem Unternehmen verwaltet werden. Das bedeutet, dass das Unternehmen nicht auf die Sicherheitslage dieses Geräts vertrauen oder sich darauf verlassen kann, was es umso wichtiger macht, Sicherheitskontrollen um den Netzwerkzugang für dieses Gerät zu erzwingen.

Eine letzte Einschränkung besteht darin, dass Sicherheitsteams im Allgemeinen nicht die Installation einer bestimmten Software auf diesen Geräten verlangen können. Dies ist etwas weniger absolut als früher, insbesondere mit der zunehmenden Verbreitung von Bring Your Own Device (BYOD) und der Akzeptanz der Nutzung von persönlichen Mobiltelefonen oder Tablets für Arbeitsaktivitäten. Zum Beispiel kann ein Drittanwender möglicherweise keine Remote-Zugangssoftware auf einem firmenverwalteten Laptop installieren, auch wenn dieser Zugang ein erforderlicher Teil seiner Arbeit ist. Aber es wird immer akzeptabler, Remote-Zugangssoftware auf einem persönlichen Tablet oder einem BYOD-Gerät zu installieren und dieses für diese Arbeitstätigkeiten zu verwenden.

Selbst wenn der Drittanwender Remote-Zugangssoftware auf seinem Gerät installieren kann, ist es sehr unwahrscheinlich, dass er die Installation von invasiverer Endpoint-Management- oder Sicherheitssoftware akzeptieren wird, und es ist nicht realistisch, diese Drittanwendergeräte in Ihr Unternehmenssicherheits- oder IT-Management-System einzubeziehen. Organisationen müssen einfach akzeptieren, dass diese Systeme und Geräte möglicherweise nicht ihren Sicherheitsstandards entsprechen und Zero Trust verwenden, um das Prinzip des geringstmöglichen Privilegs sowie MFA durchzusetzen. Wir werden in Kürze mehr darüber sprechen, im Abschnitt „Empfehlungen".

Überlegungen

Der Zugriff durch Dritte ist im Allgemeinen ein guter Kandidat für ein Zero Trust-Projekt und kann manchmal als nützliches erstes solches Projekt dienen. Diese Benutzer sind in der Regel sehr gut definiert und ihr Zugriff ist typischerweise auf eine kleine und statische Menge von Ressourcen beschränkt. Sie stellen auch typischerweise ein Risikogebiet dar, da diese Benutzer auf unternehmensverwaltete Ressourcen von Geräten zugreifen, die nicht vom Unternehmen verwaltet werden.

Architektur

Die Netzwerkarchitektur für den Zugriff durch Dritte wird wahrscheinlich Ihrer VPN ähnlich sein; tatsächlich ist es sehr wahrscheinlich, dass diese Personen Ihr bestehendes Unternehmens-VPN nutzen werden. Wichtig zu verstehen ist, wie und wo diese Personen auf das Netzwerk zugreifen und wie ihr Netzwerkverkehr das Unternehmen durchquert, um ihre Zielressourcen zu erreichen. Die Art und der Standort dieser Ressourcen sollten die Platzierung Ihrer PEPs beeinflussen und es Ihnen ermöglichen, zu vermeiden, dass der Benutzerverkehr von Dritten sehr viel von Ihrem Netzwerk durchquert. Wie immer gilt hier das Prinzip der geringsten Berechtigung, und Ihre PEPs sollten allen unnötigen Netzwerkzugriff für diese Benutzer verhindern.

Benutzer und Benutzererfahrung

Die Benutzererfahrung kann für Drittanwender eine weniger wichtige Überlegung sein, verglichen mit Mitarbeitern. Dies gilt insbesondere, wenn dieser Zugriff nur gelegentlich und nicht täglich oder den ganzen Tag über erforderlich ist. Zum Beispiel kann ein transparenter (immer aktiver) Zugriff auf Zero Trust-geschützte Ressourcen für Mitarbeiter gewünscht sein, aber nicht notwendig für Drittanwender. Das heißt aber nicht, dass Sie ihren Zugang absichtlich erschweren sollten.

Zero Trust-Systeme unterstützen oft sowohl agentenbasierten als auch agentenlosen Zugriff, und der Zugriff durch Dritte ist ein Anwendungsfall, bei dem oft agentenloser Zugriff erforderlich ist. Je nach Art der zugegriffenen Ressourcen und den verwendeten Netzwerkprotokollen kann agentenloser Zugriff eine praktikable Option sein. Typischerweise sind webbasierte Anwendungen leicht erreichbar mit einem agentenlosen Modell, während nicht-webbasierte (nicht-HTTP) Anwendungen einige

Herausforderungen darstellen können. Wenn ein Zero Trust-Agent technisch auf Benutzergeräten erforderlich ist, aber die dritte Partei sich weigert, sie zu installieren, gibt es einige Alternativen, wenn auch zu zusätzlichen Kosten. Zum Beispiel könnte das Unternehmen einen virtuellen Desktop für Drittanwender hosten, in den sie den Zero Trust-Agenten installieren würden. Oder das Unternehmen könnte ein verwaltetes Gerät bereitstellen, das von den Dritten ausschließlich für den Zugang in die Zero Trust-geschützte Umgebung genutzt wird.

Empfehlungen

Aus Sicht der Benutzerauthentifizierung und Identitätsverwaltung empfehlen wir, dass Ihr Zero Trust-System das Unternehmensidentitätsverwaltungssystem der dritten Partei für die Authentifizierung verwendet, wenn möglich, aber nur, wenn Sie ein ausreichendes Vertrauen in deren Reife und Identitätslebenszyklusprozesse haben. Wenn nicht, lassen Sie sie einen IdP unter Ihrer Kontrolle nutzen – entweder Ihren primären Unternehmens-IdP oder einen kleineren und einfacheren, der speziell für Dritte gedacht ist. Jede Zero Trust-Lösung sollte in der Lage sein, verschiedene Benutzerpopulationen gegen verschiedene IdPs zu authentifizieren.

Wir empfehlen auch, dass Sie MFA für diese Benutzer durchsetzen, jedes Mal, wenn sie versuchen, auf Ihre Ressourcen zuzugreifen. Diese Form der gestuften Authentifizierung sollte mit einem MFA-Anbieter unter Ihrer Kontrolle implementiert und mit Ihrem Zero Trust-System integriert werden. Dies stellt sicher, dass Sie Ihre Sicherheitsrichtlinien bezüglich der Häufigkeit und Art der Authentifizierung durchsetzen können und das Potenzial für die gemeinsame Nutzung von Anmeldeinformationen durch Drittanwender (was ein häufiges Vorkommnis ist) ausschließen können.

Sie sollten definitiv Ihr Zero Trust-System kontextbezogene Zugriffskontrollen durchsetzen lassen, wie zum Beispiel Geolokalisierung, und feinkörnige Zugriffsrichtlinien konfigurieren, die den Benutzerzugriff auf das absolute Minimum beschränken. Diese Richtlinien sollten einfach zu definieren sein, da der Zugriff durch Dritte in der Regel nur für eine feste und gut definierte Menge von Zielen gewährt wird. Wir empfehlen auch, dass Sie in Betracht ziehen, Ihre Zugriffsrichtlinien für Dritte an einen Geschäftsprozess zu binden, wenn möglich, um diesen Zugriff weiter einzuschränken (und zu dokumentieren). Zum Beispiel erlauben viele Zero Trust-Systeme die Erstellung von Richtlinien, bei denen der Zugriff durch das Vorhandensein

und den Zustand eines Service Desk-Tickets gesteuert wird. Dieser Ansatz funktioniert gut in Szenarien, in denen Dritte nur periodischen Zugriff benötigen, und stellt sicher, dass der gesamte Zugriff angefordert, genehmigt und nur für einen begrenzten Zeitraum gewährt wird.

Schließlich ist zu beachten, dass, wenn ein Unternehmen bereits den Übergang zu Zero Trust gemacht hat und ein „Café-Stil" Netzwerk hat, dass sogar Drittanwender, die vor Ort sind, Ressourcen nur innerhalb des Zero Trust-Modells zugreifen müssen. Das heißt, Drittanwender, die physisch in einer Unternehmenseinrichtung anwesend sind, erhalten automatisch nur den gleichen eingeschränkten Zugang, den sie auch bei Fernzugriff erhalten. Dies ist ein wichtiger Vorteil von Zero Trust – gelegentlicher persönlicher Netzwerkzugriff durch Dritte stellt nicht mehr das gesamte Unternehmensnetzwerk in Gefahr.

Cloud-Migration

Die Migration von Anwendungen und Funktionen zu Cloud-Plattformen ist zweifellos ein großer Teil der heutigen Unternehmens-IT und Anwendungsentwicklung und umfasst eine Vielzahl von Szenarien. Die Leistungsfähigkeit dieser Plattformen und die Allgegenwart und Zuverlässigkeit der Netzwerkverbindung machen diesen Trend im Grunde unumkehrbar, weshalb es wichtig ist, dass Zero Trust-Projekte und -Führungskräfte dies akzeptieren und ihre Kollegen auf der Geschäfts- und Anwendungsentwicklungsseite über diesen neuen Ansatz aufklären. Idealerweise haben Sicherheitsteams eine Zero Trust-Plattform und ein strukturiertes Menü von Ansätzen und genehmigten Komponenten im Einsatz, die es Anwendungseigentümern ermöglichen, schnell die Cloud zu umarmen.

Migrationskategorien

Natürlich ist „Cloud-Migration" nicht eine Sache, sondern viele verschiedene Arten von Dingen, abhängig von vielen Faktoren. Aber im Allgemeinen glauben wir, dass diese Migrationsprojekte in vier Kategorien fallen.

Staplermigration

In diesem Szenario wird die Anwendung „wie sie ist“ von einer physischen oder virtuellen Umgebung vor Ort in eine IaaS-Umgebung verschoben. Das heißt, es gibt keine Änderungen an der Anwendungslogik, Topologie oder Technologie. Das Endergebnis ist, dass die gleiche Anwendung an einem anderen Ort läuft. Da dies die Struktur und die Abhängigkeiten der Anwendung beibehält, kann diese Migration schneller und einfacher sein, liefert aber begrenztere Vorteile. Diese Migration erfordert keine Entwicklungsänderungen an der Anwendung; sie sollte nur eine Neukonfiguration erfordern und ist gut geeignet für COTS-Anwendungen, die das Unternehmen lizenziert hat und daher nicht ändern kann.

Die Anwendung umgestalten

In diesem Szenario wird die Anwendung in eine IaaS-Umgebung migriert, aber es beinhaltet einige technische oder strukturelle Änderungen, idealerweise um die Vorteile ihrer neuen Cloud-Plattform zu nutzen. Zum Beispiel kann die Anwendung modifiziert werden, um eine Cloud-native Datenbank zu verwenden, oder einen Cloud-basierten Identitätsanbieter. Oder einige der Bereitstellungs- oder Betriebsinfrastrukturen innerhalb der Anwendungen (wie der Webserver oder ein Logging-Server) können auf eine Cloud-basierte Variante umgestellt werden. Diese Migration erfordert technische oder Entwicklungsänderungen an der Anwendung und kann in der Regel moderate Verbesserungen erzielen. Einige COTS-Anwendungen unterstützen diese Migration in einigen geringfügigen Aspekten, zum Beispiel durch die Unterstützung der Verwendung einer Cloud-basierten Datenbank.

Die Anwendung neu schreiben

Dieser Ansatz ist technisch am schwierigsten, bietet aber potenziell einen enormen Wert. In diesem Modell haben Anwendungsentwickler die Möglichkeit, die Anwendungsarchitektur komplett neu zu denken, einschließlich eines „radikalen“ Ansatzes zur Umarmung moderner Komponenten wie Container, PaaS, Microservices oder NoSQL-Datenbanken, unter anderem. Abhängig von der aktuellen Anwendungsarchitektur können Entwickler möglicherweise Elemente der

Anwendungslogik und des Datenmodells wiederverwenden, um die Dinge zu beschleunigen. Dieser Ansatz ist nicht anwendbar auf COTS-Anwendungen.

SaaS übernehmen

Mit diesem Ansatz machen Organisationen den Übergang von On-Prem-Anwendungen (entweder benutzerdefiniert oder COTS) zu einer Cloud-basierten SaaS-Anwendung. Dies stellt natürlich eine umfassende Veränderung in der Anwendungstopologie und den Zugriffskontrollen dar. Es kann möglich sein, einige der On-Prem-Anwendungslogik wiederzuverwenden, insbesondere wenn das Unternehmen die SaaS-Version ihrer On-Prem-Anwendung übernimmt. Unternehmen sollten in der Lage sein, einige ihrer Anwendungsdaten zu importieren, um den Wert ihrer SaaS-Anwendung zu steigern.

Im Allgemeinen sind viele (wenn nicht die meisten) Cloud-Migrationsprojekte hervorragende Kandidaten für Zero Trust, da sie Änderungen an Sicherheit, Netzwerk und Architektur umfassen und daher eine Gelegenheit bieten, eine moderne und Cloud-freundliche Sicherheitsplattform zu übernehmen. Insbesondere Zero Trust-Systeme, durch ihre Eigenschaft, dynamisch und kontextsensitiv zu sein, können die reichhaltige Menge an APIs nutzen, die von Cloud-Plattformen bereitgestellt werden.

Überlegungen

Diese vier Migrationsszenarien bieten jeweils unterschiedliche Möglichkeiten, Zero Trust anzuwenden, was definitiv Wert schaffen und die Sicherheit dieser in Bewegung befindlichen Anwendungen verbessern kann. Lassen Sie uns diese aus einer architektonischen Perspektive betrachten.

Architektur

Wenn wir uns diese Szenarien ansehen, denken Sie zurück an die Diskussionen in unseren Kapiteln über IaaS und PaaS und SaaS, in denen wir über die Netzwerkzugriffskontrollen und Architekturen gesprochen haben, die mit diesen Modellen verbunden sind. Schauen Sie sich die geplante oder laufende Cloud-Migrationsarchitektur und den Ansatz Ihrer Organisation an und beeinflussen Sie sie, um sicherzustellen, dass sie am effektivsten mit Ihrer gewählten Zero Trust-Netzwerk-

Topologie und Zugriffsrichtlinien arbeiten. Und stellen Sie sich und Ihrer Organisation folgende Fragen, basierend auf Ihrem gewählten Cloud-Migrationsansatz.

Stapler

Ist die Anwendung eigenständig und werden alle Teile in die Cloud gehoben? Die meisten Anwendungen sind nicht zu 100% eigenständig, also wenn das der Fall ist, wie werden die Datenflüsse rein und raus verwaltet? Wie können Ihre Zero Trust PEPs dies erleichtern? Werden alle (nicht benutzerbezogenen) Komponenten der Anwendung innerhalb einer impliziten Vertrauenszone liegen? Wenn ja, ist dieses Risiko mit Ihrem neuen Sicherheitsmodell akzeptabel? Wenn nicht, wie werden sie authentifiziert und erhalten Zugang über einen PEP?

Die Anwendung umgestalten

Zusätzlich zu den vorherigen Stapler-Fragen, wie ist die aktuelle und beabsichtigte Netzwerk-Topologie? Was ändert sich an den Komponenteninteraktionen? In welcher Weise können Sie die Änderungen am Anwendungsdesign beeinflussen?

Die Anwendung neu schreiben

In welchem Maße wird das Anwendungsteam „von Grund auf neu anfangen", wenn sie eine neue Anwendungsarchitektur erstellen? Wie werden bestehende Anwendungskomponenten (entweder funktional oder datenbezogen) übernommen? Kann die neue Architektur mit Ihrer Zero Trust-Plattform abgestimmt werden? Müssen die alte und die neue Version für eine bestimmte Zeit nebeneinander existieren? Wenn ja, müssen sie Daten austauschen? Wie wird das gesichert? Schließlich, kann die Anwendung in einer zukunftsorientierten Weise geschrieben werden, um Zero Trust-Richtlinien vom PDP zu konsumieren und zu einer Anwendungs-PEP zu werden?

SaaS übernehmen

Dies ist eindeutig ein anderer Ansatz als die vorherigen drei, da die neue Plattform nicht unter der Kontrolle Ihres Unternehmens steht. Dies kann eine einfachere Migration aus Sicherheits- und Netzwerksicht sein, da das Ziel festgelegt ist. Aber untersuchen Sie auf jeden Fall die SaaS-Plattform aus Sicherheitssicht und bestimmen Sie, ob es sinnvoll ist, Zero Trust Sicherheit auf diese SaaS-Umgebung anzuwenden.

Benutzer und Benutzererfahrung

In den meisten Fällen werden diese neu migrierten Anwendungen aufgrund ihrer Migration in die Cloud unterschiedliche Netzwerkzugriffsmodelle haben. Dies kann das Endbenutzererlebnis stören oder herausfordern. Ihre Zero Trust-Lösung kann oft diese Reibung beseitigen, indem sie den Benutzern einen transparenten und sicheren Zugang zu diesen Cloud-basierten Anwendungen bietet und gleichzeitig dynamische und kontextsensitive Zugriffsrichtlinien durchsetzt.

Empfehlungen

Wir empfehlen nachdrücklich, dass Sie, wenn diese Anwendungen in eine Cloud-Umgebung migrieren, mit den Anwendungseigentümern zusammenarbeiten und Zero Trust als Teil des Migrations- und Bereitstellungsplans einbeziehen. Die einzige Ausnahme dazu könnte die Übernahme von SaaS-Anwendungen sein, die möglicherweise nicht in jeder Umgebung Zero Trust benötigen.

Seien Sie schließlich proaktiv und arbeiten Sie mit Ihren Anwendungseigentümer-Kollegen zusammen. Wenn Sie sie Ihrer Zero Trust-Plattformarchitektur und Roadmap aussetzen, kann dies tatsächlich ein Katalysator für die Beschleunigung von Cloud-Migrationsprojekten sein.

Zugriff von Dienst zu Dienst

Die Zugriffskontrolle von Dienst zu Dienst ist definitiv ein legitimer, wertvoller und wichtiger Anwendungsfall für Zero Trust. Dennoch beginnen viele unternehmensweite Zero Trust-Implementierungen mit dem Zugriff von Benutzer zu Dienst und konzentrieren sich darauf, aus guten Gründen. Benutzer und Server leben in sehr unterschiedlichen Welten und haben sehr unterschiedliche Risikoprofile.

Benutzer

- Sind unzuverlässig und unvorhersehbar
- Betreiben ihre Geräte in unzuverlässigen, nicht verwalteten Netzwerken
- Sind mobil – greifen von verschiedenen und wechselnden Standorten zu

- Tendieren dazu, ihre Geräte zu verlieren
- Verwenden oft Passwörter erneut oder wählen schlechte Passwörter
- Besuchen im Grunde genommen zufällige Internetziele und können ohne eine Whitelist von Internetzielen nicht arbeiten, ohne die Produktivität des Benutzers zu beeinträchtigen
- Erhalten E-Mails mit Phishing-Links und klicken gelegentlich darauf
- Installieren willkürliche und nicht verwaltete Software auf Geräten

Das heißt, Benutzer sind unvorhersehbare, kreative und fehleranfällige Menschen.

Andererseits sind Server (und die Dienste, die auf ihnen laufen) oder sollten zumindest das genaue Gegenteil sein:

- Laufen in unternehmensverwalteten Netzwerken.
- Sind vertrauenswürdiger – 100% der Dienste, die auf einem bestimmten Server laufen, sollten bekannt, verwaltet und von der IT kontrolliert werden.
- Besuchen keine zufälligen Internetziele – theoretisch kann die Menge der internen und externen Netzwerkziele bekannt und auf eine Whitelist gesetzt werden.
- Erhalten keine E-Mails mit Phishing-Links.
- Verlieren sich nicht in Bars oder Restaurants.

Tatsächlich sind Server so vertrauenswürdig, dass viele Zero Trust-Architekturen ein Segment des Netzwerks hinter einem PEP enthalten, in dem Server außerhalb der Kontrolle der Zero Trust-Umgebung kommunizieren – die implizite Vertrauenszone, über die wir im gesamten Buch gesprochen haben.

Um klar zu sein, wir versuchen nicht, Sie davon abzuhalten, Zero Trust auf einen Dienst-zu-Dienst-Anwendungsfall anzuwenden; wir weisen nur darauf hin, dass Benutzer-zu-Dienst oft ein höheres Risiko darstellt. Dennoch sollten Zugriffskontrollen von Dienst zu Dienst Teil jeder Zero Trust-Initiative sein und könnten sogar als einer der ersten Anwendungsfälle sinnvoll sein. Lassen Sie uns den Wert und die Vorteile, die Zero Trust in diesem Szenario bringen kann, überprüfen.

Am wichtigsten ist, dass Zero Trust das Prinzip der geringsten Berechtigung durchsetzt, das entscheidend ist, um die Angriffsfläche zu reduzieren und den Schadensradius eines erfolgreichen Angriffs zu verringern. Dies bringt eine damit verbundene Risikoreduktion mit sich. Es stellt auch sicher, dass, weil alle Kommunikationen explizit durch Richtlinien gewährt werden, es eine „Top-Down"-Sichtbarkeit und Kontrolle der Kommunikation von Dienst zu Dienst gibt. Das heißt, Sicherheits- und Netzwerkteams müssen sich nicht mehr auf das *Erkennen* von Kommunikationen zwischen Diensten über ein bestimmtes Protokoll verlassen. Stattdessen stellt das Zero Trust-System, weil es auf einer Default-Deny-Basis arbeitet, sicher, dass alle Kommunikationen von Dienst zu Dienst stattfinden, wenn und nur wenn sie durch eine Richtlinie gewährt wurden und daher ausdrücklich erlaubt sind.

Dies hat einen interessanten Effekt – es dient tatsächlich als eine Form der *referenziellen Integrität* für das Netzwerk – weil alle Kommunikationen von Dienst zu Dienst durch eine gewährte Richtlinie erlaubt sein müssen, stellt es sicher, dass diese Kommunikation von Bereitstellungssystemen und -prozessen erwartet wird. Da unerwartete Kommunikationswege blockiert werden, hilft es, die Reife und Vorhersehbarkeit des Entwicklungs- und Bereitstellungsprozesses zu verbessern. Obwohl dies zusätzlichen Reibungspunkt zu verursachen scheint, wird es mehr als zurückgezahlt in Bezug auf erhöhte Zuverlässigkeit, Automatisierungsfähigkeit und verbesserte Sicherheit und Resilienz. Und es stellt sicher, dass bereitgestellte Dienste dokumentiert und katalogisiert sind, wodurch das Problem „Berühren Sie diesen Server nicht, wir wissen nicht, was er tut" beseitigt wird.

Obwohl dies ausreichend wertvoll erscheinen mag, um den Anwendungsfall von Dienst zu Dienst zu rechtfertigen, bringt es auch zusätzliche Vorteile. Zero Trust bringt eine allgemeine Risikoreduktion und eine damit verbundene Verbesserung der Compliance. Es gibt viele Compliance-getriebene Kontrollen, die eine bessere Netzwerksegmentierung erfordern, insbesondere für hochwertige Workloads. Zero Trust stellt auch sicher, dass der Netzwerkverkehr verschlüsselt ist, falls Anwendungen unverschlüsselte Protokolle verwenden. Und schließlich bedeutet die Tatsache, dass Zero Trust-Systeme dynamisch und automatisch auf Änderungen innerhalb des Satzes von geschützten Ressourcen reagieren können, dass Unternehmen hochdynamische Entwicklungsprozesse (wie DevOps, die wir in Kürze diskutieren) übernehmen können, ohne die Sicherheit zu opfern.

Überlegungen

Betrachtet man Zero Trust Modelle im Kontext von Dienst-zu-Dienst, scheint die Mikrosegmentierung die offensichtliche Wahl zu sein und könnte die beste Lösung für Umgebungen sein, in denen alle Server Identitäten haben und authentifiziert werden können. Dies ist notwendig, denn in dem Mikrosegmentierungsmodell sind alle Server Identitäten (Zero Trust Subjekte) und die Zugriffskontrollmechanismen tendieren dazu, diese Dienst-zu-Dienst Symmetrie widerzuspiegeln.

Die Enklaven-basierten und Cloud-gerouteten Modelle funktionieren auch für diesen Anwendungsfall und könnten sogar eine bessere Wahl für Umgebungen sein, in denen Sie gerade erst mit Zero Trust beginnen. Diese Modelle bieten Ihnen mehr Flexibilität, insbesondere wenn Sie eine Umgebung haben, in der einige identifizierte und authentifizierte Dienste (Subjekte) auf entfernte Dienste zugreifen müssen, die Ziele sind, die durch eine PEP geschützt sind, aber selbst keine Zero Trust Subjekte sind. Tatsächlich wird dies wahrscheinlich ein häufiges Server-zu-Server Szenario in vielen Bereitstellungen sein – asymmetrischer Dienst-zu-Dienst, bei dem ein Dienst eine authentifizierte Identität ist und der andere Dienst nicht, aber hinter einer PEP sitzt, wie in Abb. 18-2 dargestellt.

Dieses Modell ist eine gute Alternative zur „reinen“ Mikrosegmentierung, die erfordert, dass jeder Dienst eine Identität ist, was für einige Organisationen oder Architekturen nicht gut geeignet sein mag. Dieser Ansatz ist auch nützlich für die Sicherung des Dienst-zu-Dienst Zugriffs über verschiedene Netzwerke hinweg, insbesondere für verteilte Anwendungskomponenten, die durch eine Cloud-Migration entstehen können. Die Dienst-zu-Dienst Zugriffskontrolle über Netzwerke hinweg ist ein guter Anwendungsfall für Zero Trust, da es von Natur aus einen Bedarf an einer Sicherheitsüberlagerung gibt, die das verwendete Zugriffskontrollmodell normalisiert.

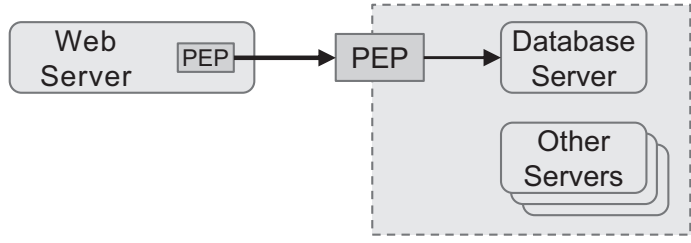

Abb. 18-2. *Asymmetrischer Dienst-zu-Dienst*

Tatsächlich gibt es noch einen weiteren Dienst-zu-Dienst Ansatz, den wir erwähnen müssen, der die Verwendung einer IoT-Stil nicht-Identitäts-Zugriffskontrollmethode beinhaltet. Wie wir in Kap. 16 besprochen haben, sind in diesem Modell keine der Dienste authentifizierte Identitäten. Das heißt, Sie können sich entscheiden, Ihre verbindungsinitiierenden Dienste so zu behandeln, als wären sie ein IoT-Gerät, mit Zugriffskontrollen, die auf schwächeren Formen der Identifikation und Authentifizierung basieren, wie MAC-Adresse, IP-Adresse, VLAN oder Switch-Port. Dies ist möglich, hat aber einige Nachteile, wie wir in Kap. 16 diskutiert haben. Aus diesen Gründen empfehlen wir diesen Ansatz für Dienst-zu-Dienst, wenn möglich, nicht – es ist viel besser, mindestens eine der Identitäten zu authentifizieren.

Empfehlungen

Eine Möglichkeit, gute Kandidaten für den Dienst-zu-Dienst Anwendungsfall zu identifizieren, besteht darin, zu ermitteln, wo Sie Server haben, die über Netzwerk- oder Domänengrenzen hinweg kommunizieren. Dies wird ein natürlicher Ort sein, um eine PEP zu implementieren, da der Verkehr eine Netzwerkgrenze überquert. Daher kann dies ein relativ einfaches Problem sein, das zu lösen ist.

Das Ziel von Peer-Servern in einem einzigen internen LAN kann schwieriger sein, abhängig von der Netzwerkkonfiguration und davon, wie schwierig oder einfach es ist, die Server hinter einer PEP zu isolieren. Andererseits kann die Isolation von Servern mit hohem Wert oder die durch Compliance getriebene Serverisolation ein guter Grund sein, dieses Szenario zu priorisieren, insbesondere wenn es einen starken Bedarf aus Risiko- oder Audit-Perspektive gibt. Diese Treiber können ein Katalysator für die notwendigen Netzwerk- und Zugriffsänderungen sein.

Wenn Sie diesen Anwendungsfall in Betracht ziehen, schauen Sie sich Ihre Umgebung an und versuchen Sie, Dienste zu identifizieren, die gut passen würden – insbesondere Dienste, die einen hohen Wert haben, gut verstanden und gut kontrolliert sind und vielleicht sehr dynamisch sind und schwer mit aktuellen Lösungen zu sichern sind. Automatisierte Zero Trust Richtlinien können hier eine große Hilfe sein, indem sie den Zugriff an Änderungen in Ihrer Serverumgebung anpassen, ohne manuellen Aufwand zu erfordern.

Denken Sie auch daran, dass viele Server mehrere Dienste hosten und Sie können sich dafür entscheiden, nur einige der Dienste hinter einer PEP zu platzieren und die anderen unverändert zu lassen. Zum Beispiel können Sie eine PEP einsetzen, um den

Server-zu-Server Zugriff für einen Datenbankdienst, der auf einem bestimmten Host läuft, zu kontrollieren, während Sie weiterhin Nicht-Zero Trust Benutzern den direkten Zugriff auf einen Webserver auf demselben Host erlauben.

Schauen Sie sich schließlich alle Microservices-Umgebungen an, die Ihre Organisation eingesetzt hat. Wie wir in Kap. 14 diskutiert haben, ist eine Microservices-Umgebung wie ein Service-Mesh möglicherweise nicht der beste Zero Trust Kandidat, da sie wahrscheinlich ihr eigenes internes und in sich geschlossenes Autorisierungsmodell hat. Aber Dienst-zu-Microservice kann ein guter Anfang sein, solange es eine klare Abgrenzung und eine natürliche Passform für eine PEP gibt. Natürlich muss Ihr Richtlinienmodell die Definition von Microservices als Ziele unterstützen, mit attribut- und kontextbasierten Zugriffskontrollen, damit dies effektiv sein kann.

DevOps

DevOps – eine Kombination der Begriffe *Entwicklung* und *Betrieb* – repräsentiert eine neuere Art der Anwendungsentwicklung, die auf der Zusammenarbeit zwischen ehemals isolierten Softwareentwicklungs- und Betriebsteams basiert. Durch den Einsatz von automatisierten Werkzeugen und schnellen Zykluszeiten hat sich dieser Ansatz – der kulturelle und prozessuale Veränderungen erfordert – als hilfreich erwiesen, um die Bereitstellungsgeschwindigkeit, die Qualität der Freigaben und den Geschäftswert von Organisationen dramatisch zu erhöhen.

Letztendlich geht es bei DevOps darum, Code schnell und kontinuierlich in die Produktion zu bringen. Häufig setzen DevOps-Teams Continuous Integration (CI) und Continuous Delivery (CD) Ansätze ein, die einen hohen Grad an Automatisierung während der Build-, Test-, Release- und Deploy-Phasen von DevOps nutzen. Diese Automatisierung ist in den Ansatz „Infrastruktur als Code“ eingebunden, bei dem nicht nur die Softwareanwendung automatisch gebaut und bereitgestellt wird, sondern auch die virtuelle Infrastruktur, auf der sie läuft – und beide werden durch Konfiguration (Code) in einem Repository beschrieben.

Das mag komplex klingen – und das ist es auch – aber es hat Organisationen die Möglichkeit gegeben, Anwendungen schnell auf den Markt zu bringen, die Produktivität der Teams zu steigern, Produktionsumgebungen zu stabilisieren, die Kundenzufriedenheit zu erhöhen und konsistente Code-Bereitstellungen zu gewährleisten – letztendlich den Geschäftswert zu liefern.

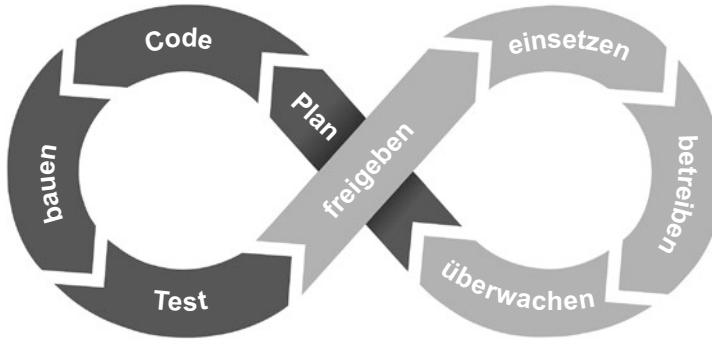

Abb. 18-3. *Der DevOps Zyklus*

Abb. 18-3 zeigt die verschiedenen Phasen von DevOps. Dies wird häufig (und absichtlich) mit dem „Unendlichkeits"-Symbol dargestellt, das die kontinuierliche und nie endende Natur von DevOps repräsentiert. Eine natürliche Frage ist natürlich, wo die Sicherheit in das DevOps-Modell passt. Die Antwort – die einzige richtige Antwort – ist „überall".

Tatsächlich gibt es einen Begriff und eine Reihe von Praktiken, die sich der Anwendung von Sicherheit in ganz DevOps widmen, genannt *DevSecOps*. Dieser Ansatz stellt sicher, dass mehrere Aspekte der Sicherheit ordnungsgemäß in das Software-Design, die Entwicklung, die Bereitstellung und den Betrieb integriert werden. Dies ist wichtig, denn traditionell war die Sicherheit ein Nachgedanke der Entwicklung, mit nachteiligen Ergebnissen. Im Gegensatz dazu können Sicherheitsframeworks effektiv in den gesamten DevOps-Zyklus eingewoben werden, wenn die Sicherheit von Anfang an konzipiert und durchdacht wird.

Beachten Sie, dass wir in diesem Abschnitt DevOps aus einer engen Zero Trust-Perspektive betrachten, es gibt jedoch einen viel größeren Teil der Anwendungssicherheit, der außerhalb des Geltungsbereichs von Zero Trust liegt – wie statische Code-Analyse, funktionale Sicherheitstests, Fuzzing/Input-Validierung und Bibliotheks-Schwachstellenmanagement.

DevOps Phasen

Schauen wir uns nun die DevOps-Phasen an und sehen, wie Zero Trust auf sie angewendet wird.

Planen und Codieren

Aus Designperspektive sollten Sicherheitsteams in dieser Phase mit den Anwendungsentwicklern zusammenarbeiten und sie über ihre Zero Trust-Architektur, Fähigkeiten und Richtlinienmodelle aufklären. Diese Kenntnisse helfen den Anwendungsentwicklern zu entscheiden, wo sie sich auf die Zero Trust-Plattform verlassen können und wo sie selbst Verantwortung übernehmen müssen. Zum Beispiel muss eine hochwertige Anwendung keine MFA, Gerätehaltungsprüfungen oder Geolokalisierungsbeschränkungen implementieren, wenn sie sich darauf verlassen kann, dass die Zero Trust-Plattform dies tut.

Und Anwendungsentwickler könnten in der Lage sein, die Zero Trust-Plattform zu nutzen, um zusätzlichen Benutzerkontext zu erhalten, wie zum Beispiel die Validierung von Rollen oder Berechtigungen. Diese könnten innerhalb der Anwendung konsumiert und durchgesetzt werden, was die Anwendung im Wesentlichen zu einem Richtliniendurchsetzungspunkt macht.

Bauen und Testen

Wenn der Anwendungscode durch die Build- und Testphasen geht, ist dies ein natürlicher Ort für das Zero Trust-System, um automatisierte Richtlinien zu verwenden, die nur den richtigen Personen und Tools Zugang gewähren, basierend auf den Attributen der Arbeitslast. Zum Beispiel könnte eine Test-Arbeitslast automatisch hochgefahren werden und nur Zugang zu in Bearbeitung befindlichen Anwendungsinstanzen haben, die ordnungsgemäß als *Test* gekennzeichnet sind.

Freigeben und Bereitstellen

Diese letzten Schritte des Freigabeprozesses führen dazu, dass die Anwendung in einer Produktionsumgebung mit einem vollständigen Satz von Richtliniendurchsetzungen platziert wird. Das heißt, der Zugang zu Anwendungsdiensten wird durch Richtlinien gesteuert, die nur authentifizierten und autorisierten Subjekten gewährt werden. Abhängig vom Grad der Automatisierung können Zero Trust-Richtlinien sogar den Zugang zur Produktionsumgebung steuern, zum Beispiel basierend auf genehmigten Änderungsfenstern oder einem gültigen Service Desk-Ticket.

Betreiben und Überwachen

Für diese Phase wird Zero Trust dazu beitragen, die Stabilität der Umgebung zu gewährleisten und jeglichen administrativen oder Fehlerbehebungszugang zu Produktionsanwendungen zu steuern. Es wird auch identitätsangereicherte Logs bereitstellen, um sicherzustellen, dass der gesamte Zugang ordnungsgemäß mit authentifizierten Identitäten verknüpft ist.

Überlegungen

DevOps ist ein interessanter und relevanter Anwendungsfall für Zero Trust, weil es so viele Möglichkeiten gibt, es damit zu verknüpfen und Wert daraus zu ziehen. Selbst eine grundlegende Integration gibt Sicherheits- und Anwendungsentwicklungsteams die Möglichkeit, Zugriffskontrollansätze und -richtlinien auszugleichen und zu teilen. Das Aufbrechen dieses traditionellen Silos hilft dabei, die Integration von Zero Trust in den gesamten Anwendungslebenszyklus „einzubacken".

Das Design eines Anwendungskomponenten (oder Mikroservice) zur Verbrauch und Durchsetzung von PDP-definierten Richtlinien kann die Anwendungssicherheit beeinflussen und die Auswirkungen und den Wert von Zero Trust im Unternehmen vertiefen. Im Wesentlichen kann dies es einer Anwendung ermöglichen, in gewisser Weise ihr eigener PEP zu werden (abhängig davon, wie viel Zero Trust-Richtlinie oder Kontext sie vom PDP konsumieren kann). Dies kann in DevOps-Zyklen eingewoben werden – wobei der Satz von Richtlinien, die der Anwendung geliefert (und daher durchgesetzt) werden, geändert wird, um ihrer aktuellen Phase zu entsprechen.

Betrachten Sie als nächstes den Anwendungsfall, auf den wir zuvor angespielt haben, bei dem die manuelle Freigabe und Bereitstellung von Code eine Sicherheitsschwäche darstellen kann. Durch die Anwendung von Zero Trust-Richtlinien während der Freigabe- und Bereitstellungsphasen können Organisationen sicherstellen, dass dieser hochwirksame Zugang ordnungsgemäß kontrolliert wird, zum Beispiel durch die Durchsetzung von genehmigten Änderungsfenstern.

Schließlich ist das Verwalten des Zugangs zu den Software-Designs und dem Quellcode Ihrer Organisation ein zentraler Anwendungsfall von Zero Trust. Diese Vermögenswerte sind offensichtlich wertvoll und wie alle hochwertigen Daten verdienen sie es, ordnungsgemäß gesichert zu werden, wobei der Zugang von einem PEP kontrolliert wird.

Empfehlungen

Der Zweck von DevOps besteht darin, eine hochgeschwindige, hochwertige, hochzuverlässige Methode zur Bereitstellung von Anwendungscode in der Produktion zu bieten, im deutlichen Gegensatz zum traditionellen Softwareentwicklungslebenszyklus (SDLC). DevOps ist besser geeignet für viele der heutigen schnell wechselnden Umgebungen, in denen das schnelle Einbringen von inkrementellem Code in die Produktion oft den Geschäftswert vorantreibt.

Da Zero Trust-Systeme selbst von Natur aus dynamisch sind und auf Benutzer-, Service- und Infrastrukturkontext reagieren, eignen sie sich gut für den Einsatz in einer DevOps-Umgebung. Ein Zero Trust-System kann mit den DevOps-Plattformen einer Organisation verbunden werden und den Zugang automatisch anpassen, wenn Arbeitslasten durch den gesamten Anwendungslebenszyklus fließen. Zero Trust hilft auch dabei, die Sicherheit zu verbessern und zu automatisieren, in Bereichen, die möglicherweise noch manuelle Schritte erfordern, zum Beispiel durch die Automatisierung von Zugangskontrollen basierend auf genehmigten Änderungsfenstern.

DevOps und Zero Trust sind beides moderne und effektive Ansätze, und Organisationen sollten definitiv prüfen, wie sie in Unterstützung voneinander integriert werden können.

Fusionen und Übernahmen

Aus sicherheitstechnischer und technischer Sicht stellen Fusionen und Übernahmen (M&A) komplexe und oft langwierige Projekte dar, die versuchen müssen, zwei zuvor unabhängige Unternehmen in Einklang zu bringen. Die IT- und Sicherheitsinfrastrukturen dieser Unternehmen wurden vollständig getrennt aufgebaut und weiterentwickelt, wobei Technologien und Architekturen auf Weisen genutzt wurden, die inkompatibel sein können (oder zumindest schwer zu vereinbaren sind). Diese beiden Organisationen werden fast sicher in vielen Bereichen doppelte Lösungen haben und wahrscheinlich überlappende Netzwerk-IP-Adressbereiche haben, die Probleme verursachen werden – ein allzu häufiges Auftreten in unserer IP v4-zentrierten Welt.

Denken Sie daran, dass Zero Trust-Plattformen neben der Bereitstellung von Sicherheit auch eine vereinheitlichende oder normalisierende Schicht über heterogene Ressourcen und Netzwerke bieten. Dies hat viele Vorteile innerhalb eines einzelnen Unternehmens, wie wir in diesem Buch diskutiert haben, und es hilft auch, den Netzwerkzugriff in einem M&A-Szenario schnell zu ermöglichen.

Insbesondere und taktisch kann ein Zero Trust-System nahezu sofortigen IT-Zugriff über Domänen hinweg bieten, um eine schnelle gemeinsame Verwaltung zu ermöglichen. Ebenso kann es einen präzisen und sicheren Benutzerzugriff auf bestimmte geschäftskritische Anwendungen ermöglichen, zum Beispiel Finanzmanagementsysteme. Angesichts dieses Werts wollen wir uns das nächste Detaillevel ansehen.

Überlegungen

Wenn eines der beiden Unternehmen bereits eine Zero Trust-Implementierung hat, sollte eine M&A-Aktivität ein offensichtlicher Katalysator sein, um deren Nutzung auszuweiten, insbesondere wenn es sich um das übernehmende Unternehmen handelt (das tendenziell größer ist und seine IT- und Sicherheitsinfrastruktur besser durchsetzen kann). Aber selbst wenn das erworbene Unternehmen dasjenige mit Zero Trust ist, kann das fusionierte Unternehmen diese Plattform immer noch nutzen, um zumindest die Integrationsaktivitäten zu beschleunigen. Der Wert davon sollte offensichtlich sein – keine andere Sicherheits- oder Remote-Zugriffslösung kann zwei unterschiedliche (und oft widersprüchliche) Unternehmen so schnell, zuverlässig oder präzise zusammenbringen.

Ein Zero Trust-Ansatz kann auch eine Gelegenheit darstellen, um erhebliche Kosten und Anstrengungen zu vermeiden, die normalerweise benötigt werden, um die Netzwerke letztendlich zu fusionieren, zu normalisieren oder zu entwirren. Zum Beispiel könnte es nicht notwendig sein, ein WAN zu implementieren, um die Unternehmensnetzwerke zu verbinden, wenn alle Benutzer und Server den Zugriff erhalten, den sie durch ein Zero Trust-System benötigen. Und die Unternehmen müssen möglicherweise keine überlappenden IP-Adressen in den Netzwerken entwirren, wenn das Zero Trust-System Zugriffsmechanismen unterstützt, die dies kompensieren können.

Wenn Sie sich diesem Anwendungsfall nähern, denken Sie darüber nach, auf welche Ressourcen die Menschen sofortigen Zugriff benötigen, wo sie sich befinden und wie sie heute geschützt sind. Natürlich wird jedes Unternehmen seinen eigenen Identitätsanbieter, IT-Management und Sicherheitstools haben – all dies kann Zero Trust fast sofort normalisieren.

Empfehlungen

Wenn Sie eine Zero Trust-Lösung haben und ein Unternehmen erwerben, sollte es ein „No-Brainer" sein, diese zur Beschleunigung des Übergangs zu nutzen. Wenn Sie noch keine solche Lösung implementiert haben, aber das Unternehmen, das Sie erwerben, dies tut, sollten Sie ernsthaft in Erwägung ziehen, diese Zero Trust-Plattform zur Unterstützung Ihres Übergangs zu nutzen. Mindestens sollten Ihre Mitarbeiter in der Lage sein, sie zu nutzen, um auf Ressourcen des erworbenen Unternehmens zuzugreifen. Und Sie sollten in der Lage sein, dieses System leicht zu erweitern, um den Benutzern des erworbenen Unternehmens Zugang zu den Ressourcen Ihres Unternehmens zu gewähren, zum Beispiel durch die Bereitstellung eines PEP in Ihrem Unternehmensnetzwerk. Idealerweise können Sie dies nutzen, um den Fall für die Einführung von Zero Trust in Ihrem größeren Unternehmen zu machen – das erworbene Unternehmen hat Erfolg damit gehabt, und Sie sollten in der Lage sein, dies schnell zu nutzen, um Wert zu liefern.

Vergessen Sie schließlich nicht den Server-zu-Server-Anwendungsfall. In vielen Fällen gibt es Datensynchronisations- oder Export-/Importaktivitäten, die erfordern, dass Produktionsserver in einer Domäne sicher mit Produktionsservern in einer anderen kommunizieren. Zero Trust-Systeme ermöglichen es, dies schnell und sicher zu erreichen, ohne dass eine der Organisationen gefährdet wird.

Abspaltung

Abspaltung, bei der ein Unternehmen einen Teil seines Geschäfts in eine neu gegründete unabhängige Einheit ausgliedert, stellt in der Regel eine komplexe Herausforderung für IT und Sicherheit dar, ist aber auch eine spannende Gelegenheit. Das neue Unternehmen wird sicherlich einen Teil der IT- und Sicherheitsinfrastruktur erben, oft einschließlich physischer Vermögenswerte wie Hardware,

Netzwerkausrüstung, Netzwerke und Gebäude. Während diese Vermögenswerte die Definition von „Brownfield“-Umgebungen sind, werden IT- und Sicherheitsteams in der Regel auch befugt sein, neue Systeme und Tools auszuwählen, um Lücken zu füllen oder Elemente zu ersetzen, die im Laufe der Zeit stillgelegt werden müssen. Dies sollte den IT- und Sicherheitsteams die Möglichkeit (und das Budget) geben, ein Zero Trust-System für diese neue Umgebung zu implementieren.

Neben der Bereitstellung einer Infrastruktur für ein neues Unternehmen gibt es auch einen weiteren Aspekt einer Abspaltung, der sich für Zero Trust eignet – die Übergangsphase. Bei fast jeder Abspaltung erfolgt die geschäftliche und rechtliche Transaktion, bevor ein Großteil der technischen Arbeit überhaupt beginnen kann. Auch wenn die Unternehmen rechtlich getrennt sind, werden sie immer noch durch zahlreiche technische Systeme, Datenflüsse und Geschäftsprozesse miteinander verbunden sein, die in der Regel Monate dauern, um sie zu entwirren. Zero Trust kann sehr effektiv eingesetzt werden, um eine präzise Zugriffskontrolle auf kritische Ressourcen zu bieten, die während dieser Übergangsphase „zurückgelassen“ wurden – Benutzer und Server produktiv zu halten, während unbefugter Netzwerkzugriff verhindert wird. Während das neue Unternehmen nach und nach von den Systemen umsteigt, kann der Zugriff auf sie durch eine einfache Richtlinienänderung im Zero Trust-System leicht beendet werden.

Vollständige Zero Trust-Netzwerk-/ Netzwerktransformation

Dies ist ein passender Anwendungsfall, um das Kapitel abzuschließen und uns auf die Diskussion über den Weg der Implementierung von Zero Trust vorzubereiten, in Kap. 19. Dieses Szenario ist in gewisser Weise eine Zusammenstellung der gerade behandelten Szenarien und in gewisser Weise erheblich anders als alle anderen.

Der wichtigste Unterschied besteht darin, dass der vollständige Umstieg auf „Zero Trust“ einen Wechsel in der Netzwerkphilosophie beinhaltet, nämlich alle Ihre Benutzer „off net“ zu nehmen und die Nutzung des Zero Trust-Systems für den Zugriff auf *jede* Unternehmensressource zu erfordern. Interessanterweise hat der abrupte, durch COVID-19 bedingte Wechsel zu einer überwiegend von zu Hause aus arbeitenden Benutzerpopulation Anfang 2020 die Bereitschaft vieler Organisationen zur Durchführung dieser Änderung beschleunigt. Der größte Denkwechsel, der damit

verbunden ist, ist die Erkenntnis, dass das zu lösende Problem nicht „Remote-Zugriff“ ist – es ist einfach „Zugriff“. Tatsächlich untermauert ein einheitlicher Ansatz zur Sicherung *aller* Zugriffe einen Großteil des Werts einer Zero Trust-Umgebung.

Der Begriff „vollständiges Zero Trust-Netzwerk“ impliziert einen großen und umfassenden Umfang, aber in der Praxis definieren Sie die Grenzen und Grenzen für Ihre Initiative – nicht jede Zero Trust-Reise muss mit einer Mikrosegmentierung für jede einzelne Ressource enden. In gewisser Weise ist es vorteilhaft, den eher mehrdeutigen Begriff „Netzwerktransformation“ zu verwenden, anstatt den Begriff „vollständiges Zero Trust“, der einige Leute zu einer falschen Schlussfolgerung führen könnte.

Definieren Sie also, während Sie diesen Prozess durchlaufen, Grenzen und haben Sie eine realistische Vision für Ihren Endzustand im Kopf. Nach unserer Erfahrung haben wir am häufigsten gesehen, dass Unternehmen ihren Zero Trust-Endzustand wie folgt vorstellen:

- Alle Benutzer sind vom Unternehmensnetzwerk getrennt.
- Die meisten privaten Dienste sind durch PEPs geschützt, in der Regel nach dem Enklaven-basierten Modell.
- Einige SaaS-Dienste können durch PEPs geschützt sein.
- Es kann einige Dienstesätze geben, die Mikrosegmentierung verwenden.
- Es wird einige implizite Vertrauenszonen geben, in denen Dienste laufen.

Die Implikationen davon sind natürlich die Veränderungen und Vorteile, die wir in diesem Buch immer wieder betont haben. Die Beseitigung des vertrauenswürdigen Unternehmensnetzwerks verleiht der Organisation viel mehr Resilienz und reduziert sowohl die Angriffsfläche als auch den Schadensradius. Benutzer haben einen „immer aktiven“ Zero Trust-Zugang, bei dem dynamische und kontextsensitive Richtlinien bewertet werden, um ihnen ausreichenden Zugang zur Produktivität zu gewähren, während das Prinzip der geringsten Privilegien durchgesetzt wird. Dieses Prinzip stellt sicher, dass alle Zugriffe explizit durch Richtlinien gewährt werden, wodurch die Sichtbarkeit der Organisation auf Netzwerk- und Rechenressourcen erhöht wird. Und die IT- und Sicherheitsinfrastruktur des Unternehmens ist auf Daten- und Prozessebene integriert, was die Effizienz und Effektivität erhöht. Werfen wir noch einmal einen Blick

auf das konzeptionelle Zero Trust-Architekturdiagramm, das wir zu Beginn des Buches in Kap. 3 eingeführt haben, das in Abb. 18-4 erneut dargestellt ist.

Dieses Diagramm zeigt die Wege, auf denen das repräsentative Unternehmen aus Kap. 3 ihre „vollständige Zero Trust"-Architektur implementiert hat. Sie haben die meisten der im Buch diskutierten Ansätze integriert, um ihre Bedenken zu adressieren und ihre gewünschten Vorteile zu erzielen. Schauen wir uns an, wie sie das angegangen sind.

Ihr PDP ist natürlich mit ihrem Unternehmensidentitätsanbieter (IAM) verbunden – das ist eine grundlegende Voraussetzung. Und ihr PDP ist auch mit anderen IT- und Sicherheitsinfrastrukturelementen integriert, wie zum Beispiel ihren MFA, SIEM, GRC, Endpunktverwaltung und PKI-Systemen. Es gibt eine Reihe von verteilten PEPs in ihrer Infrastruktur – viele davon erzwingen den Zugang zu Ressourcenklaven. Die Organisation verwendet auch lokale Benutzeragenten-PEPs auf den meisten

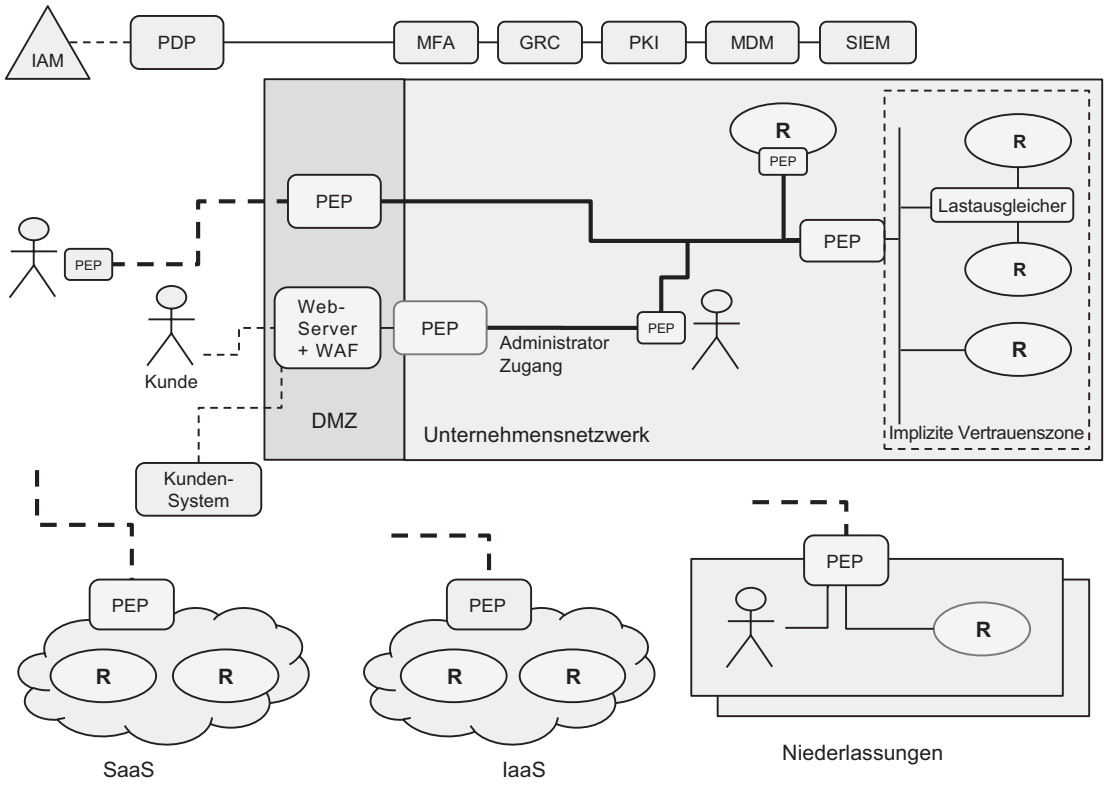

Abb. 18-4. *Zero Trust Architektur*

Benutzergeräten und hat PEPs direkt auf einige Server implementiert. Beachten Sie, dass es eine verschlüsselte PEP-zu-PEP-Verbindung zwischen dem PEP in der DMZ und dem PEP vor der impliziten Vertrauenszone gibt – dies ist eine Konfiguration, die von einigen Zero Trust-Plattformen unterstützt wird.

Ihr Zero Trust-System sichert den Zugang zu SaaS- und IaaS-Ressourcen, und die PEPs in ihrer IaaS-Umgebung verwenden dynamische Attribute (Metadaten) auf den Workloads, um Zugriffskontrollentscheidungen zu treffen. Beachten Sie, dass sie in ihren Niederlassungen den PEP so implementiert haben, dass er Ressourcen und Benutzer aus einer IoT-Stil-Perspektive verwaltet. Das heißt, Geräte (und Benutzer) in diesem Netzwerk können auf Zero Trust-geschützte Ressourcen zugreifen (und von ihnen zugegriffen werden).

Schließlich beachten Sie, dass nicht *alle* Elemente im Netzwerk für die Zero Trust-Lösung relevant sind. Zum Beispiel gibt es implizite Vertrauenszonen (Ressourcenklaven) in der IaaS-Umgebung sowie zwischen den Ressourcen im Unternehmensnetzwerk. Beachten Sie auch, dass der Admin-Zugang zum Webserver in der DMZ von einem PEP kontrolliert wird, der Kundenzugang zu anderen Diensten auf diesem Server jedoch außerhalb des Anwendungsbereichs der Zero Trust-Lösung liegt.

Überlegungen

Offensichtlich ist ein vollständiges Zero Trust eine große Initiative und wird auch mit Unterstützung und Zustimmung von oben eine technische und organisatorische Herausforderung sein. Tatsächlich werden nicht alle Unternehmen dafür bereit sein, insbesondere als erste Zero Trust-Maßnahme. Wir werden diesen Aspekt in Kap. 19 weiter untersuchen, aber bevor wir das tun, möchten wir einige Empfehlungen aussprechen.

Empfehlungen

Obwohl ein groß angelegtes Netzwerktransformationsprojekt möglicherweise zunächst nicht möglich ist, möchten wir betonen, dass die Reduzierung der Netzwerkprivilegien der Benutzer ein wichtiges Ziel ist; tatsächlich ist es eine der wichtigsten Maßnahmen, die Sie im Rahmen Ihrer Zero Trust-Initiative durchführen können. Dies kann

schrittweise erreicht werden, so dass selbst wenn Sie dies Subnetz für Subnetz (oder VPC für VPC, oder Anwendung für Anwendung) erreichen, es einen Wert bietet.

Wir erkennen an, dass Unternehmensnetzwerke komplex sind und dass es viele vorhandene Elemente gibt, die als Einschränkungen oder Barrieren erscheinen könnten. Aber das muss nicht unbedingt der Fall sein. Betrachten Sie zum Beispiel ein Büro mit Druckern, zu denen Benutzer impliziten Zugang erhalten, wenn sie vor Ort sind. Dieser Zugang kann leicht durch eine Zero Trust-Richtlinie bereitgestellt werden, und diese Anforderung sollte kein Hindernis für die Einführung von Zero Trust sein. Tatsächlich können in einigen Fällen vorhandene Komponenten genutzt werden, um Zero Trust zu ermöglichen. Einer unserer Unternehmenskunden hatte eine NAC-Lösung, die bereits in über 50 Niederlassungen implementiert war. Als sie ihren Zero Trust-Agenten auf den Geräten der Benutzer gruppenweise ausrollten, konfigurierten sie das NAC so, dass Benutzer in den relevanten Gruppen dem *Gast* VLAN statt dem *Mitarbeiter* VLAN zugewiesen wurden, was sie effektiv vom Netz nahm. Das Schöne an dieser Änderung ist, dass die Endbenutzer es nicht einmal bemerkten – sie blieben voll produktiv und konnten auf alle ihre Anwendungen zugreifen.

In gewisser Weise ist jeder der vorherigen sechs Anwendungsfälle ein Mikrokosmos der Ideen, Ansätze und Herausforderungen des vollständigen Zero Trust-Netzwerkszenarios. Das macht diese Probleme so interessant und ist auch ein weiterer guter Grund, mit einem fokussierteren Anwendungsfall statt mit vollständigem Zero Trust zu beginnen. Indem Sie mit einem kleineren Szenario und Benutzerpopulation beginnen, müssen Sie nicht jedes Problem „im großen Stil“ strategisch lösen, und doch werden Sie unterwegs Dinge lernen und schaffen (Richtlinien, Teams, Prozesse usw.), die es Ihnen viel leichter machen, diesen größeren Anwendungsfall im Laufe der Zeit zu erreichen.

Zusammenfassung

Zusammenfassend haben wir in diesem Kapitel sieben verschiedene Szenarien für die Anwendung von Zero Trust im Unternehmen analysiert. Die meisten dieser Anwendungsfälle haben wir im Laufe des Buches erwähnt, aber dieses Kapitel gab uns die Möglichkeit, jeden von ihnen in der Tiefe zu untersuchen und dies mit dem Vorteil zu tun, auf dem Wissen und Kontext aufzubauen, den wir in den vorangegangenen 17

Kapiteln gelernt haben. Wenn wir aus den Details dieser Anwendungsfälle auftauchen, nehmen Sie einen Atemzug und einen Schritt zurück – in Kap. 19 werden wir uns damit beschäftigen, wie Ihre Organisation Zero Trust aus der Perspektive eines Programms und einer Initiative angehen sollte, um den Erfolg zu gewährleisten.

KAPITEL 19

Zero Trust erfolgreich machen

In den ersten 18 Kapiteln dieses Buches haben wir eine Vielzahl von Sicherheits- und technischen Themen behandelt – einschließlich Zero Trust-Prinzipien und architektonischen Ansätzen, einer Untersuchung einer breiten Palette von IT- und Sicherheitselementen und einer Diskussion über Zero Trust-Richtlinien und Anwendungsfälle. Diese architektonischen Prinzipien und technischen Themen sind der Kern jeder Unterhaltung über Zero Trust. Es gibt jedoch noch einen verbleibenden Aspekt, der in der am häufigsten gestellten Zero Trust-Frage zum Ausdruck kommt: „Wie fange ich an?“ Das ist eine berechtigte Frage, aber die *Frage hinter der Frage* ist das, was wir für das fehlende Thema halten: „Wie kann ich sicherstellen, dass mein Zero Trust-Projekt erfolgreich ist?“ Dieses Kapitel zielt darauf ab, diese Frage zu beantworten.

Unsere beste Antwort in einem Satz ist eine Empfehlung, einen fokussierten und schrittweisen Ansatz zu verfolgen, während Sie immer noch den Überblick über (und die Planung für) Ihre größere Zero Trust-Initiative behalten und sich bewusst die Zeit nehmen, Brücken und Kommunikationslinien mit Ihren Kollegen in der gesamten Organisation aufzubauen. Das bedeutet nicht, dass Sie kein rein taktisches Zero Trust-Projekt haben können, das von einer größeren Initiative getrennt ist – das können Sie – aber Zero Trust erfordert von seiner Natur aus die Integration mit anderen IT- oder Sicherheitskomponenten, die von anderen Teams besessen oder verwaltet werden. Dies erfordert Kommunikation und Integration mit diesen Teams, was ein wichtiger Faktor bei der Bestimmung des Erfolgsgrads sein wird, den Sie mit Ihren Zero Trust-Projekten erleben werden.

In diesem Kapitel werden wir dieses Thema untersuchen, Ihnen Anleitungen geben, wie Sie anfangen können, und diskutieren, wie Sie sicherstellen können, dass Ihr Projekt und Ihr größeres Zero Trust *Programm* erfolgreich ist. Bedenken Sie, dass Zero Trust, wie jedes breit angelegte Unternehmenssicherheits- oder IT-Projekt, neben technischen

J. Garbis und J. W. Chapman, *Zero Trust Sicherheit*, https://doi.org/10.1007/979-8-8688-0105-1_19

auch nichttechnische Herausforderungen stellen kann. Tatsächlich sind manchmal die weicheren Aspekte des Programmdesigns, der Kommunikation und des Verständnisses der Organisationskultur schwieriger als die Technologie, insbesondere für technisch orientierte Menschen wie die Autoren dieses Buches.

Wir werden Zero Trust-Initiativen aus zwei Perspektiven betrachten – von oben nach unten und von unten nach oben.[1] Dies ist eine bequeme und nützliche Möglichkeit für uns, Dinge zu trennen und darüber zu sprechen, aber in Wirklichkeit ist es eine künstliche Unterscheidung. Jedes Zero Trust-Projekt und jede Initiative wird Elemente aus beiden Perspektiven kombinieren, also betrachten Sie sie nicht als gegenseitig ausschließend – dies ist nur eine nützliche Möglichkeit, die Diskussion in diesem Kapitel zu organisieren. Insbesondere, selbst wenn Ihre Organisation eine strategische, von oben nach unten gerichtete Vision und Mission für Zero Trust hat, werden Sie immer noch taktische Projekte und Entscheidungen zu treffen haben. Ebenso wird selbst ein taktisches „unter dem Radar" Zero Trust-Projekt, das darauf abzielt, ein fokussiertes Problem zu lösen, eine Koordination und Integration mit anderen Tools und Teams erfordern und wird daher mindestens einige Elemente einer strategischen Initiative enthalten. Tatsächlich ist es eine ausgezeichnete Möglichkeit, sich auf genehmigte und unterstützte zweite und dritte Projekte vorzubereiten, wenn man strategische Aspekte in ein erstes taktisches Zero Trust-Projekt einbezieht. Nachdem wir das alles gesagt haben, lassen Sie uns eintauchen, beginnend mit der strategischen Perspektive.

Zero Trust: Ein strategischer Ansatz (Top-Down)

Ein strategischer Ansatz zu Zero Trust erfordert (per Definition) einen Befürworter auf der Führungsebene in der Organisation, idealerweise einen C-Level-Manager. Da Zero Trust keine reine IT-Initiative ist, ist eine Abstimmung zwischen den Geschäftsführern sehr wichtig für die vollständige Unterstützung und Einführung einer Zero Trust-Strategie im Unternehmen. Während Sicherheitsteams verstehen können, dass Zero Trust den Stand der Technik in den Sicherheitsbestpraktiken darstellt, mag das nicht ausreichend motivierend sein, um die Organisation dazu zu bewegen, eine strategische Zero Trust-Reise zu beginnen. In vielen Fällen kann es einen deutlichen Katalysator erfordern, wie zum Beispiel neue Sicherheits- oder Führungskräfte, einen Datenverstoß,

[1]Wir haben Gerüchte über einen dritten Ansatz – „middle-out" – von Praktikern im Silicon Valley gehört.

M&A oder sogar ein Nebenprodukt von pandemiebedingten Zugangs- und Sicherheitsänderungen. Andere Katalysatoren könnten sich ändernde regulatorische Anforderungen oder Prüfungsergebnisse innerhalb der Organisation sein.

Da dies eine unternehmensübergreifende Initiative sein wird, müssen Sicherheitsteams sich bewusst sein, dass es Geschäftsziele gibt, die erreicht werden müssen, und dass diese strategische Initiative zwangsläufig Geschäfts- und Aufsichtsprozesse beinhalten wird. Diese sollten nicht als Hindernisse wahrgenommen werden, sondern vielmehr als notwendige Sorgfalt bei der Durchführung einer Initiative von strategischer Bedeutung für das Geschäft. Mit diesem Hintergedanken werden wir nun einige organisatorische Strukturen diskutieren, die eine Rolle in einer Zero Trust-Strategie spielen könnten. Bedenken Sie, dass nicht jede Organisation alle diese Strukturen hat oder benötigt – wir stellen in gewissem Maße das „maximale Set“ dar, das nur in größeren und formelleren Organisationen existieren mag. Mit diesem Hintergedanken sollten Sie, wenn Sie Ihre Zero Trust-Strategie aufbauen, prüfen, welche der folgenden organisatorischen Strukturen vorhanden sind oder vielleicht eingerichtet werden sollten: Governance Board, Architecture Review Board und Change Management Board. Lassen Sie uns jede davon nacheinander betrachten.

Governance Board

Typischerweise erstellen Governance Boards Richtlinien, die der Organisation Orientierung geben und die allgemeine (finanzielle und personelle) Gesundheit der Organisation unterstützen. Governance Boards werden oft verwendet, um einer Organisation zu helfen, ihre Governance, Risk, and Compliance (GRC) Ziele zu erreichen, und können funktional Teil einer GRC-Gruppe sein. Sie sollten die folgenden Elemente der Organisation einschließen, da sie für Zero Trust relevant sein werden:

- Risiko
- Audit
- Betrieb
- Sicherheit
- Identität

Die Teams, die für jeden dieser Bereiche verantwortlich sind, sollten einen gewissen Einfluss auf die Erstellung von Richtlinien für die Zero Trust-Initiative haben, und ihre

Unterstützung wird entscheidend für ihren Erfolg sein. Insbesondere hat dieses Board oft ein Vetorecht, wenn Technologien überprüft und für die Aufnahme in neue Initiativen in Betracht gezogen werden. Auf einer höheren Geschäftsebene wird das Verständnis der Risikoschwelle der Organisation und die Verwaltung dieser Schwelle ein Schlüsselelement sein, das den Grad der Unterstützung für die Zero Trust-Initiative bestimmt.

Architecture Review Board

Ein Architecture Review Board (manchmal auch als Enterprise Architecture Board bezeichnet) ist verantwortlich für die Überprüfung der aktuellen und geplanten Technologie im Unternehmen und wird sehr involviert sein und relevant für eine Zero Trust-Strategie. Das Board definiert auch in der Regel die Architekturstandards des Unternehmens, die ein wichtiger Teil jeder Zero Trust-Initiative sind. Die technischen Anforderungen für Zero Trust können recht komplex sein (wie in diesem Buch mehrfach erwähnt), können aber schnell mit bestehender Technologie integriert werden, solange Architekturstandards sowohl genutzt als auch durchgesetzt werden. Diese Art von Konsistenz und unternehmensweiter Sichtbarkeit ist einer der Gründe, warum Organisationen Enterprise Architecture Boards haben. Schließlich werden die Mitglieder dieses Boards kollektive Weisheit darüber liefern können, welche Auswirkungen Änderungen an der Umgebung haben, was eindeutig relevant für jede Zero Trust-Initiative ist.

Change Management Board

Schließlich sollte ein Change Management Board in jede Initiative einbezogen werden, da es letztendlich für den Zeitpunkt und die Planung der Einführung neuer Lösungen in eine Produktionsumgebung verantwortlich sein wird. Da Zero Trust ein immer größerer und betrieblicherer Teil der Organisation wird, wird die Integration von Anwendungen und Infrastrukturen mit Zero Trust-Systemen unerlässlich werden. Dies kann tatsächlich Change Management-Prozesse beschleunigen, da mit Zero Trust die Integration und Bereitstellung stärker auf Richtlinien basieren und automatisiert werden können.

Denken Sie daran, nicht jede Organisation benötigt dieses Maß an Formalität, aber wenn Sie bereits diese Teams und ihre zugehörigen Prozesse haben, werden sie Ihre

Zero Trust-Strategie verbessern und Ihre Fähigkeit beschleunigen, Zero Trust-Elemente mit Ihrer Umgebung zu integrieren.

Werttreiber

Obwohl die Implementierung von Zero Trust in der Regel technologieorientiert ist, werden letztendlich Geschäftsziele den Anstoß für diese Projekte geben. Lassen Sie uns das Thema wechseln und die geschäftlichen Werttreiber diskutieren, die eine Zero Trust-Initiative liefern kann: Sicherheit, Audit und Compliance, Agilität/Neue Geschäftsinitiativen, Kunden-/Partnerintegrationen und Technologiemodernisierung.

Sicherheit

Sicherheit ist ein offensichtlicher Werttreiber, da sie der Fokus von Zero Trust ist. Daher ist sie in der Regel eine der treibenden Kräfte hinter jeder Zero Trust-Initiative. Beachten Sie, dass der Sicherheitsnutzen in einem bestimmten Projekt so einfach sein könnte wie die Einbeziehung von MFA in das Benutzererlebnis oder so komplex wie die Bereitstellung eines unternehmensweiten Zero Trust-Netzwerks. Beachten Sie auch, dass in einigen Fällen die Sicherheit möglicherweise nicht der primäre Fokus für jedes Projekt innerhalb einer Zero Trust-Initiative ist. Zum Beispiel könnten Sie ein Projekt haben, das eine bereits bereitgestellte Zero Trust-Plattform verwendet, um die Systeme der Kunden mit Ihren zu integrieren. Dies könnte die Sicherheit tatsächlich nicht verbessern, sondern stattdessen den Treiber für die Kunden-/Partnerintegration erfüllen, den wir später diskutieren.

Audit und Compliance

Audit und Compliance Verbesserungen sind möglicherweise nicht so offensichtlich oder technisch wertvoll, aber mit der verbesserten Protokollierung, die mit einem identitätszentrierten Ansatz verbunden ist, erhalten Sie verbesserte Audit-Ergebnisse und eine bessere Compliance-Erfüllung. Die Sichtbarkeit darüber, welche Identitäten welche Geschäftsprozesse ausüben und auf welche Technologie-Assets zugreifen, ist entscheidend für die Erfüllung der Unternehmensaudit-Anforderungen. Und Zero Trust-Projekte reduzieren oft Audit-Kosten und -Zeiten, da sie leicht zugängliche und leicht

verständliche Zugriffsprotokolle bereitstellen. Verschaffen Sie sich ein Verständnis dafür, welche Arten von Audit-Protokollberichten Ihr Zero Trust-System bereitstellt und wie sie auf die Arten von Berichten abgebildet werden, die Ihre internen und externen Prüfer suchen. Dies kann Ihrem Unternehmen einen echten Mehrwert liefern.

Agilität/Neue Geschäftsinitiativen

Zero Trust wird oft verwendet, um die Anwendungsagilität sicher zu ermöglichen oder neue Geschäfts-Initiativen, die für eine Organisation von großem Wert sein können. Zum Beispiel nehmen viele Organisationen einen „Cloud First"-Ansatz, und Zero Trust kann verwendet werden, um Leitplanken und Richtungen zu bieten. Im Allgemeinen ist das automatisierte und kontextbasierte Sicherheitsmodell von Zero Trust sehr gut geeignet, um schnell voranschreitende und innovative Geschäftsinitiativen auf der Grundlage sicherer, präziser Zugriffskontrollen zu ermöglichen.

Kunden-/Partnerintegrationen

Eines der Kernprinzipien von Zero Trust ist die Ermöglichung und der Nutzen von sicherer Integration über normalerweise abgeschottete Technologien hinweg. Dies gilt sowohl innerhalb des Unternehmens als auch extern. Daher können Unternehmen Zero Trust-Plattformen verwenden, um neue Arten von System-, Daten- und Prozessintegrationen mit Kunden und Partnern zu ermöglichen. Dies könnte so einfach sein wie die Ermöglichung eines sicheren Kundenzugangs zu einer normalerweise privaten Webanwendung oder so komplex wie der Echtzeitaustausch von Daten über Unternehmen hinweg. Beides kann erheblichen Geschäftswert und Innovation vorantreiben.

Technologiemodernisierung

Schließlich ist der Werttreiber der Technologiemodernisierung etwas breit gefasst; er kann eine Vielzahl von Vorteilen darstellen, einschließlich Upgrades veralteter Sicherheits- oder IT-Infrastrukturen, Stilllegung nun ineffektiver Systeme und Übergänge zu modernen Ersatzlösungen. Ein Großteil dieser Modernisierung wird auf die IT- und Sicherheitssysteme angewendet, die wir im Teil II dieses Buches besprochen haben, obwohl es auch andere geben wird.

Wir haben festgestellt, dass diese fünf allgemeinen Kategorien eine nützliche Möglichkeit sind, die Auswirkungen zu messen und zu kategorisieren, die jedes Zero Trust-Projekt als Bestandteil der breiteren Zero Trust-Initiative des Unternehmens haben wird. Das heißt, es hilft, die Antwort auf die Frage *„Was versucht das Unternehmen mit dieser Investition von Zeit und Geld zu erreichen?“* grob zu quantifizieren und visuell darzustellen. Diese Werttreiber gelten gleichermaßen für taktische und strategische Projekte (obwohl das Ausmaß des Nutzens variieren kann). Die Darstellung dieser in einem visuellen *Radar-Diagramm* ist eine effektive Möglichkeit, dies zu kommunizieren, und wir werden später in diesem Kapitel ein Beispiel-Szenario durchgehen. Diese Vergleiche können Ihnen und Ihrem Team helfen, Kandidatenprojekte im Laufe Ihrer Initiative objektiver zu bewerten, zu vergleichen und zu priorisieren.

Jetzt, da wir untersucht haben, wie Organisationen Zero Trust aus strategischer Sicht angehen sollten, betrachten wir es aus taktischer Sicht.

Zero Trust: Ein taktischer Ansatz (Bottom-Up)

Wir definieren ein taktisches Zero Trust-Projekt als eines, das in Umfang und Dauer begrenzt ist und darauf abzielt, ein spezifisches Problemset zu lösen. Am wichtigsten ist, dass die Lösung auf eine Weise angegangen wird, die die Prinzipien der Zero Trust-Sicherheit berücksichtigt und möglicherweise Sicherheitstools und -plattformen auf neue und andere Weise für die Organisation verwendet. Während ein erstes Zero Trust-Projekt neue Konzepte und Plattformen in eine Organisation einführen wird (und daher Veränderungen einführen wird), muss dies auf eine Weise geschehen, die mit den allgemeinen Sicherheits-, Risiko- und Architekturansätzen der Organisation im Einklang steht.

Diese Arten von eigenständigen Projekten können aus einer Vielzahl von Quellen initiiert werden. Zum Beispiel können sie von Anwendungsteams mit einem spezifischen Zugriffsbedarf angetrieben werden. In dieser Situation kann das Sicherheitsteam den Anwendungseigentümern helfen zu verstehen, warum Zero Trust der beste Ansatz ist. Tatsächlich ist es eine ausgezeichnete Möglichkeit, mit Zero Trust zu beginnen, eine Geschäfts- oder Anwendungsgruppe als Sponsor zu haben, da sie das Projekt unterstützen und dabei helfen können, politische oder technische Barrieren zu überwinden, die Sie möglicherweise treffen.

In vielen Fällen wird jedoch das Sicherheitsteam selbst dasjenige sein, das ein erstes Zero Trust-Projekt vorantreibt, um ein spezifisches Sicherheits- oder Risikoproblem zu lösen, mit dem Ziel, dies zu nutzen, um ihre Zero Trust-Reise zu beginnen. Diese Projekte können definitiv erfolgreich sein, laufen aber Gefahr, als „Lösung auf der Suche nach einem Problem“ zu erscheinen und können auf Widerstand von Netzwerk- oder Geschäftsteams stoßen, die den Wert einer Veränderung nicht sehen. Ignorieren Sie dieses Risiko nicht oder hoffen Sie einfach, dass Sie nicht darauf stoßen – dies kann ein echtes und bedeutendes Hindernis sein, da die meisten Zero Trust-Implementierungen Änderungen an IT-Elementen außerhalb des Bereichs des Sicherheitsteams erfordern, wie z. B. Benutzererfahrung oder Netzwerkkonfiguration. Der Schlüssel hier ist, ein Pilotprojekt für Zero Trust zu identifizieren, das einige aktuelle Schmerzpunkte löst, idealerweise, die ein Kopfschmerz für Teams über die Sicherheit hinaus sind, und die ihr Interesse und ihre Unterstützung für das Projekt wecken werden. Überprüfen Sie die sechs fokussierten Anwendungsfälle aus Kap. 18 – diese könnten gute Kandidaten für erste Projekte sein. Halten Sie auch Ihre Ohren offen für neue Geschäftsinitiativen, die in Ihrer Organisation im Gange sind; wenn Zero Trust sie einfacher und sicherer ermöglichen kann, könnten diese auch passen.

Bedenken Sie auch, dass strategische Zero Trust-Initiativen irgendwo beginnen müssen und selbst in diesem Kontext empfehlen wir, mit einem kleineren und fokussierteren Projekt zu beginnen, aus verschiedenen Gründen. Es gibt Ihnen ein Fahrzeug, mit dem Sie Anbieter- oder Plattformforschung durchführen und einen kleineren Proof of Concept (POC) durchführen können. Es gibt Ihnen auch die Chance, Dinge auszuprobieren, Fehler zu machen und aus ihnen in einer Situation mit geringeren Einsätzen zu lernen. Zero Trust ist eine Reise und da die IT- und Sicherheitslandschaft jedes Unternehmens einzigartig ist, wird auch die Reise jedes Unternehmens einzigartig sein. Umarmen Sie dies und lernen Sie, indem Sie iterativ vorgehen. Es wird viele Unbekannte geben, wenn Sie beginnen, und Sie werden nicht alles beim ersten Versuch richtig machen. Das Wichtigste ist, zumindest teilweisen Erfolg zu zeigen und Unterstützung für Zero Trust innerhalb Ihrer Organisation aufzubauen.

Mindestens müssen selbst die taktischsten Zero Trust-Projektteams Personen aus dem Bereich Identitätsmanagement und Netzwerk einbeziehen und Personen einbeziehen, die für die Unternehmensarchitektur verantwortlich sind. Unser nächster Abschnitt, in dem wir ein Beispiel für ein Bottom-Up-Projekt vorstellen, sollte dies verdeutlichen.

Beispielhafte Zero Trust-Implementierungen

Das Ziel dieses Abschnitts ist es, zwei beispielhafte Zero Trust-Implementierungen aus der Perspektive von Projekt und Meilenstein zu zeigen. Diese sollten Ihnen eine Vorstellung davon geben, wie und warum diese beiden fiktiven Projektteams sich für einen Ansatz entschieden haben. Bedenken Sie, dass dies nur repräsentative Beispiele sind und dazu dienen sollen, Ihnen bei der Entscheidungsfindung für Ihre realen Projekte zu helfen.

Szenario 1: Ein taktisches Zero Trust-Projekt

In unserem ersten Szenario hat diese Organisation für Transportdienstleistungen den Betrieb ihrer Finanzmanagementsysteme an einen Dritten ausgelagert, der ihnen diesen kritischen Geschäftsdienst über einen Pool von etwa 30 Teilzeit-Finanzanalysten bietet. Obwohl die Benutzer des Drittanbieters remote sind (und tatsächlich in zwei verschiedenen Ländern ansässig sind), bleiben die Finanzsysteme der Organisation am Hauptsitz untergebracht, auf traditionellen hardwarebasierten Servern bereitgestellt. Diese Architektur ist notwendig, da die Finanzsysteme mit vielen anderen On-Premises-Systemen integriert sind, die für den Geschäftsbetrieb unerlässlich sind.

Derzeit greifen die Benutzer des Drittanbieters über ein traditionelles VPN auf das Finanzsystem zu, aber aufgrund eines Wechsels der IT-Auditoren hat die Organisation nun mehrere Sicherheitsfeststellungen, die sie beheben müssen. Insbesondere müssen sie nun MFA für Benutzer von Drittanbietern durchsetzen und müssen auch an die Identitätslebenszyklusereignisse dieser Organisationen anknüpfen, um sicherzustellen, dass der Zugriff deaktivierter Benutzer ordnungsgemäß deaktiviert wird.

Während das Sicherheitsteam diese Probleme durch Anwendung einer eigenständigen MFA-Lösung lösen und einen Geschäftsprozess zur Sicherstellung der Benutzerabmeldung einrichten könnte, haben sie über Zero Trust geforscht und gelernt und sind begeistert, ein fokussiertes Anfangsprojekt gefunden zu haben. Eine Übersicht über den Projektzeitplan und -ablauf ist in Abb. 19-1 dargestellt, wobei die Schritte zwischen denen des Projektteams und denen, die das Unternehmensarchitekturteam betreffen, getrennt sind. Beachten Sie, dass in diesem Beispiel die Benutzer des Drittanbieters bereits Zugriff über die VPN-Lösung haben und die Prüfer keine

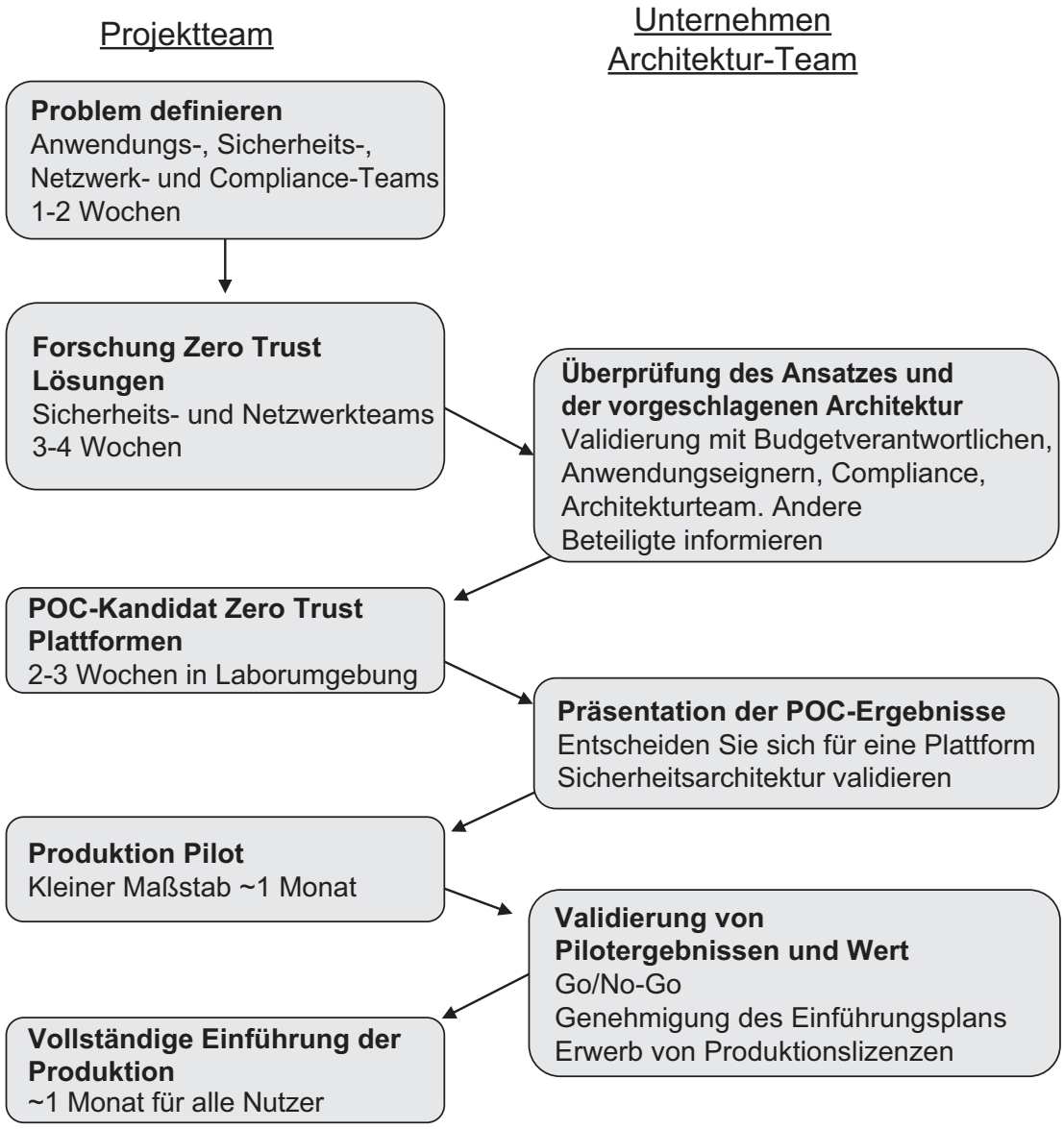

Abb. 19-1. *Beispiel Zeitplan für taktisches Zero Trust-Projekt*

Änderungen für 6 Monate verlangen, sodass es keinen hohen Druck oder Dringlichkeit für eine sofortige Änderung gibt. Dies kommt dem Projektteam zugute, da sie bei der Erforschung und Bewertung von Zero Trust-Plattformen überlegter vorgehen können. Mit all diesem Kontext betrachten wir nun jeden Schritt des Projekts im Einzelnen.

Problem definieren

Während die Prüfer nur MFA und Zombie-Konten als zu lösende Probleme identifizierten, möchte das Sicherheitsteam auch zusätzliche Sicherheitskontrollen durchsetzen, wie z. B. grundlegende Gerätehaltungsprüfungen, Geolokalisierungsprüfungen und sicherstellen, dass der Benutzer in der richtigen Verzeichnisgruppe im IAM-System des Drittanbieters ist. Das Sicherheitsteam, das dies leitet, benötigt ein paar Wochen Kalenderzeit, um die Anwendungs-, Netzwerk- und Compliance-Teams über den beabsichtigten Umfang und die Zero Trust-Prinzipien und -Ziele aufzuklären.

Zero Trust-Lösungen erforschen

Nachdem sie die Zustimmung der Stakeholder im vorherigen Schritt erhalten haben, nimmt das Sicherheitsteam einige Wochen Zeit, um Zero Trust-Plattformen zu erforschen und zu bewerten, und schaut sich eine Vielzahl von Angeboten von großen Anbietern, kleineren Anbietern und Open Source an. Die meisten Lösungen sind frei für Tests verfügbar, und technische Mitglieder des Sicherheitsteams nutzen ihre Freizeit, um in ein einzelnes Angebot einzutauchen und ihre Erkenntnisse zu teilen. Nach dieser ersten Phase entscheiden sie sich für zwei Kandidaten für Zero Trust-Plattformen und erstellen einen Entwurf für Sicherheits- und Bereitstellungsarchitektur.

Überprüfungsansatz und vorgeschlagene Architektur

Das Team stellt dann die vorgeschlagene Architektur und den Projektplan den relevanten Stakeholdern im Team für Unternehmensarchitektur vor, einschließlich dem Eigentümer der Finanzanwendung, Compliance, Netzwerk, Betrieb und dem Budgeteigentümer. Diese Organisation hat ein halbformelles Team für Unternehmensarchitektur, aber das Sicherheitsteam nimmt für dieses Projekt bewusst einen strukturierteren Ansatz, da sie beabsichtigen, den Umfang und die Reife ihrer Zero Trust-Initiative im Laufe der Zeit zu erweitern.

POC Zwei Kandidaten für Zero Trust-Plattformen

Sobald das Team für Unternehmensarchitektur den Ansatz genehmigt hat, bringt das Sicherheitsteam ihre beiden Kandidaten für Zero Trust-Plattformen ein und führt einen Proof of Concept in ihrer Nicht-Produktions-Lab-Umgebung durch. Dies ermöglicht es ihnen, diese Lösungen auf quantifizierbare Weise gegen die definierten Kriterien zu bewerten. Da dies ein gut abgegrenztes und nicht zu komplexes Szenario ist, dauert es nur 2–3 Wochen Teilzeitaufwand, um dies abzuschließen und eine Plattform auszuwählen.

Präsentieren POC-Ergebnisse

Sobald dies abgeschlossen ist, versammelt das Sicherheitsteam das Team für Unternehmensarchitektur erneut, um ihre Ergebnisse zu präsentieren, die höher bewertete Lösung zu demonstrieren und eine Empfehlung über die gewählte Plattform und Sicherheitsarchitektur zu geben. Diese Präsentation behandelt Integrationen, Benutzererfahrung und betriebliche Auswirkungen sowie Kernsicherheitsfunktionen.

Produktionspilot

Alle Stakeholder im Team für Unternehmensarchitektur genehmigen den Plan, sodass das Sicherheitsteam eine Pilotinstanz der Zero Trust-Plattform bereitstellt. Sie nutzen diese Phase, um sich mit dem Identitätsmanagement-Team des Drittanbieters für die Integration abzustimmen und die Zero Trust- (und integrierte MFA-) Software für 10 Endbenutzer an den beiden Standorten auszurollen. Diese Benutzer behalten ihren bestehenden VPN-Zugang von ihren Geräten, sodass sie bei einem Problem mit dem Zero Trust-Ansatz sofort zurückwechseln können, ohne ihre Produktivität zu beeinträchtigen. Das Sicherheitsteam benötigt etwa 1,5 Wochen, um das neue System auszurollen, und lässt die Endbenutzer es weitere 2,5 Wochen in der Produktion laufen. Es gibt ein paar kleinere Probleme und einige Benutzerbildungsthemen, aber der Pilot ist weitgehend ein Erfolg.

Pilotergebnisse und Wert validieren

Da der Pilot ein Erfolg war, ist das abschließende formelle Treffen mit dem Team für Unternehmensarchitektur einfach zu haben. Das Sicherheitsteam präsentiert die Ergebnisse und gibt eine starke „Go"-Empfehlung, die genehmigt wird. Das Team genehmigt auch ihren Plan für die Ausrollung in die Produktion (und, sehr wichtig, die Abschaltung der aktuellen VPN-Lösung). Das Team kauft auch Produktionslizenzen von ihrem ausgewählten Anbieter.

Vollständige Produktionsausrollung

Das Sicherheitsteam setzt die Zero Trust-Lösung für die verbleibenden Drittanwender ein und schaltet ihre VPN-Zugangslösung ab. Außerdem nutzen sie diese Zeit, um den Produktionsbetrieb der Zero Trust-Lösung an ihr Netzwerkbetriebsteam zu übergeben. Dieses Team war während des gesamten Prozesses beteiligt, daher ist dies keine Überraschung. Schließlich, obwohl dies das erste Zero Trust-Projekt war, wird es nicht das letzte sein. Das Sicherheitsteam sorgt dafür, den Erfolg dieses Projekts und seine Behebung der offenen Audit-Probleme zu fördern, um Schwung und Unterstützung für zukünftige Projekte zu erzeugen, die auf ihrer Zero Trust-Plattform aufbauen.

Natürlich kann ein reales Projekt komplexer sein als dieses und kann viel mehr Interaktion zwischen den verschiedenen Teams beinhalten. Wir verwenden hier das *Team für Unternehmensarchitektur* ein wenig als Platzhalter; Ihre Organisation könnte ein Team mit einem anderen Namen haben, das eine ähnliche Funktion ausführt. Und beachten Sie auch, dass verschiedene Organisationen die Dinge unterschiedlich angehen. Zum Beispiel könnte in einigen Organisationen das Team für Unternehmensarchitektur nur treffen, um vom Sicherheits-Team informiert zu werden, während sie in anderen Entscheidungsbefugnisse haben (und daher ein Veto-Recht über das Projekt).

Betrachten wir nun ein ganz anderes Szenario, das Zero Trust aus einer strategischen Perspektive angeht.

Szenario 2: Eine strategische Zero Trust Initiative

Dieses Szenario beginnt mit einem glücklichen Zufall. Das Sicherheitsteam dieses Pharmaunternehmens hatte kürzlich einen Junior-Sicherheitsingenieur eingestellt, und eine ihrer ersten Aufgaben bestand darin, die großen Mengen an lauten und unordentlichen Ereignisprotokollen, die von ihren Tausenden von Windows-Geräten ausgingen, zu konsolidieren, abzugleichen, zu normalisieren und insgesamt einfach zu versuchen, dem SOC zu helfen, diese zu verstehen. Dies ist genau die Art von undankbarer Arbeit, die oft aufgrund dringenderer Aufgaben verschoben wird. In diesem Fall entdeckte der Ingenieur einige intermittierende anomale Aktivitäten und meldete dies als „Hey, kann mir jemand helfen zu verstehen, was hier vor sich geht? Das sieht für mich nicht richtig aus." Es stellte sich heraus, dass Malware in ihrem Netzwerk vorhanden war, die anscheinend eine langsame und unauffällige Aufklärung durchführte. Sie holten schnell ein externes Incident Response Team, das erfolgreich Abhilfe schaffte.

Während der nachträglichen Analyse wurde der Organisation klar, wie glücklich sie gewesen war. Der ursprüngliche Zugangspunkt der Malware zum Netzwerk wurde nie vollständig ermittelt, obwohl sie vermuteten, dass er möglicherweise über eine gezielte Phishing-E-Mail erfolgt sein könnte. Sie kamen jedoch zu dem Schluss, dass sie von einem entfernten Befehls- und Kontrollserver gesteuert wurde und sich methodisch über ihr flaches Netzwerk ausgebreitet hatte, und zwar durch eine Kombination aus ungepatchten Windows-Maschinen und schlechten Admin-Passwortpraktiken. Der Hauptbefund des IR-Teamberichts war, dass sie den Angreifer anscheinend früh genug entdeckt hatten, um eine Datenexfiltration zu verhindern, aber wenn es sich um einen Ransomware-Angriff gehandelt hätte, wäre der Großteil ihres Netzwerks innerhalb weniger Stunden ausgefallen.

Die strategische Auswirkung dieses „Beinahe-Unfalls" war schnell und entscheidend – als Pharmaunternehmen basiert ihr gesamtes Unternehmen auf der Vertraulichkeit, Integrität und Verfügbarkeit ihrer Forschungsdaten und Fertigungssysteme. Die Geschäftsleitung Team und der Aufsichtsrat forderten zu Recht, dass diese Schwachstellen behoben werden, und der CEO ermächtigte den CISO, Änderungen vorzunehmen. Der CISO, dessen Sicherheitsführungsteam Zero Trust diskutiert und bewertet hatte, stellte einen strategischen Plan zur Einführung auf, in zwei breiten Phasen.

Phase 1 sollte die wertvollsten Vermögenswerte der Organisation besser absichern, indem sie den Zero Trust-Zugang von Endbenutzern, Entwicklern und Systemadministratoren durchsetzte. Zu den durchzusetzenden neuen Kontrollen gehörten die weit verbreitete Nutzung von MFA, gründliche Geräteposture-Checks, bessere Netzwerksegmentierung und die Beseitigung von umfassendem Admin-Netzwerkzugang. Phase 2 war geplant, um das Netzwerk weiter zu segmentieren, alle Benutzer „off net“ zu versetzen mit einem Zero Trust Café-Stil Netzwerk. Sie beinhaltete auch eine Migration weg von ihrem komplexen Set von On-Premises-Verzeichnissen und hin zu cloudbasiertem Identity-as-a-Service, mit moderner und passwortloser Authentifizierung. Schließlich war diese Phase geplant, um die Nutzung von cloudbasierten IaaS- und PaaS-Plattformen durch die Organisation zu integrieren und zu erweitern, um eine schnellere und effektivere Zusammenarbeit mit Kunden und Partnern zu ermöglichen.

Natürlich wurde jede dieser Phasen in einzelne Projekte unterteilt, und die Organisation nutzte die fünf Werttreiber, um jedes Projekt zu planen. Das erste Projekt auf dieser Reise konzentrierte sich auf die Behebung der dringendsten Sicherheitsschwächen, die im Vorfall identifiziert wurden, und wird in Abb. 19-2 dargestellt, wobei die beabsichtigte Auswirkung jedes Treibers auf einer Skala von 0 (niedrig) bis 10 (hoch) eingestuft wird.

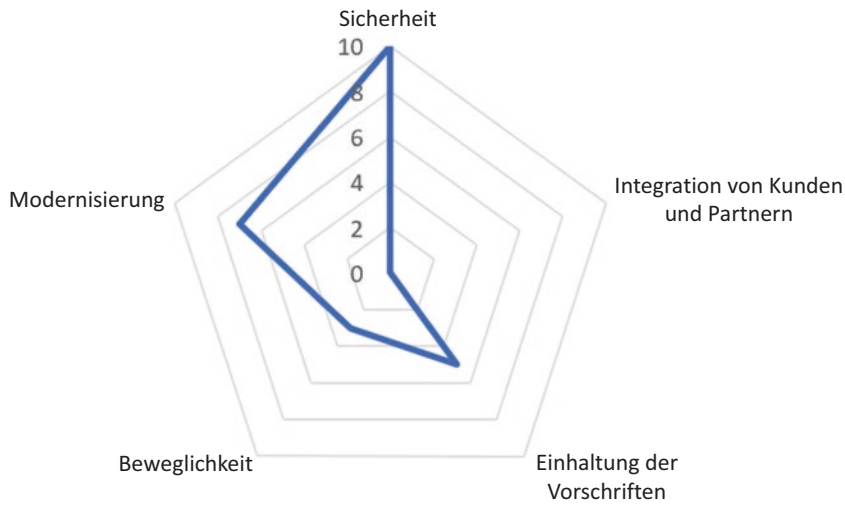

Abb. 19-2. *Zero Trust Projekt Wert – Radar Diagramm*

Insbesondere konzentrierte sich dieses erste Projekt auf die Verbesserung der Endbenutzersicherheit für den Zugang zu den kritischsten Produktionssystemen der Organisation. Der erste Satz von Zero Trust-Richtlinien erforderte MFA und validierte Gerätezertifikat- und Posture-Checks, bevor Benutzern Zugang gewährt wurde. Sie wendeten diese Kontrollen einheitlich an, unabhängig davon, ob das Gerät des Benutzers direkt mit dem Unternehmensnetzwerk verbunden war oder remote – schließlich lief die Malware, die dieses Projekt initiierte, lokal im Netzwerk.

Durch Design – um dieses erste Zero Trust-Projekt fokussiert zu halten – gab es weniger Auswirkungen auf die anderen Werttreiber. Dieses Projekt befasste sich mit einer Reihe offener Sicherheitskonformitätsprüfungen. Aber es gab keine Änderungen an Kunden- oder Partnerintegrationen, und es verbesserte die Agilität nur geringfügig, indem es mehrere isolierte Zugriffskontrollsysteme beseitigte. Das Team bewertete dieses Projekt jedoch als erhebliche Modernisierung ihrer Sicherheitsinfrastruktur, da es ihre erste produktive Zero Trust-Implementierung darstellte.

In Verbindung mit dem ersten Projekt arbeiteten der CISO und der CIO zusammen, um formalere Strukturen und Prozesse um ihre bestehenden Architektur- und Change Management Boards zu etablieren, um sicherzustellen, dass es ausreichende Kommunikation und Zusammenarbeit zwischen den Teams gab. Sie entschieden sich gegen die Einrichtung eines formalen Governance Boards, da das Architektur Board bereits Risiko und Compliance als Teil ihres Entscheidungsprozesses einbezogen hatte. Der CISO entschied sich jedoch, einen erfahrenen externen Berater zum Team hinzuzufügen, um Objektivität zu gewährleisten und ihre Perspektive zu erweitern.

Insgesamt illustriert dieses Beispiel, wie eine Organisation den ersten Teil einer strategischen Zero Trust-Initiative umsetzen könnte, gegeben einen starken Katalysator und begeisterte Unterstützung des CEO. Natürlich wird nicht jede Initiative so viel „Saft“ haben, um Budget freizusetzen, Barrieren abzubauen und (falls notwendig) Köpfe zu stoßen. Unser nächster Abschnitt behandelt einige häufige Hindernisse, die Sicherheitsleiter während ihrer Zero Trust Reisen begegnen können.

Häufige Hindernisse

Dieses Kapitel wäre nicht vollständig ohne eine Diskussion über reale Herausforderungen, die wir bei Zero Trust-Projekten und -Initiativen gesehen haben. Enterprise IT und Sicherheit sind hart und komplex, und einige Zero Trust-Projekte

werden scheitern. Das ist bedauerlich, aber wahr. Die gute Nachricht ist, dass die meisten ein Erfolg sein werden, und die Anleitung und Empfehlung, die wir in diesem Buch gegeben haben, sollten Sie auf einen Weg zum Erfolg führen. Und denken Sie daran, dass es *immer* technische Pannen und einige Mängel oder raue Teile in jedem komplexen System geben wird, Zero Trust eingeschlossen. Perfektion ist ein unerreichbares Ziel, aber dramatische Verbesserungen in Sicherheit und Effizienz sind erreichbar und realistisch. Mit diesem im Hinterkopf, schauen wir uns häufig auftretende Hindernisse an und Wege, sie zu vermeiden oder zu überwinden.

Unreife des Identitätsmanagements

Zero Trust ist eng mit dem Identitätsmanagement verbunden, und Zero Trust-Projekte laufen Gefahr, durch einen wahrgenommenen oder tatsächlichen Mangel an IAM-Reife verzögert zu werden. Diese Unreife kann sich auf verschiedene Weisen manifestieren, wie zum Beispiel die allzu häufige Anekdote „unser Verzeichnis ist ein Durcheinander", die Verbreitung von Gruppen (manchmal Zehntausende) oder ein laufendes Projekt zur Konsolidierung oder Abstimmung von Identitätsanbietern. Dies ist die Realität für viele IAM-Teams, sollte aber dennoch kein Hindernis für die Einführung von Zero Trust sein.

Zero Trust-Systeme nutzen einen Identitätsanbieter zur Benutzerauthentifizierung, und Sie können entscheiden, in welchem Maße Sie IAM-Attribute und -Gruppen in Ihren Zero Trust-Richtlinien verwenden möchten. Beachten Sie, dass Zero Trust-Systeme durch die Automatisierung der Nutzung dieser Identitätsattribute tatsächlich ein Katalysator für eine verbesserte Reife und Datenintegrität in Ihrem IAM-System sein können, selbst wenn es nur um einen engen Bereich geht. Denken Sie daran, dass wir dies bereits im Kap. 5 Abschnitt „Zero Trust als Katalysator für die Verbesserung von IAM" diskutiert haben.

Politische Widerstände

Leider werden Sicherheitsverantwortliche in einigen Organisationen auf politisch motivierten Widerstand gegen Veränderungen stoßen. Wir definieren dies als Personen, die Barrieren gegen Veränderungen aufbauen, trotz der klaren Vorteile für die Organisation. Dies kann durch Kultur, technische Vorurteile oder eine emotionale Bindung an aktuelle Sicherheitswerkzeuge oder -architekturen getrieben sein. Es gibt

mehrere Möglichkeiten, dem entgegenzuwirken. Zuerst und vor allem steht die Bildung. Einige Menschen leisten möglicherweise aus Unwissenheit Widerstand, daher sollten Sie daran arbeiten, sie über die konkreten Vorteile von Zero Trust aufzuklären und sie davon zu überzeugen, dass es sich nicht nur um ein Marketing-Schlagwort handelt. Zweitens, wenn Ihr Programm einen starken und energischen Executive Sponsor hat, sollte er in der Lage sein, diese Barriere zu überwinden. Drittens können Sie auch einen Befürworter für Ihr Projekt aus der Geschäftslinie aufbauen – Projekte, die zu erhöhten Einnahmen oder niedrigeren Kosten führen, sind besonders wirksam beim Abbau von Barrieren. Schließlich können Sie manchmal jemanden innerhalb der gegnerischen Organisation finden, der bereit ist, mit Ihnen zusammenzuarbeiten. Da Zero Trust-Systeme von Natur aus integrierbar sind, gibt es möglicherweise einige kreative Möglichkeiten, sich in die bestehende Infrastruktur einzubinden und diese zu erweitern, um die Wahrnehmung zu vermeiden, dass Sie ihre Umgebung „ausreißen und ersetzen“ werden.

Regulatorische oder Compliance Einschränkungen

Viele Unternehmen sind reguliert oder haben zumindest einige Datensätze oder Systeme, die regulatorischen Compliance-Anforderungen unterliegen. Typischerweise hinken staatliche und industrielle Vorschriften der Technologie um einige Jahre hinterher und können es Organisationen erschweren, neuere Ansätze zur Erfüllung dieser Anforderungen zu übernehmen. In vielen Fällen wird Ihr externer Drittanbieter/Auditor der entscheidende Faktor sein, daher ist es wichtig, proaktiv mit ihnen zusammenzuarbeiten. Zögern Sie nicht, frühzeitig in Ihrem Zero Trust-Projekt mit ihnen zusammenzuarbeiten und mit ihnen zusammenzuarbeiten und sie zu schulen, um sicherzustellen, dass sie Ihren Kurs verstehen. Dies wird dazu beitragen, ein positives Ergebnis sicherzustellen.

Entdeckung und Sichtbarkeit von Ressourcen

Ein genaues Bild aller Ressourcen in einer komplexen Unternehmens-IT-Umgebung zu erhalten, kann definitiv eine Herausforderung sein. Dies kann insbesondere für Umgebungen gelten, die ohne große Aufsicht gewachsen sind oder sich schnell

bewegen. Dies wird oft durch anekdotische Kommentare wie „Ich weiß nicht, wer auf was zugreift, wie kann ich sie kontrollieren?“ ausgedrückt.

Die Fallstudien aus Kap. 4 illustrieren zwei verschiedene Ansätze. Sowohl BeyondCorp als auch PagerDuty haben ihre Zero Trust-Plattformen breitflächig über komplexe Produktionsnetzwerke eingesetzt und feingranulare Zugriffskontrollrichtlinien definiert. Sie gingen einen beobachtenden Ansatz an, sammelten und analysierten Netzwerkdaten, um sicherzustellen, dass ihr System die Benutzerproduktivität nicht unterbrechen würde. Dies war effektiv, erforderte aber Zeit und Mühe. Im Gegensatz dazu nahm die Fallstudie zum Software-Defined Perimeter einen inkrementellen Ansatz an, indem sie Benutzer und Gruppen schrittweise integrierte. Sie begannen auch mit einigen gröberen Zugriffskontrollen und verschärften diese im Laufe der Zeit schrittweise.

Beide Ansätze sind gültig. Es ist wichtig zu erkennen, dass *Sie* entscheiden, wo und wie Sie Ihre Zero Trust-Plattform einsetzen und wie feingranular die Zugriffskontrollen sind. Fallen Sie also nicht in die Falle zu glauben, dass Sie eine perfekte Sichtbarkeit jeder Verbindung und jedes Datenflusses benötigen, bevor Sie beginnen können. Arbeiten Sie mit den Informationen, die Sie haben, oder verwenden Sie eines der vielen Open-Source- oder kommerziellen Tools zur Netzwerkentdeckung und Ressourcensichtbarkeit.

Analyseparalyse

Das Ziel, jede neue Technologie oder Herangehensweise vollständig zu verstehen, Risiken zu identifizieren und abzustecken, ist lobenswert, hat aber den allzu häufigen Nachteil, dass jede Entscheidung oder Aktion auf unbestimmte Zeit verzögert wird. Diese „Paralyse durch Analyse“ ist für alle Beteiligten frustrierend. Sie kann kulturell innerhalb einer Organisation sein, oder sie kann von einem Sicherheitsteam, das versucht, Veränderungen durch Konsens herbeizuführen, etwas selbst auferlegt sein, was nie ein leichter Spagat ist.

Wir haben gesehen, wie Organisationen damit zu kämpfen haben, wenn sie sich auf eine strategische Zero Trust-Reise begeben, und ihre Projekte sich über mehrere Jahre erstrecken, ohne dass mehr als ein paar Dutzend Benutzer in Produktion gehen. Dies ist im Nachhinein (und abstrakt) leicht zu erkennen, aber oft schwer im Moment zu

erkennen. Dies liegt daran, dass die meisten von uns und die meisten Teams eine ordnungsgemäße, gründliche Planung, Recherche und Validierung durchführen wollen.

Diese Art von Paralyse kann auftreten, wenn Organisationen auf einer strategischen Zero Trust-Reise voranschreiten und die Zustimmung einer Vielzahl von Stakeholdern einholen müssen, bevor sie etwas in Produktion bringen können. Dies kann problematisch sein. Dies gilt insbesondere, wenn diese anderen Teams verlangen, dass die neuen Systeme das gleiche Maß an betrieblicher Reife, Automatisierung und Integration erfüllen wie andere Systeme, die seit Jahren in Produktion sind. Dies kann zu einem „Henne-Ei-Problem" führen, insbesondere wenn das Projekt und die Architektur so gestaltet sind, dass die Organisation eine große und komplexe Infrastruktur bereitstellen muss, bevor sogar die erste Gruppe von Produktionsbenutzern eingesetzt werden kann.

Wir plädieren nicht dafür, dass Projektteams oder Sicherheitsarchitekten Abkürzungen nehmen oder eine ordnungsgemäße Recherche und Validierung vermeiden – ganz im Gegenteil. Aber wir plädieren dafür, dass Teams mit allen relevanten Stakeholdern zusammenarbeiten und ihre Initiative aus der Perspektive angehen, wie sie Zero Trust so schnell wie möglich in die Pilot- oder Produktionsphase bringen können, auch wenn es zunächst begrenzt ist. Während Betriebsteams verständlicherweise rigoros und konservativ gegenüber Veränderungen sind, werden die meisten bereit sein, mit Ihnen zusammenzuarbeiten. Zum Beispiel können Sie vorschlagen, den Zero Trust-Zugriff parallel zu bestehenden Zugriffsmethoden laufen zu lassen, bis das Team ein hohes Maß an Vertrauen in das neue System hat. Erst dann würden Sie die ältere Zugriffsmethode stilllegen.

Zum Abschluss dieses Abschnitts über häufige Hindernisse wollen wir definitiv nicht auf einer negativen Note enden. Wie alle IT- und Sicherheitsprojekte in Unternehmen beinhalten auch Zero Trust-Projekte ein gewisses Maß an Risiko und Unbekannten. Aber die überwiegende Mehrheit der gut geführten Projekte ist erfolgreich und liefert Wert für die Organisation, auch wenn sie auf ein paar Stolpersteine stoßen. Aus unserer Sicht ist das Wichtigste, zu iterieren, zu lernen und keine Angst davor zu haben, Änderungen an Ihrer laufenden Zero Trust-Architektur vorzunehmen. Stellen Sie sicher, dass jedes Zero Trust-Projekt in konsumierbare, erreichbare Meilensteine unterteilt ist. Zu Beginn Ihrer Reise werden Sie nie alle Antworten kennen, aber machen Sie genug Hausaufgaben, damit Sie einige der Antworten und die meisten Fragen kennen. Haben Sie Vertrauen in sich selbst und Ihr Team – Sie werden unterwegs das finden, was Sie brauchen Weg.

Zusammenfassung

In diesem Kapitel haben wir die Top-Down- und Bottom-Up-Ansätze für Zero Trust beschrieben. In der Praxis werden die meisten Organisationen Elemente von jedem in einem gemischten Ansatz verwenden. Wir glauben, dass in allen Fällen die Identifizierung eines guten ersten Kandidatenprojekts der Schlüssel zum Erfolg ist. Schauen Sie sich die sechs fokussierten Anwendungsfälle aus Kap. 18 an, um Ideen zu bekommen, wo Sie anfangen können. Und bauen Sie Verbindungen zu Ihren Kollegen in Ihrer gesamten Organisation auf – beginnen Sie, die Ideen hinter Zero Trust und die Vorteile, die es bieten kann, zu verbreiten und stellen Sie viele Fragen. Gibt es Bereiche, in denen die Organisation derzeit operative, sicherheitsrelevante, effizienz- oder benutzererfahrungsbedingte Kopfschmerzen hat? Gibt es irgendwelche Prüfungsergebnisse, die angegangen werden müssen? Was ist mit Projekten, die neue Umgebungen wie IaaS oder PaaS nutzen? Gibt es Probleme, die ein geringes Risiko, aber eine hohe Rendite haben?

Überlegen Sie auch, ob Sie möchten, dass Ihr erstes Projekt eine hohe oder niedrige Sichtbarkeit hat. Es gibt keine falsche Antwort! Ein Projekt mit geringerer Sichtbarkeit gibt Ihnen die Möglichkeit, Fehler zu machen (und daraus zu lernen) mit weniger Konsequenzen, obwohl der Nachteil sein könnte, dass Sie härter um Ressourcen kämpfen müssen. Ein Projekt mit höherer Sichtbarkeit kann diese Barrieren abbauen, kann aber die Kontrolle erhöhen und eine geringere Toleranz für Fehler haben.

Unsere Perspektive ist, dass das beste Anzeichen für den Erfolg des ersten Zero Trust-Projekts ist, dass Sie sofort begeisterte Unterstützung für die Projekte 2 und 3 erhalten. Seien Sie auf die Arten von qualitativen und quantitativen Messungen, die Ihre Organisation wichtig findet, abgestimmt und bereiten Sie sich darauf vor, sie zu erfassen und zu präsentieren, um den erzielten Wert zu demonstrieren. Und bauen Sie Brücken zu Ihren Kollegen in der gesamten Organisation. Sowohl strategische als auch taktische Zero Trust-Projekte beinhalten Veränderungen im gesamten Unternehmen, und dies kann ohne Unterstützung schwer zu erreichen sein. Zero Trust-Projekte können eine Herausforderung sein, aber die Ergebnisse sind die Anstrengung wert.

KAPITEL 20

Schlussfolgerung

Obwohl wir das Ende dieses Buches erreicht haben, stehen Sie wahrscheinlich noch am Anfang Ihrer Zero Trust-Reise. Wir haben eine Menge Material behandelt, das konzeptionelle, technische, strategische und organisatorische Themen umfasst, und dennoch, trotz der Breite der Themen, erkennen wir an, dass wir nicht alles abdecken konnten. Zero Trust ist sehr breit gefächert – im Grunde so breit wie die Unternehmens-IT – und entwickelt sich schnell. Neue Technologien, Plattformen und Lösungen entstehen scheinbar jeden Tag. Ganz zu schweigen davon, dass jedes Unternehmen IT- und Sicherheitskomponenten in einzigartigen Kombinationen zusammengestellt hat, um ihren spezifischen Bedürfnissen gerecht zu werden. Daher sind wir zuversichtlich, dass es in diesem Bereich noch viel zukünftige Arbeit gibt. (Tatsächlich haben wir eine Begleitwebsite unter `https://ZeroTrustSecurity.guide` erstellt, auf der wir Inhalte hosten, die das Buch ergänzen und uns den Dialog fortsetzen lassen).

Angesichts der sich ständig ändernden Natur dieses Bereichs haben wir in diesem Buch versucht, mehr als nur Wissen zu vermitteln, sondern auch die Weisheit, zu wissen, wo Grenzen zu ziehen sind. Es ist weder möglich noch angemessen, Ihr Zero Trust-System in jeden Teil Ihrer Umgebung zu zwingen. Tatsächlich wird das bewusste Ausschließen bestimmter Komponenten Ihrer IT-Infrastruktur Ihnen helfen, sich zu konzentrieren, schneller voranzukommen und erfolgreich zu sein. Sie sind die beste Person, um sicherzustellen, dass Sie die geeignetste und effektivste Sicherheitsplattform, Tools und Prozesse für jeden Teil Ihres IT- und Sicherheitsökosystems auswählen.

Wenn Sie diesen Prozess durchlaufen, denken Sie an unsere Definition von Zero Trust, die wir in Kap. 2 vorgestellt haben:

> *Ein Zero Trust-System ist eine integrierte Sicherheitsplattform, die kontextbezogene Informationen aus Identität, Sicherheit und IT-Infrastruktur sowie Risiko- und Analysetools verwendet, um die dynamische Durchsetzung von Sicherheitsrichtlinien im*

J. Garbis und J. W. Chapman, *Zero Trust Sicherheit*, https://doi.org/10.1007/979-8-8688-0105-1_20

gesamten Unternehmen zu informieren und zu ermöglichen. Zero Trust verlagert die Sicherheit von einem ineffektiven, auf den Perimeter ausgerichteten Modell zu einem ressourcen- und identitätszentrierten Modell. Dadurch können Organisationen den Zugriffskontrollen kontinuierlich an eine sich ändernde Umgebung anpassen und verbesserte Sicherheit, reduziertes Risiko, vereinfachte und widerstandsfähige Operationen und erhöhte Geschäftsagilität erzielen.

Diese Definition sollte als Grundprinzipien für das gesamte Zero Trust-Programm Ihrer Organisation dienen und Ihre Entscheidungsfindung und Prioritäten während Ihrer Reise informieren.

Letztendlich ist Sicherheit für jede Organisation ein Mittel zum Zweck, eine Möglichkeit, den kreativen und engagierten Menschen in Ihrem Unternehmen zu ermöglichen, ihre Aufgaben zuverlässig, effizient und vertraulich zu erfüllen. Ein gut gestaltetes und gut eingesetztes Zero Trust-Sicherheitssystem wird transparent arbeiten, sich im Hintergrund halten, während es strikt Sicherheitskontrollen für Benutzer und Dienste durchsetzt, den Zugriff basierend auf dem Kontext automatisch anpasst und Benutzer nur bei Bedarf unterbricht. Sicherer und angemessener Zugang wird ein natürlicher Nebeneffekt von Prozessen und Aktionen sein, anstatt eine Auferlegung.

Hoffentlich haben wir Sie mit ausreichendem Wissen, Kontext, Fähigkeiten und Werkzeugen ausgestattet, so dass Sie gut vorbereitet sind, um selbstbewusst auf Ihre Zero Trust-Reise zu gehen. Wie mythische Abenteurer, die sich auf eine große Quest begeben, haben Sie jetzt Waffen, Zaubersprüche, Tränke und Vorräte. Stellen Sie Ihr Team zusammen, bilden Sie Allianzen und ziehen Sie aus, um Monster zu besiegen. Gott beschütze Sie.

KAPITEL 21

Nachwort

—Christopher Steffen, CISSP, CISA
Research Director, Information Security and Compliance,
Enterprise Management Associates

Wenn Sie es bis hierher geschafft haben, herzlichen Glückwunsch! Die fast 300 Seiten vor diesem haben sehr aufschlussreich gewesen und, ich hoffe, haben Ihnen einige Denkanstöße auf Ihrer Zero Trust-Reise gegeben.

Ich verwende den Begriff „Reise“ sehr spezifisch, denn die Implementierung von Zero Trust ist keine „einmalige“ Lösung. Selten (wenn überhaupt) werden Sie eine saubere Tafel/Grünfläche zur Implementierung haben. Es *ist* eine Reise, und eine, die sich sehr lohnen wird für Sie und Ihre Organisation. Die Sicherheitsvorteile für Ihre Organisation liegen auf der Hand, aber auch die einfache Verwaltung und Administration für das Betriebs- und Sicherheitspersonal sind ein großer Vorteil.

Wenn Sie das Wissen aus diesem Buch nehmen und sich auf Ihre Zero Trust-Reise vorbereiten, möchte ich mehrere Dinge mit Ihnen teilen, die meisten davon wurden bereits abgedeckt, also betrachten Sie dies als Zusammenfassung.

Planen, Planen, Dann Noch Mehr Planen

So viele Zero Trust-Implementierungen scheitern aufgrund unvollständiger Planung. Verstehen Sie, dass dies anders ist als ein Mangel an Planung, da die meisten Organisationen irgendeinen Spielplan für das Projekt haben. Dieses Buch bietet eine großartige Grundlage für das Verständnis von Zero Trust-Architekturen und -Implementierungen, und es gibt viele Ressourcen, die Ihnen helfen, darauf aufzubauen. Da Sie wahrscheinlich mit einigen Infrastruktur-/Sicherheitslösungen beginnen, untersuchen Sie, wie Sie diese auf der Grundlage der im gesamten Buch diskutierten Prinzipien weiterentwickeln können.

J. Garbis und J. W. Chapman, *Zero Trust Sicherheit*, https://doi.org/10.1007/979-8-8688-0105-1_21

Zero Trust Ist (Leider) Politisch

Aufgrund des Umfangs der meisten Zero Trust-Projekte hat es viele Stakeholder. Alle diese Stakeholder zu einer Einigung zu bringen, kann eine massive Herausforderung sein und das Projekt noch bevor es beginnt entgleisen lassen. Sie müssen Ihre besten politischen Manövrierfähigkeiten aufsetzen, um das Projekt abzuschließen, und die bereitwillige Unterstützung (sowie Finanzierung und Ressourcen) Ihrer Schlüsselstakeholder ist entscheidend für Ihren Erfolg. Die Unterstützung und Förderung der Geschäftsleitung setzt den Ton von oben und räumt viele Hindernisse aus dem Weg – aber unterschätzen Sie nicht die Unterstützung der Geschäftsbereiche. Ihre Empfehlungen auf ihrer spezifischen Leiter werden viel Gewicht haben.

Träumen Sie Groß, Starten Sie Klein

Zero Trust muss nicht auf einmal implementiert werden. Tatsächlich sollte es *nicht* so sein. Besser ist es, mit einer spezifischen Testgruppe und einem Team zu beginnen, die möglicherweise bereits Infrastruktur und Lösungen nutzen, die leicht verfügbar sind. Sobald Sie einen Proof of Concept und den Wert von Zero Trust etabliert haben, verringern sich die politischen Probleme und die Unterstützung nimmt zu.

Zeigen Sie Mir das Geld

Es sei denn, Sie sind der Sicherheits-/Netzwerkadministrator mit scheinbar unbegrenztem Budget und Ressourcen (was für ein Traum das wäre), besteht eine ziemlich gute Chance, dass Sie Ihr Zero Trust-Projekt über die Jahre und mit Hilfe planen müssen. Es gibt erhebliche Vorteile von Zero Trust (wieder, in diesem Buch skizziert) für viele Abteilungen Ihres Unternehmens, insbesondere Betrieb, DevOps und Compliance. Stellen Sie sicher, dass Sie Ihre Ziele mit ihren abstimmen, und vielleicht – nur vielleicht – können Sie einige der wertvollen Budget-Dollar von diesen Abteilungen bekommen.

Digitale Transformation Ist Ihr Freund

So viele Organisationen durchlaufen eine digitale Transformation, indem sie Richtlinien und Verfahren aktualisieren, um die neuesten Technologien, wie Cloud und Mikroservices, zu nutzen. Integrieren Sie Ihr Zero Trust-Framework als Teil des digitalen Transformationsprozesses für Ihre Organisation. Sie hätten die Sicherheitskontrollen für diese digitalen Transformationsprojekte sowieso aktualisieren müssen, also nutzen Sie die Gelegenheit, sie mit Ihrer Zero Trust-Vision abzustimmen.

Zero Trust ist nicht nur das Buzzword-Bingo-Zentralfeld: es ist die Art und Weise, wie wir in den nächsten zehn Jahren auf die Unternehmenssicherheit blicken werden. Sie haben die ersten Schritte auf Ihrer Zero Trust-Reise gemacht, und ich wünsche Ihnen nichts als Erfolg!

ANHANG A

Weiterführende Literatur: Eine kommentierte Liste

Industrienormen und Spezifikationen

Standards und Spezifikationen spielen eine unglaublich wichtige Rolle in unserer Branche; die Interoperabilität, die sie ermöglicht haben, hat enormen Wert geschaffen. Vielen Dank an alle, die dazu beigetragen haben.

OAuth2 – RFC 6749: Das OAuth2 Autorisierungs-Framework: https://tools.ietf.org/html/rfc6749

OAuth2 – RFC 6750: Das OAuth 2.0 Autorisierungsrahmenwerk: Bearer Token Nutzung https://tools.ietf.org/html/rfc6750

JSON Web Token (JWT) – RFC 7519: https://tools.ietf.org/html/rfc7519

JWT ist ein offenes Standard-Framework für die sichere Darstellung von Ansprüchen, die zwischen zwei Parteien übertragen werden sollen.

SCIM – RFC 7652: Das System für das Management von Identitäten über Domänengrenzen hinweg: https://tools.ietf.org/wg/scim/ und http://www.simplecloud.info/

LDAP: RFC 4150: LDAP-Übersicht (“Roadmap”) Spezifikation https://tools.ietf.org/html/rfc4510

HTOP: RFC 4226: HOTP: Ein HMAC-basierter Einmal-Passwort-Algorithmus https://tools.ietf.org/html/rfc4226

DNS über TLS: RFC 7858 https://tools.ietf.org/html/rfc7858

DNS über HTTPs: RFC 8484 https://tools.ietf.org/html/rfc8484

Diese beiden RFCs skizzieren die vorgeschlagenen Standards für zwei verschiedene Wege, um die Sicherheit von DNS-Anfragen zu verbessern:

J. Garbis und J. Chapman, *Zero Trust Sicherheit,* https://doi.org/10.1007/979-8-8688-0105-1

FIPS 199, Standards für die Sicherheitskategorisierung von Bundesinformationen und Informationssystemen, US National Institute of Standards and Technology, 2004 https://csrc.nist.gov/publications/detail/fips/199/final

Die Software-Defined Perimeter Spezifikation 1.0, Cloud Security Alliance, 2014 https://cloudsecurityalliance.org/artifacts/sdp-specification-v1-0/

Dies ist die anfängliche Definition der Software-Defined Perimeter-Architektur.

Leitfaden zur Software-Defined Perimeter Architektur, Cloud Security Alliance, 2019 https://cloudsecurityalliance.org/artifacts/sdp-architecture-guide-v2/

Dieses Dokument untersucht die SDP-Architektur genauer, einschließlich der Bereitstellungsmodelle.

Single-Packet Authorization (SPA): https://www.cipherdyne.org/blog/2012/09/single-packet-authorization-the-fwknop-approach.html

Dieses Dokument erklärt die Konzepte und bietet eine Open-Source-Implementierung der Single-Packet-Autorisierung.

Die FIDO Alliance: Bewegung der Welt jenseits von Passwörtern mit WebAuthn & CTAP: https://fidoalliance.org/ und https://fidoalliance.org/specifications/

Die CTAP-Standards definieren das Anwendungsschichtprotokoll für die Kommunikation zwischen Roaming- und Client-Anwendungen, einschließlich passwortloser Lösungen.

XACML: eXtensible Access Control Markup Language https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

NAC: Das Extensible Authentication Protocol (EAP): RFP 3748 https://tools.ietf.org/html/rfc3748 und 802.1x: https://1.ieee802.org/security/802-1x/

STIX: Der Structured Threat Intelligence eXchange und TAXII: der Trusted Automated eXchange of Intelligence Information: https://oasis-open.github.io/cti-documentation/

Bücwher

Zero Trust Networks von Evan Gilman und Doug Barth (O'Reilly, 2017)

Dieses Buch bietet eine ausgezeichnete Analyse und Grundlage für Zero Trust aus einer Netzwerkperspektive und untersucht die PagerDuty-Fallstudie eingehend.

Cyber Warfare – Wahrheit, Taktiken und Strategien von Dr. Chase Cunningham (Packt, 2020)

Dieses sehr lesbare Buch betrachtet die Informationssicherheit aus der Perspektive eines Kämpfers und webt die Treiber und Konzepte von Zero Trust ein.

Defensive Security Handbook: Best Practices für die Sicherung von Infrastrukturen von Lee Brotherston und Amanda Berlin (O'Reilly, 2017)

Dieses Buch dient als selbstbeschriebenes "Security 101 Handbuch," das darauf abzielt, Menschen dabei zu helfen, ein umfassendes Sicherheitsprogramm in ihrem Unternehmen zu erstellen (oder zu verstehen).

Forschungsdokumente und Publikationen

NIST Dokumente

NIST Sonderveröffentlichung 800.207 – Zero Trust Architektur, August 2020 https://csrc.nist.gov/publications/detail/sp/800-207/final

Wir empfehlen Ihnen dringend, dieses Dokument zu lesen, da es eine starke Ergänzung zu (und in vielerlei Hinsicht eine Grundlage für) unsere Arbeit in diesem Buch ist.

Dies ist NIST's assoziiertes Zero Trust Proof-of-Concept-Projekt: https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture

NIST-Sonderveröffentlichung 800-162: Leitfaden zur attributbasierten Zugriffskontrolle (ABAC) Definition und Überlegungen, 2014 https://csrc.nist.gov/publications/detail/sp/800-162/final

Google's BeyondCorp-Whitepapers

Verfügbar unter https://research.google/pubs/ (suchen Sie nach "BeyondCorp")

Überblick: https://security.googleblog.com/2019/06/how-google-adopted-beyondcorp.html

BeyondCorp: Ein neuer Ansatz für Unternehmenssicherheit, ;login: Dezember 2014, Vol. 39, Nr. 6.

BeyondCorp: Design bis zur Bereitstellung bei Google, :login; Frühling 2016 Vol. 41, Nr. 1

BeyondCorp: Der Zugangsproxy, ;login: Winter 2016, Vol. 41, Nr. 4

Migration zu BeyondCorp: Produktivität aufrechterhalten während der Verbesserung der Sicherheit, ;login: Sommer 2017, Vol. 42, Nr. 2

BeyondCorp: Die Benutzererfahrung: ;login: Herbst 2017, Vol. 42, Nr. 3

BeyondCorp: Aufbau einer gesunden Flotte, ;login: Herbst 2018, Vol. 43, Nr. 3

Andere Dokumente

IETF Auswirkungen von TLS 1.3 auf operative Netzwerksicherheitspraktiken: https://datatracker.ietf.org/doc/draft-ietf-opsec-ns-impact/

Dieses sehr lesbare Dokument leistet hervorragende Arbeit bei der Erklärung, wie die Umstellung auf TLS 1.3 verschiedene Anwendungsfälle für Netzwerksicherheit beeinflusst.

Das bedrohte Netz: Wie das Web zu einem gefährlichen Ort wurde. eBook vom *The Washington Post* Journalist Craig Timberg, 2015: http://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/

Keine Kauzigen Zentren mehr: Einführung des Zero Trust Modells der Informationssicherheit, Forrester Research, Inc. September 2010 https://www.forrester.com/report/No+More+Chewy+Centers+The+Zero+Trust+Model+Of+Information+Security/-/E-RES56682

Das Zero Trust eXtended Ökosystem: Daten, Forrester Research, Inc., August 2020 https://www.forrester.com/report/The+Zero+Trust+eXtended+Ecosystem+Data/-/E-RES161356

Für einige Gegenargumente zu verschlüsseltem DNS, die die Abwägungen untersuchen, siehe die Veröffentlichung vom Januar 2021 "Adopting Encrypted DNS in Enterprise Environments" von der National Security Agency, https://media.defense.gov/2021/Jan/14/2002564889/-1/-1/0/CSI_ADOPTING_ENCRYPTED_DNS_U_OO_102904_21.PDF sowie https://www.zdnet.com/article/dns-overhttps-causes-more-problems-than-it-solves-experts-say/

https://go.forrester.com/blogs/smackdown-enterprise-monitoring-vs-tls-1-3-and-dns-over-https/

Service Meshes

Istio Service Mesh: https://istio.io/

Linkerd Service Mesh: https://linkerd.io/