paloalto NETWORKS | CORTEX XPANSE BY PALO ALTO NETWORKS

ERKENNTNISSE ZUM ANGRIFFSFLÄCHENMANAGEMENT, DIE AUF BELEGBAREN DATEN UND NICHT NUR AUF UMFRAGEN UNTER BETROFFENEN BASIEREN

CORTEX XPANSE-BEDROHUNGSBERICHT 2022 ZUR ANGRIFFSFLÄCHE

AUSG. 2.1

Inhalt

Kurzfassung

Einleitung

Verbringen Sie aus Sorge vor der nächsten Zero-Day-Sicherheitslücke schlaflose Nächte? Oder haben Sie Albträume, dass ein Mitarbeiter ein neues Cloud-Asset außerhalb der Sicherheitsprozesse erstellt und dabei nicht einmal die einfachsten Einstellungen wie die RDP-Deaktivierung (Remote Desktop Protocol) bedacht hat?

Erfahrene Sicherheitsexperten wissen, dass bekannte Zero-Day-Sicherheitslücken zwar Schlagzeilen machen, die wahren Probleme jedoch von den zahlreichen Entscheidungen im Unternehmensalltag verursacht werden. Schon bei einem einzigen Fehler oder einer vergessenen Einstellung in den Sicherheitsprotokollen haben Angreifer leichtes Spiel. Cyberkriminelle können inzwischen relativ einfach und kostengünstig Sicherheitslücken, Schwachstellen oder sonstige unbekannte Zugangspunkte finden und dann den Weg des geringsten Widerstands für ihren Angriff auswählen.

Selbst technisch nicht sonderlich versierte Angreifer können einen oberflächlichen Scan im Internet durchführen, um anfällige Assets zu finden. Manche versuchen, die erkannten Schwachstellen auszunutzen. Geschäftstüchtige Cyberkriminelle hingegen verkaufen diese Daten im Dark Web an andere Hacker, die dann komplexere Angriffe ausführen. Für offengelegte RDP-Instanzen (Services, über die sich Beschäftigte per Remotezugriff auf einem Gerät anmelden) zahlen Hacker beispielsweise zwischen drei und zehn USD[1], um anschließend im Netzwerk der ahnungslosen Opfer Ransomware zu installieren.

Doch Angreifer sind nicht die einzigen, die das gesamte Internet nach Schwachstellen durchsuchen können – Cortex Xpanse kann das ebenfalls. Das Xpanse-Forschungsteam hat die über das Internet zugängliche Angriffsfläche einiger der größten Unternehmen der Welt untersucht, um sie bei ihren Sicherheitsbemühungen zu unterstützen.

Nachfolgend finden Sie die wichtigsten Erkenntnisse zum Zustand der globalen Angriffsfläche basierend auf den analysierten Scandaten und nicht nur Umfragen unter Betroffenen. Damit möchten wir Unternehmen helfen, kritische Schwachstellen zu beheben, bevor Angreifer sie ausnutzen können.

Wir haben die Scans von 50 Millionen IP-Adressen – und damit mehr als 1 Prozent des gesamten Internets – von über 100 weltweit agierenden Unternehmen untersucht und ermittelt, wie schnell Angreifer anfällige Systeme identifizieren können. Die Ergebnisse in Punkt 1 bis 5 basieren auf Daten, die zwischen März 2021 und September 2021 erfasst wurden. Für einen Teil von Punkt 5 und den gesamten Punkt 6 wurden Daten aus dem Zeitraum von Dezember 2021 bis Juni 2022 untersucht.

Das sind unsere wichtigsten Erkenntnisse:

- Die Cloud ist weiterhin ein beliebtes Angriffsziel.
- Viele Unternehmen machen es den Angreifern leicht.
- End-of-Life-Software bedeutet auch das Ende der Sicherheit.
- Die Probleme sind komplex und branchenspezifisch.
- In Angriffsflächen sammeln sich Probleme schnell an.
- RDP- und Cloud-Schwachstellen sind persistent.

Wichtige Erkenntnisse

Unseren Untersuchungen zufolge sind Cloud-Schwachstellen im Allgemeinen und auch öffentlich zugängliche RDP-Server weiterhin ein Problem. Bei der Suche nach den Gründen für die mangelnde Sicherheit haben wir zahlreiche Schwachstellen in Anmeldeseiten für Administratoren und nicht mehr unterstützter Software (End-of-Life, EOL) mit Internetschnittstellen gefunden.

Laut unseren Analysen lässt sich die Persistenz der Risiken und Schwachstellen auch darauf zurückführen, dass moderne Angriffsflächen dynamisch sind, das heißt, sie wachsen und verändern sich ständig. Ohne einen umfassenden Überblick und die richtigen Prozesse führt dies leider allzu häufig zu neuen Problemen, während die alten Fehler noch behoben werden.

1. Brian Krebs, „Hacked Via RDP: Really Dumb Passwords“, Krebs on Security, 13. Dezember 2013, https://krebsonsecurity.com/2013/12/hacked-via-rdp-really-dumb-passwords/.

Punkt 1: Die Cloud ist weiterhin ein beliebtes Angriffsziel

2021 kamen knapp 80 Prozent aller beobachteten Probleme in Cloud-Infrastrukturen vor. Bei den Daten, die zwischen Dezember 2021 und Juni 2022 erfasst wurden, waren es sogar 91 Prozent. Das ist keine große Überraschung, da durch die Pandemie die Cloud-Migration stark vorangetrieben wurde.

Dass deutlich mehr Probleme in der Cloud als in On-Premises-Umgebungen gefunden wurden, deutet darauf hin, dass die Bereitstellung wesentlich einfacher als der Schutz der Cloud-Infrastrukturen ist. Das kann verschiedene Gründe haben – von Cloud-Assets, die außerhalb der Sicherheitskontrollen erstellt werden, über unsichere Standardeinstellungen bis zur Vielzahl an Cloud-Assets, von denen unterbesetzte Sicherheitsteam einfach überfordert sind. Die Cloud ist eine moderne Angriffsfläche in einem Mikrokosmos: Sie verändert sich so schnell, dass herkömmliche Sicherheitslösungen oft nicht Schritt halten können.

Wir haben uns die Unterschiede zwischen Cloud- und On-Premises-Umgebungen in vier Kategorien genauer angesehen, die vor Kurzem ausgenutzt und in mehreren Sicherheitshinweisen von Behörden aufgeführt wurden (mehr dazu unter Punkt 5). Probleme mit unsicheren Apache Web Servern treten nahezu ausschließlich in der Cloud auf (97 Prozent). Gleiches gilt für die unsicheren Microsoft List-Server und Sicherheitslücken in F5 BIG-IP TMUI. Bei den unsicheren Microsoft Exchange-Servern ist es jedoch genau umgekehrt. Das könnte bedeuten, dass diese noch überwiegend in On-Premises-Umgebungen genutzt werden. Haben Unternehmen keinen umfassenden Überblick über ihre Bereitstellungen, können sie auch nur begrenzt auf neue CVE reagieren, die ihr Netzwerk bedrohen.

Die Tatsache, dass 91 Prozent der Probleme in der Cloud auftreten, ist auch für unsere weiteren Erkenntnisse relevant.

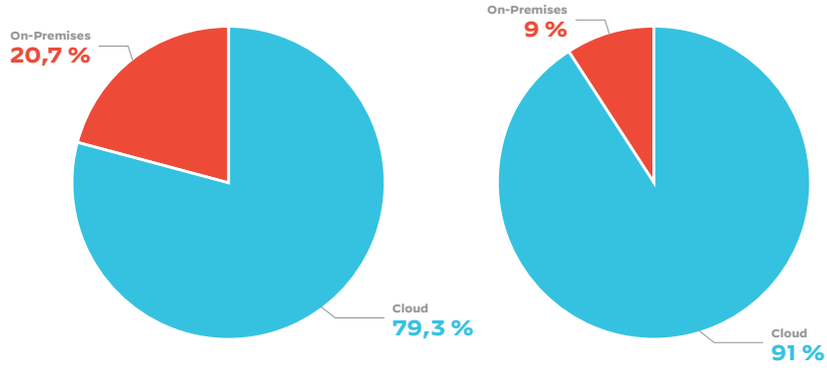

Abbildung 1: Laut den Daten von Mitte 2021 traten fast 80 Prozent der neuen Probleme in der Cloud auf (links). Im ersten Halbjahr 2022 waren es schon 91 Prozent (rechts).

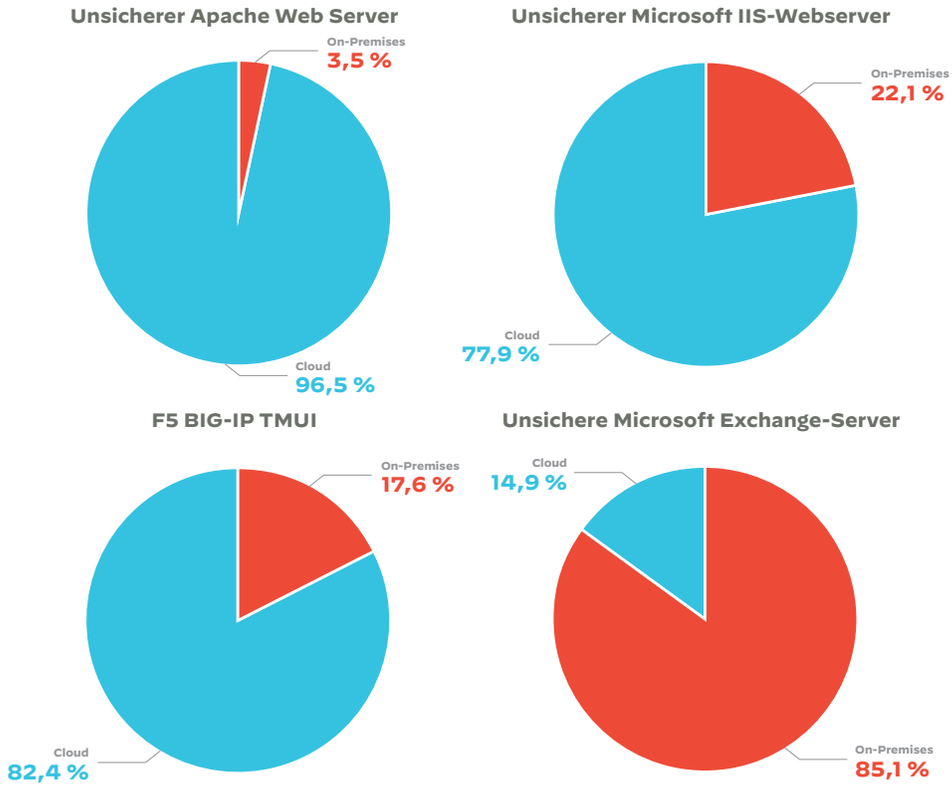

Abbildung 2: Cloud-Probleme können auch vom Servertyp abhängen.

Punkt 2: Viele Unternehmen machen es den Angreifern leicht

Angreifer müssen oft nicht lange suchen, um einen Zugangspunkt zu finden. Öffentlich zugängliche Anmeldeseiten für Administratoren wirken auf sie wie Leuchtreklame.

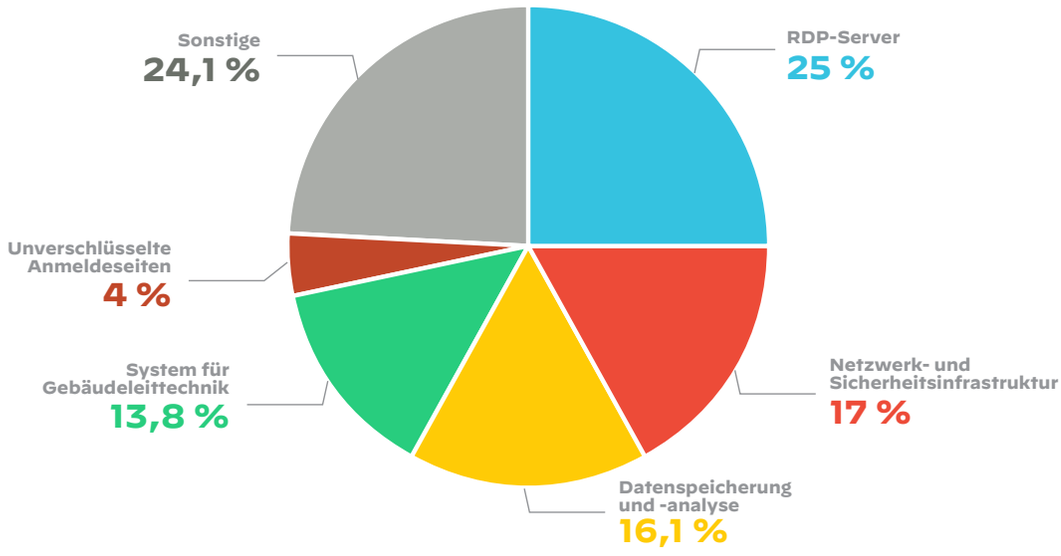

Abbildung 3: Risikoverteilung in der globalen Angriffsfläche

Fast jedes vierte Problem, das wir in der Angriffsfläche gefunden haben, war auf einen öffentlich zugänglichen RDP-Server zurückzuführen. Und selbst bei dem zweithäufigsten Problem (Netzwerk- und Sicherheitsinfrastruktur) war die Ursache meist ein öffentlich zugängliches Anmeldeportal für Systemadministratoren.

Hat sich ein Angreifer erst einmal Zugriff auf einen solchen RDP-Server verschafft, hat er anschließend dieselben Rechte wie ein Benutzer mit legitimen Anmeldedaten. In der Netzwerk- und Sicherheitsstruktur wurden Portale für IT-Administratoren gefunden, über die Angreifer an wesentlich umfassendere Rechte gelangen und bis in das Herz des Unternehmensnetzwerks vordringen könnten. Außerdem wurden bei Xpanse-Analysen über 700 Anmeldeseiten für verschiedene IT-Services gefunden, die unverschlüsselt und über das Internet erreichbar waren.

Über unverschlüsselte Anmeldeseiten können Angreifer die Anmeldedaten ohne großen Aufwand stehlen. Unternehmen sollten daher diese problematischen Seiten und Portale unbedingt finden und deaktivieren. Sind diese Anmeldedaten auch noch für andere öffentlich zugängliche Portale gültig, haben die Angreifer wirklich leichtes Spiel.

Bei jedem öffentlich zugänglichen Portal ohne Multifaktor-Authentifizierung droht ein primitiver Brute-Force-Angriff. Nicht gepatchte Systeme können zudem über bekannte Sicherheitslücken ausgenutzt werden. All diese Probleme lassen sich ganz einfach vermeiden, indem die Anmeldeportale durch ein VPN oder eine Firewall geschützt werden.

Diese Schwachstellen sind allerdings nicht nur weitverbreitet, sondern kommen Unternehmen auch teuer zu stehen. RDP wird inzwischen häufig für die Verbreitung von Ransomware ausgenutzt. Laut dem aktuellen Ransomware Threat Report 2022 von Unit 42 beliefen sich die durchschnittlichen Kosten eines Ransomwareangriffs im Jahr 2021 auf 312.493 USD. Als Folge der Zunahme an Ransomwareangriffen in den letzten Jahren führen Führungskräfte in Unternehmen weltweit entsprechende Abwehrmaßnahmen ein und viele Vorstände fordern Pläne für das Angriffsflächenmanagement, damit keine unbekannten Assets für Angriffe ausgenutzt werden können.

Fast 3.000 Datenbanken und Analysesysteme waren regelmäßig über das öffentliche Internet zugänglich. Diese Systeme enthalten unter Umständen kritische Kundendaten oder geistiges Eigentum und sollten nie öffentlich erreichbar sein. Die Ursache dafür war vermutlich eine versehentliche Fehlkonfigurationen.

Bei unseren Analysen haben wir außerdem über 2.500 kritische Systeme für Gebäudeleittechnik gefunden, die über das öffentliche Internet zugänglich waren. Das zeigt, dass Unternehmen in einer digitalen Welt mit immer mehr Remoteverbindungen nicht nur ihre IT-Assets, sondern auch ihre OT-Assets (Operational Technology) schützen müssen. Diese Assets werden häufig von speziellen Unternehmenszweigen oder Abteilungen verwaltet und daher eventuell nicht von den IT-Sicherheitssystemen überwacht.

Punkt 3: End-of-Life-Software bedeutet auch das Ende der Sicherheit

Wenn öffentlich zugängliche Seiten für den Remotezugriff oder die Remoteanmeldung wie Leuchtreklame wirken, lässt sich End-of-Life-Software vielleicht am besten mit Wertsachen vergleichen, die im Herbst in einem Haus aus Stroh untergebracht werden. Wenn es solide gebaut wurde, übersteht es eventuell einen verregneten Herbst, aber im Winter können die zahlreichen Löcher nicht mehr gestopft werden.

Bei unseren Untersuchungen sind uns mehrere Unternehmen in allen Branchen aufgefallen, die nicht mehr unterstützte Softwareversionen nutzen. Von den unten aufgeführten Anwendungen verwendeten etwa 30 % der Unternehmen EOL-Versionen.

Apache Web Server	~32 % mit EOL-Versionen
Microsoft Exchange-Server	29 % mit EOL-/nicht unterstützten Versionen

Außerdem sind immer noch nicht gepatchte Versionen von Software im Einsatz, bei denen bekannt ist, dass sie bereits ausgenutzt werden. Obwohl es schon seit vier oder fünf Monaten Patches gab, lieferten die Xpanse-Analysen die folgenden Ergebnisse basierend auf den von den Anwendungen gemeldeten Versionen:

- 11.511 Instanzen der Apache Web Server, die ungesichert im öffentlichen Internet ausgeführt wurden, waren für die Sicherheitslücken CVE-2021-41773 und CVE-2021-42013 anfällig.
- 2.700 Instanzen waren durch CVE-2021-26084 (Atlassian Confluence) gefährdet.
- 74 Prozent der Instanzen der Zoho ManageEngine ServiceDesk Plus-Software (3.400 insgesamt) waren für zwei kritische CVEs anfällig (CVE-2021-44077 und CVE-2021-44526), von denen eine aktiv ausgenutzt wurde.

Über solche Sicherheitslücken können sich Angreifer Zugriff auf das Netzwerk des Opfers verschaffen, die Zugriffsrechte ausweiten, sich im Netzwerk ausbreiten und per Remotezugriff Code ausführen.

Auswirkungen auf den Geschäftsbetrieb

Angreifer müssen sich gar nicht einzelne Opfer herauspicken, sondern einfach nur nach Schwachstellen suchen – und kaum etwas enthält mehr Schwachstellen als EOL-Software. Assets mit EOL-Software sollten niemals über das Internet zugänglich sein. Falls auf einem Asset kein sicheres Update einer Software installiert werden kann, sollte es isoliert oder sogar vollständig außer Betrieb genommen werden.

Ansonsten brauchen Angreifer nur im Internet nach Assets oder Services mit unbeabsichtigten Fehlkonfigurationen zu suchen, um potenzielle Opfer zu finden. Unternehmen müssen automatische Prozesse einrichten, um EOL-Software, Fehlkonfigurationen und unbekannte Assets zu finden und alle Zero-Day-Sicherheitslücken in ihrer Angriffsfläche zu identifizieren.

Punkt 4: Die Probleme sind komplex und branchenspezifisch

Wenn Unternehmen gefragt werden, weshalb sie wohl zum Angriffsziel wurden, wird damit auf gewisse Weise den Opfern die Schuld zugewiesen. Angreifer interessieren sich beispielsweise für die Daten von Finanzdienstleistern oder wissen, dass einige Unternehmen eher bereit sind, ein Lösegeld zu zahlen, da Ausfallzeiten zu riskant wären, wie beispielweise im Gesundheitswesen.

Wenn Unternehmen wissen, dass sie zu den potenziellen Angriffszielen gehören, können sie Daten und Systeme, die nicht öffentlich zugänglich sein müssen, gezielt isolieren. Bei Geräten mit Internetzugang geht es hingegen in erster Linie darum, Schwachstellen und Sicherheitslücken zu identifizieren. Aus Sicht der Angreifer haben Unternehmen daher mehr Gemeinsamkeiten als Unterschiede.

Bei den Xpanse-Analysen wurden in allen Branchen ähnliche Probleme gefunden, aber deren Verteilung variierte erheblich. So tritt in Unternehmen häufig eine Kombination aus öffentlich zugänglichen RDP-Servern, Schwachstellen in der Netzwerk- und Sicherheitsinfrastruktur oder in Datenbanken und Analysesystemen auf, doch die Details in Bezug auf die Assets, die Art der Schwachstellen und die Gründe für den Angriff unterscheiden sich in jeder Situation.

Störung des Geschäftsbetriebs

Im Allgemeinen gibt es zwei Gründe, warum Angreifer ein Unternehmen ins Visier nehmen: Störung des Geschäftsbetriebs oder Datendiebstahl. Unter die erste Kategorie fallen Branchen wie Versorgung und Energie, Gesundheitswesen, Transport und Logistik und (manchmal) der Groß- und Einzelhandel. Das Ziel der Angreifer ist es, den Geschäftsbetrieb zu stören oder mit der Störung zu drohen, entweder aus politischen Motiven oder weil sie hoffen, dass für die Opfer eine Lösegeldzahlung ein geringerer Verlust als die drohende oder tatsächliche Störung ist.

Versorgung und Energie

Versorgungs- und Energieunternehmen bilden fast schon eine eigene Kategorie. Zum einen unterscheiden sich ihre Probleme stark von den meisten anderen Branchen und zum anderen ist die industrielle Infrastruktur seit jeher ein Ziel für Angriffe mit einem politischen Hintergrund.

Das bekannteste Beispiel ist Stuxnet, ein Wurm, der Berichten zufolge von US-amerikanischen und israelischen Behörden entwickelt wurde, um das iranische und angeblich auch das nordkoreanische Atomprogramm zu stören.

Das größte Problem in dieser Kategorie waren öffentlich zugängliche Administratorbereiche in der IT-Infrastruktur. Unsere Analyse offenbarte mehrere wichtige OT-Systeme, zum Beispiel für die Gebäudeleittechnik, die nicht über das Internet erreichbar sein sollten.

Der Schutz der kritischen IT- und OT-Infrastrukturen hat daher für Versorgungs- und Energieunternehmen höchste Priorität. Kritische Versorgungs- und Energieunternehmen sind auch ein beliebtes Ziel staatlich gesponserter Hackergruppen. Ist also ein Portal für die Gebäudeleittechnik über das öffentliche Internet erreichbar, können Angreifer die Systeme, einschließlich Feueralarmen, Aufzügen und Brandschutz, kapern und einen enormen Schaden anrichten.

Der Angriff auf Colonial Pipeline im April 2021 wurde durch ein einziges manipuliertes Benutzerkonto und VPN-Zugriff möglich, für den keine Multifaktor-Authentifizierung aktiviert war. Die Folge war ein Ransomwareangriff und die vollständige Stilllegung der Pipeline für fünf Tage.

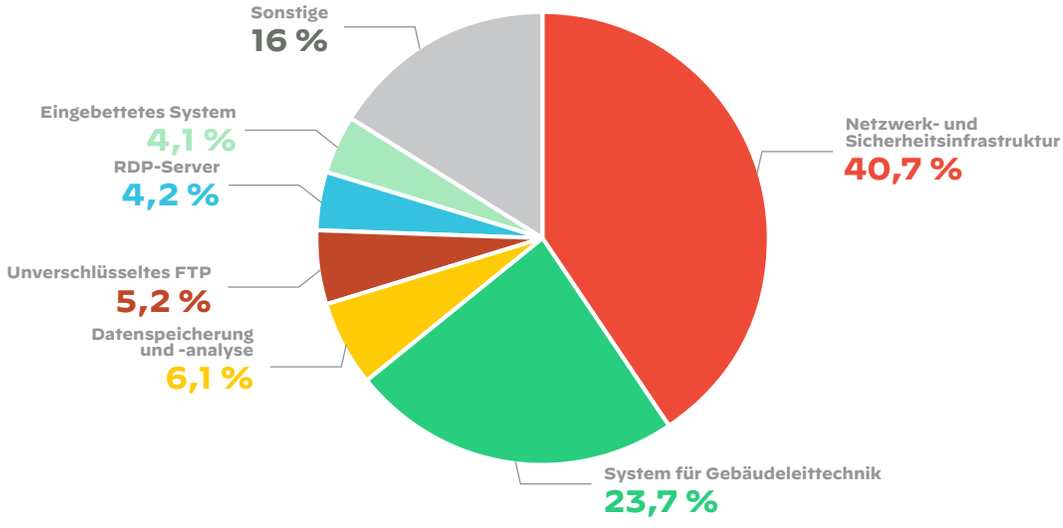

Abbildung 4: Risikoverteilung in der Angriffsfläche der Versorgungs- und Energiebranche

Gesundheitswesen

Mit einem HIPAA-konformen RDP-Server können medizinische Mitarbeiter per Remotezugriff alle wichtigen Informationen abrufen, die ihnen auch im Krankenhaus vor Ort zur Verfügung stehen. Auf diese Weise können sie auch im Homeoffice oder unterwegs produktiv arbeiten.

Unseren Analysen zufolge werden RDP-Server im Gesundheitswesen am häufigsten ausgenutzt, sodass diese Einrichtungen anfälliger für Ransomwareangriffe sind als Unternehmen anderer Branchen. Das ist im Gesundheitswesen jedoch besonders gefährlich, da dadurch unter Umständen Menschenleben auf dem Spiel stehen.

Laut dem Ransomware Threat Report 2022 von Unit 42 werden RDP-Server inzwischen von Hackgruppen für Ransomwareangriffe bevorzugt, da es relativ einfach ist, versehentlich offengelegte RDP-Server zu finden und sich per Brute-Force-Angriff Zugang zu verschaffen.

Das Gesundheitswesen ist schon seit Jahren im Visier der Ransomware-Hacker und da der potenzielle Schaden so groß ist, zahlen viele Krankenhäuser lieber das Lösegeld, als eine Störung der Abläufe zu riskieren – wodurch sie für Cyberkriminelle natürlich äußerst attraktive Ziele darstellen.

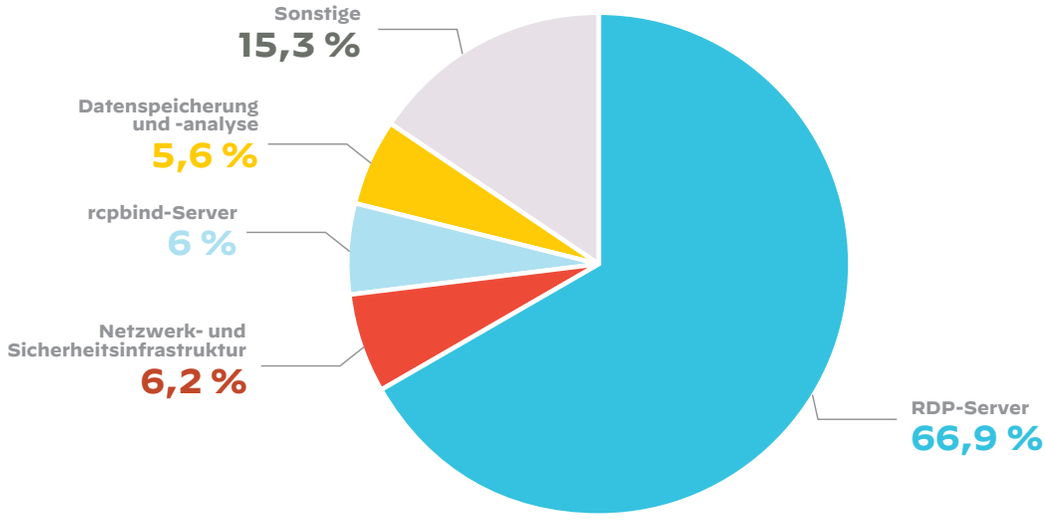

Abbildung 5: Risikoverteilung in der Angriffsfläche des Gesundheitswesens

Transport und Logistik

Auch im Transport- und Logistikwesen stellen RDP-Schwachstellen das größte Risiko dar. Unternehmen sollten eng mit ihren Logistikpartnern in der Lieferkette zusammenarbeiten, um kritische RDP-Probleme zu identifizieren und zu beheben, bevor es zu einem Vorfall kommt.

2017 wurde das dänische Logistikunternehmen Maersk Opfer eines Ransomwareangriffs, der den Betrieb zwei Wochen lang lahmlegte und Berichten zufolge Kosten in Höhe von etwa 300 Millionen USD verursachte.

Die Pandemie hat in den globalen Lieferketten für Chaos gesorgt und die Nachfrage ist zudem stark gestiegen. Infolgedessen zielen Ransomwareangriffe inzwischen auf Unternehmen in der globalen Transport- und Logistikbranche ab.

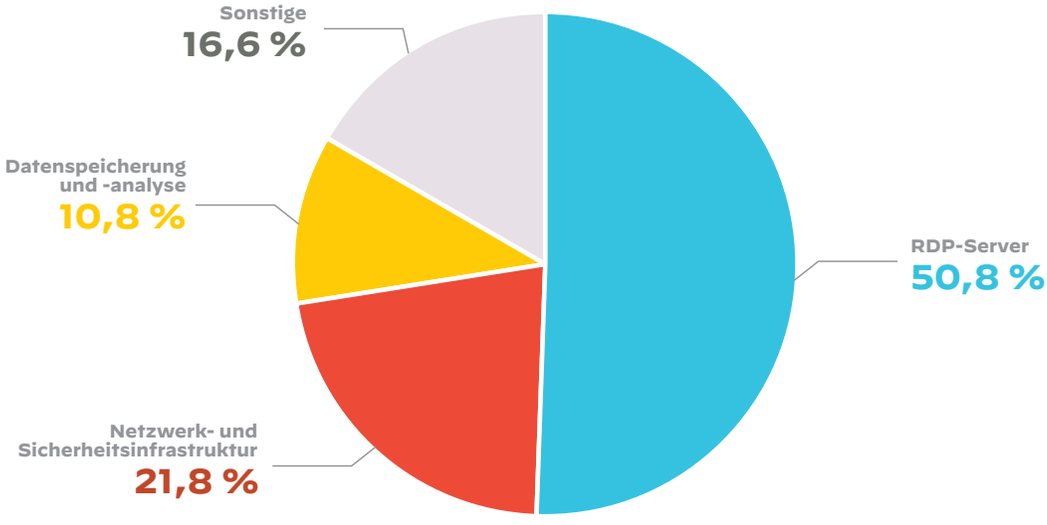

Abbildung 6: Risikoverteilung in der Angriffsfläche der Transport- und Logistikbranche

Groß- und Einzelhandel

Im Groß- und Einzelhandel halten sich Angriffe zur Störung des Geschäftsbetriebs und für den Datendiebstahl in etwa die Waage. So können Angriffe auf den Einzelhandel erhebliche Störungen verursachen, aber wenn Kassensysteme angegriffen werden, steigt auch das Risiko für die Kreditkartendaten der Kunden.

Für Ransomware-Hacker sind Angriffe auf Unternehmen im Groß- und Einzelhandel lukrativ, da diese rund um die Uhr betriebsbereit sein müssen und daher schneller in eine Lösegeldzahlung einwilligen. Das sollte Unternehmen in der Branche zu denken geben. Wir haben festgestellt, dass RDP-Server für mehr als 60 % der Schwachstellen in der Angriffsfläche des Groß- und Einzelhandels verantwortlich sind. Das ist die größte Kategorie in dieser Branche.

Einer der größten Cyberangriffe der Geschichte wurde 2013 auf Target verübt. Dabei wurden die Kreditkartendaten von 40 Millionen Kunden gestohlen und sonstige Informationen zu 70 Millionen Kunden offengelegt. Target gab über 200 Millionen USD für Anwaltskosten aus und musste letztendlich eine Strafzahlung in Höhe von 18,5 Millionen USD an US-Bundesstaaten zahlen.

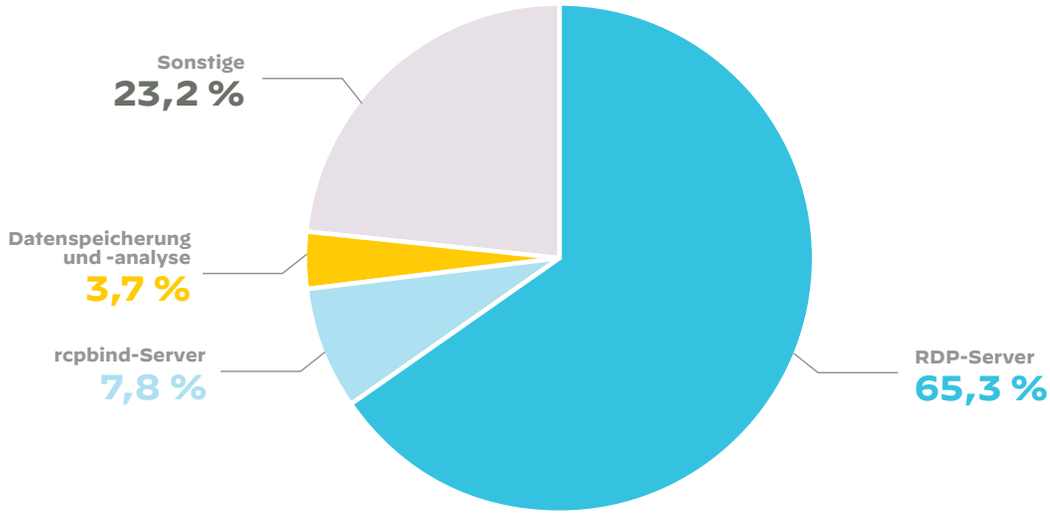

Abbildung 7: Risikoverteilung in der Angriffsfläche des Groß- und Einzelhandels

Wertvolle Daten

Wenn die Störung des Geschäftsbetriebs nicht ausreicht, setzen Angreifer meist auf den Diebstahl wertvoller Daten. Dabei kann es sich um Finanzdaten handeln, die dann an Identitätsdiebe weiterverkauft werden, oder um Daten, die für das jeweilige Unternehmen wertvoll sind, zum Beispiel geistiges Eigentum.

Finanzdienstleistungen

Die striktesten IT-Verordnungen und Compliancevorgaben gelten vermutlich in der Finanzbranche. Aus diesem Grund führen viele Unternehmen in dieser Branche bereits sehr früh Cybersicherheitsmaßnahmen und -lösungen ein, aber da sie wertvolle Daten verarbeiten, bleiben sie für Cyberkriminelle trotzdem interessant.

Mehr als 80 Prozent der Probleme, die wir in der Angriffsfläche der Finanzbranche gefunden haben, betreffen entweder öffentlich zugängliche RDP-Server oder sogar versehentlich offengelegte Datenbanken und Analysesysteme. Datenbanken sollten niemals über das öffentliche Internet erreichbar sein, sondern immer durch eine Firewall oder ein VPN geschützt werden.

Offengelegte Datenspeicher sind in dieser Branche besonders besorgniserregend, da sie unter Umständen wichtige Kunden- oder Transaktionsdaten enthalten. Durch die Zunahme des mobilen Arbeitens steigt auch das Risiko, da Mitarbeiter diese wichtigen Daten über potenziell anfällige Zugangspunkte abrufen.

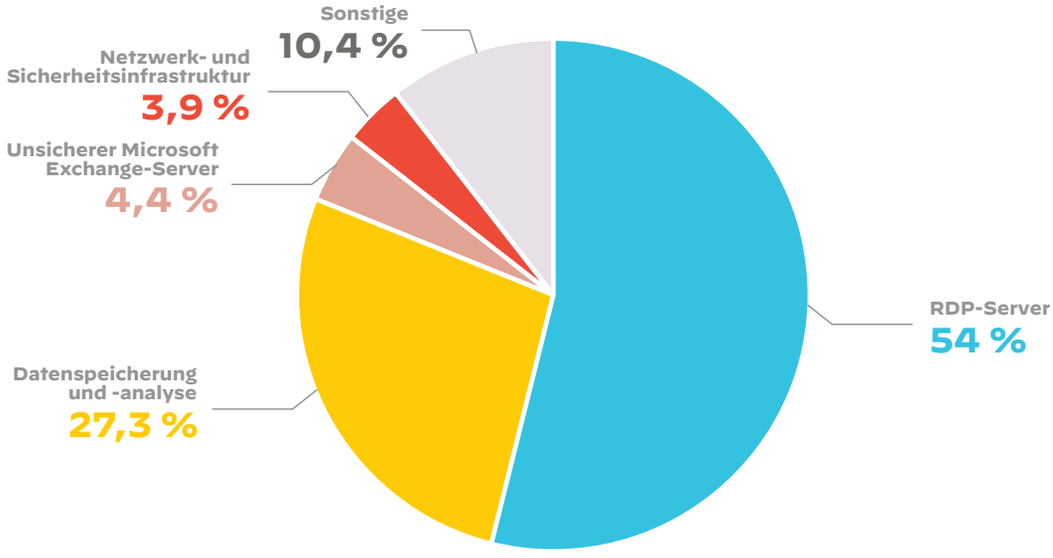

Abbildung 8: Risikoverteilung in der Angriffsfläche der Finanzdienstleistungen

Professional Services und Rechtsberatung

Die Kombination der häufigsten Schwachstellen bei Professional Services und Rechtsberatung ist besonders gefährlich. Für Unternehmen, die öffentlich zugängliche Datenspeicher mit unverschlüsselten Anmeldeseiten nutzen, ist es nur eine Frage der Zeit, bis sie Opfer eines schwerwiegenden Datendiebstahls oder Ransomwareangriffs werden.

Dabei droht die Offenlegung von geistigem Eigentum, kritischen Kundendaten und anderen hochsensiblen Informationen.

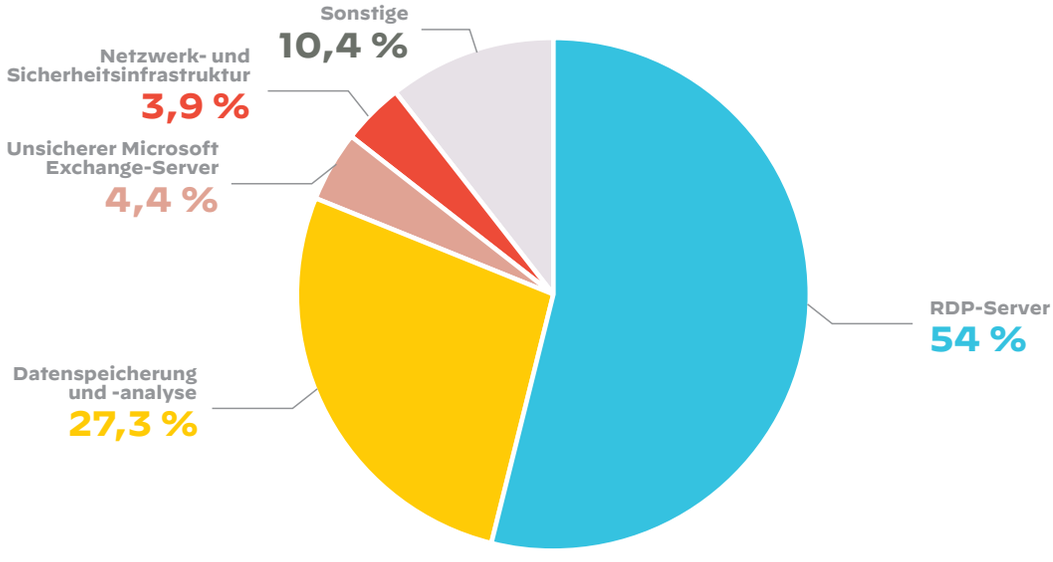

Abbildung 9: Risikoverteilung in der Angriffsfläche der Professional Services und Rechtsberatung

Hightech

In Hightech-Unternehmen sind öffentlich zugängliche Portale für IT-Administratoren das größte Problem und (wie schon zuvor angemerkt) für Angreifer besonders interessant, da sie sich darüber Zugang zu dem gesamten Netzwerk und den Zugriffsrechten verschaffen können. Der Schaden kann immens sein. Hightech-Unternehmen müssen daher öffentlich zugängliche Anmeldeseiten für IT-Administratoren schnellstmöglich finden und sofort durch eine Firewall oder ein VPN schützen.

FTP gehört nicht mehr zu den Standardprotokollen der Branche und verstößt gegen zahlreiche gesetzliche Compliancevorgaben, da bei der Authentifizierung Benutzernamen und Passwörter im Klartext übermittelt und nicht verschlüsselt werden. Unseren Beobachtungen zufolge wird es aber immer noch in der Branche eingesetzt (6,9 Prozent der Schwachstellen). Daten, die über FTP gesendet werden, sind anfällig für Sniffing-, Spoofing- und Brute-Force-Angriffe sowie andere primitive Angriffsmethoden.

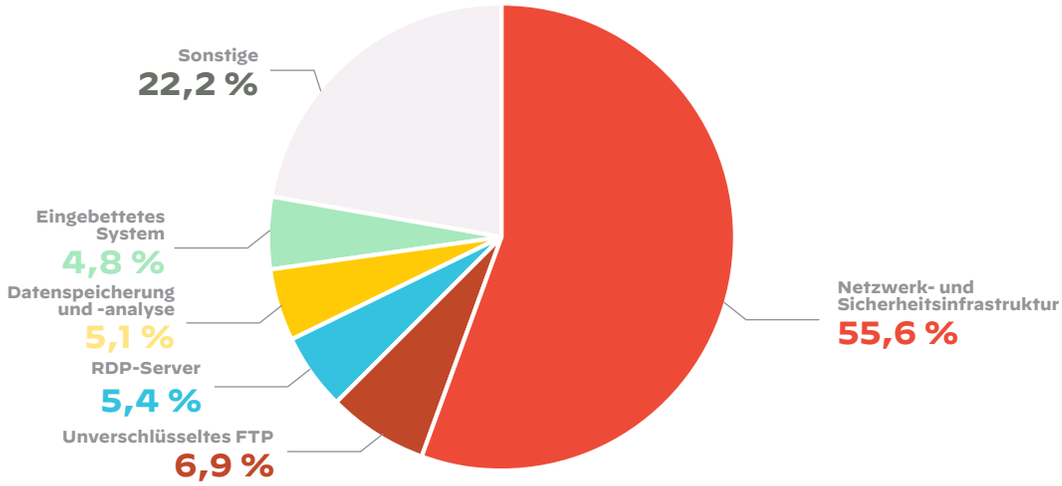

Abbildung 10: Risikoverteilung in der Angriffsfläche der Hightech-Branche

Medien und Unterhaltung

In der Medien- und Unterhaltungsbranche stellen Datenspeicher und Analyse-Infrastrukturen das größte Risiko dar, da sie unter Umständen wichtige IP-Adressen und Kundendaten enthalten.

Einer der aufsehenerregendsten Angriffe wurde 2014 auf Sony Pictures verübt. Dabei stahlen die Hacker mehrere Terabyte an Daten und Sony musste sein Netzwerk mehrere Tage außer Betrieb nehmen. Nach dem Angriff wurden fünf Filme, von denen vier zu diesem Zeitpunkt noch unveröffentlicht waren, von den Hackern preisgegeben.

Die zweitgrößte Kategorie waren RDP-Services. Potenzielle Angriffe könnten die Services der Branche nahezu lahmlegen.

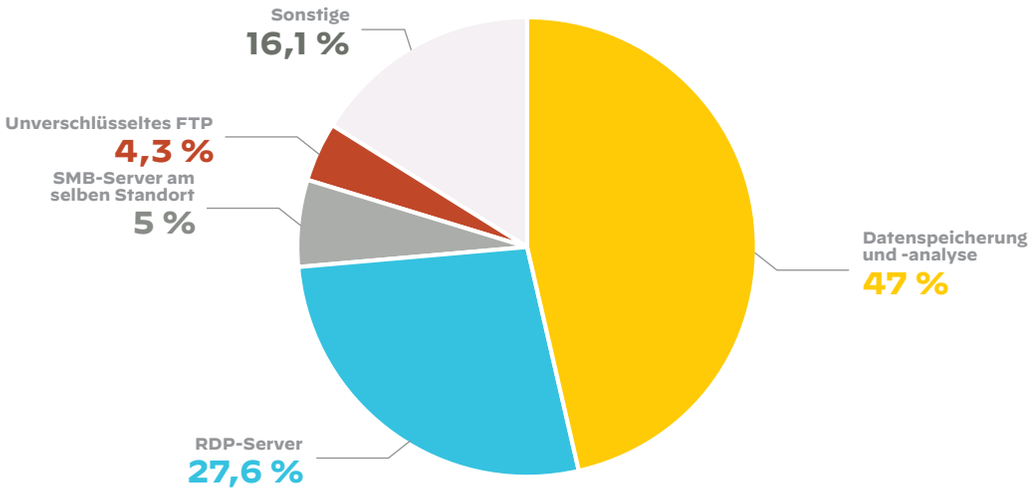

Abbildung 11: Risikoverteilung in der Angriffsfläche der Medien- und Unterhaltungsbranche

Versicherungswesen

In der Versicherungsbranche liegen Sicherheitslücken in Datenspeichern, RDP-Servern und der Netzwerkinfrastruktur in etwa gleichauf.

Im Mai 2021 zahlte das Versicherungsunternehmen CNA Financial Berichten zufolge 40 Millionen USD an Lösegeld, da es auch zwei Wochen nach einem Angriff seine Systeme nicht wiederherstellen konnte. Außerdem waren personenbezogene Daten von mehr als 75.000 Kunden betroffen.

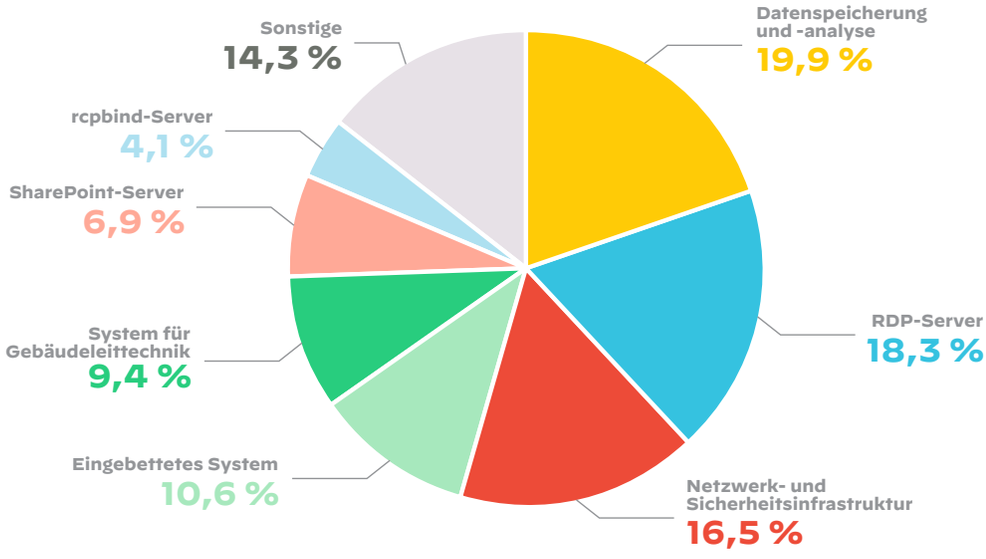

Abbildung 12: Risikoverteilung in der Angriffsfläche der Versicherungsbranche

Auswirkungen auf den Geschäftsbetrieb

Zwar spezialisieren sich einige Angreifer auf bestimmte Angriffsflächen, doch einige Schwachstellentypen sind häufiger vertreten, sodass der erste Angriffsvektor eventuell gar nicht so stark variiert. An den Daten lässt sich ablesen, dass Protokolle für den Remotezugriff und Remote-Anmeldeseiten auf unterschiedliche Weise offengelegt werden und dann einen einfachen Zugangspunkt für Angreifer bieten.

Unabhängig davon, ob Angreifer es auf eine Störung des Geschäftsbetriebs oder den Diebstahl wertvoller Daten abgesehen haben, müssen Unternehmen wissen, welche Sicherheitslücken das größte Risiko für sie bergen.

Wer die typischen Risiken kennt, kann das Schwachstellenmanagement konkret auf diese Bereiche ausrichten. Doch in jeder Branche geht die Gefahr nicht nur von einer einzigen Angriffsmethode aus. Der sicherste Weg ist, eine umfassende Liste aller Assets und potenziellen Schwachstellen zu erstellen und kontinuierlich zu aktualisieren, um alle Risiken abzudecken.

Punkt 5: In Angriffsflächen sammeln sich Probleme schnell an

Eines sollte inzwischen deutlich geworden sein: Die globale Angriffsfläche ist äußerst dynamisch – sie verändert sich ständig und wächst kontinuierlich. Für Sicherheitsexperten bedeutet dies, dass sie ständig auf der Hut sein müssen. Werden bestimmte Aufgaben vernachlässigt, wächst schnell ein unüberwindlicher Berg an Problemen und Schwachstellen an.

In den Angriffsflächen treten fortlaufend neue Probleme auf – zum Beispiel neue Sicherheitslücken, Konfigurationsänderungen, die Schwachstellen verursachen, und abgelaufene Zertifikate. Nicht behobene Probleme machen es den Angreifern dann leicht (wie schon in Punkt 2 erläutert).

Bei unserer ersten Untersuchung der globalen Angriffsfläche im Jahr 2021 haben wir uns auf vier spezifische Schwachstellen konzentriert, die bereits in der Praxis ausgenutzt und in mehreren Sicherheitshinweisen von Behörden aufgeführt wurden:

- Unsichere Apache Web Server
- F5 BIG-IP TMUI
- Unsichere Microsoft Exchange-Server
- Unsichere Microsoft IIS-Webserver

Wir haben diese vier Typen einen Monat lang in einer nicht verwalteten Angriffsfläche beobachtet.

Dabei fiel auf, dass in allen Branchen neue Probleme hinzukamen, selbst wenn Unternehmen versuchten, die aktiven Schwachstellen zu beheben. Man könnte nun behaupten, dass diese Unternehmen niemals sicher und während des gesamten Monats für Angriffe anfällig waren, da die nicht verwaltete Angriffsfläche anwuchs und die Anzahl der Sicherheitsprobleme weiter stieg.

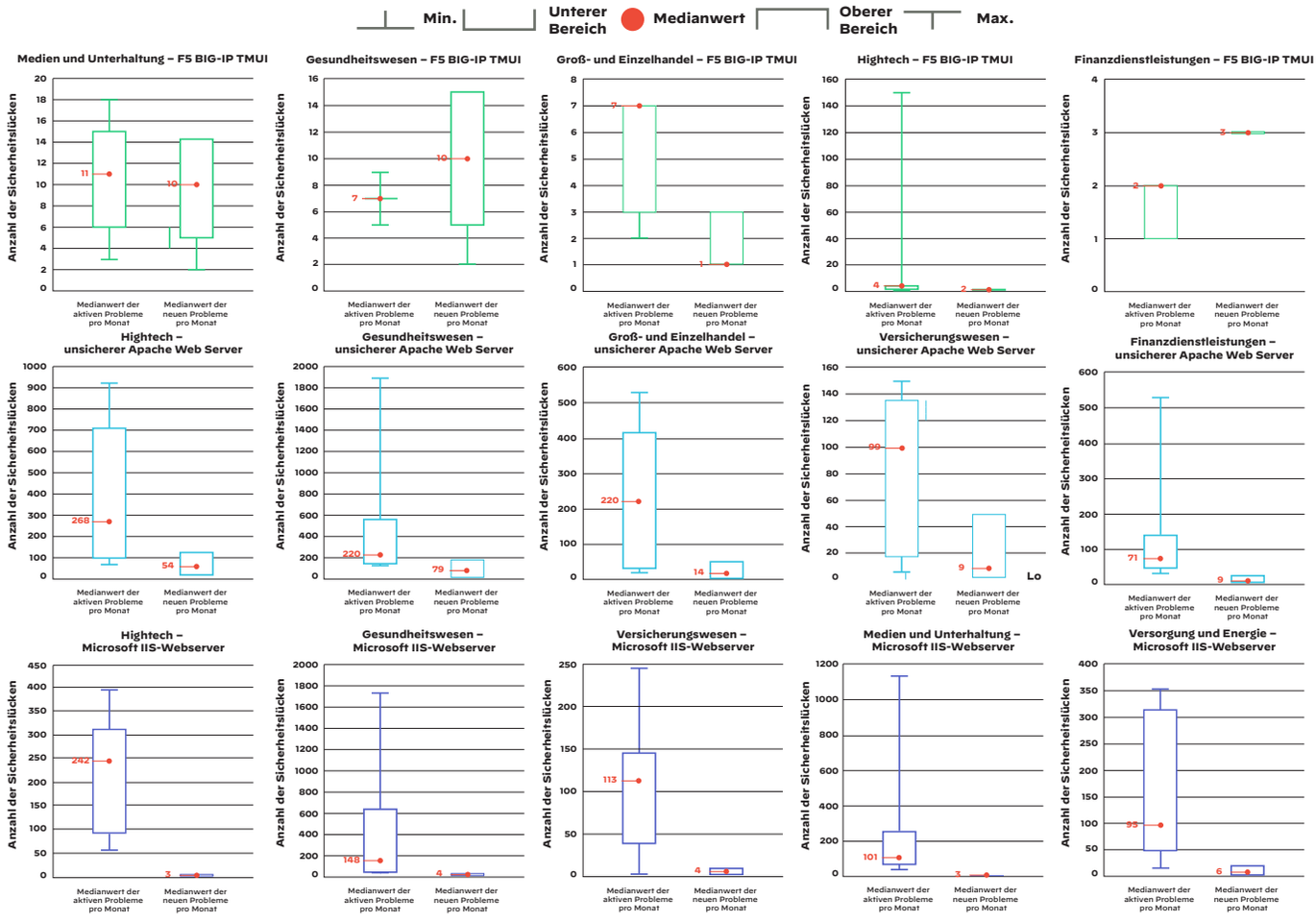

Abbildung 13: Medianwert der aktiven und neuen Probleme pro Monat/Unternehmen in einer Branche

Diese vier Typen machen nur einen winzigen Teil (<1 %) aller Kategorien einer Angriffsfläche aus. Bei unserer Untersuchung der Daten von Dezember 2021 bis Juni 2022 haben wir daher auch ermittelt, wie schnell neue Probleme mit einem hohen oder kritischen Schweregrad in den Angriffsflächen erkannt wurden.

Wir stellten fest, dass die Probleme branchenübergreifend konstant sind. Keine der von uns analysierten Branche konnte ihre Angriffsfläche verkleinern.

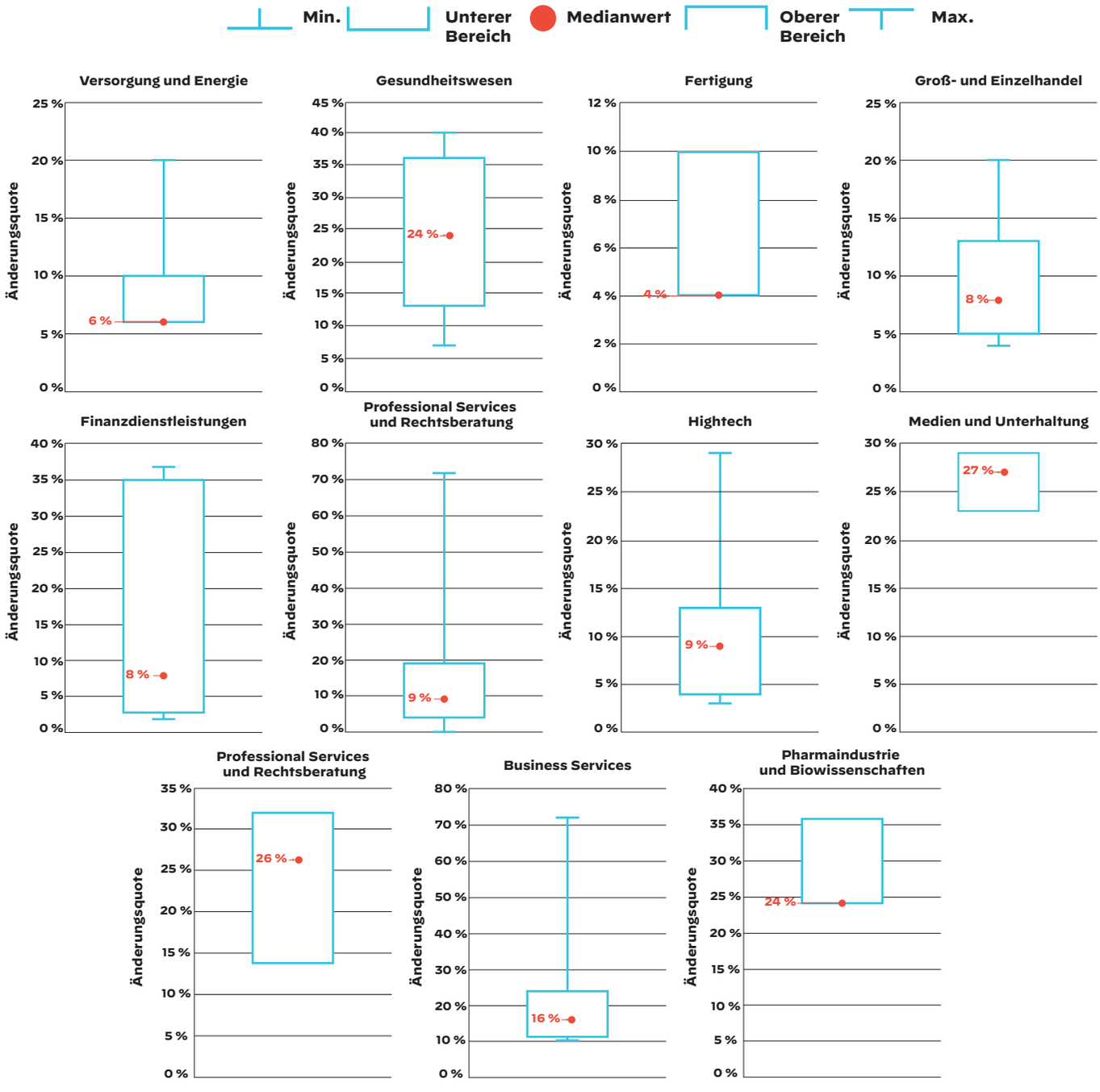

Abbildung 14: Änderungsquote für die Angriffsfläche pro Monat nach Branche

In Branchen, in denen man einen größeren Anteil an On-Premises-Assets erwartet, wie Transport und Logistik oder Versorgung und Energie, stieg die Anzahl der neuen Probleme langsamer an als in anderen Branchen (um 3,67 Prozent bzw. 6,36 Prozent). Branchen, die verstärkt Cloud-Umgebungen nutzen, wie der Medien- und Unterhaltungssektor, wiesen auch eine höhere Änderungsquote von 26,89 Prozent auf.

Es gab allerdings einige interessante Ausreißer: Gesundheitswesen, Versicherungswesen sowie Pharmaindustrie und Biowissenschaften, von denen man annehmen würde, dass sie vornehmlich On-Premises-Assets nutzen, wiesen einige der höchsten Änderungsquoten auf (24 Prozent; 26,2 Prozent; 24 Prozent). Schwachstellen sind in diesen Branchen allerdings besonders riskant, da große Mengen an personenbezogenen Daten und geistigem Eigentum gefährdet werden und in den Krankenhäusern sogar Menschenleben auf dem Spiel stehen.

Auswirkungen auf den Geschäftsbetrieb

Das Hauptziel sollte immer die Verkleinerung der Angriffsfläche sein, aber mit manuellen Anstrengungen ist das derzeit nicht zu erreichen. Die Angriffsflächen wachsen in allen Branchen und die Sicherheitsteams hinken ständig hinterher. Da neue Probleme nicht sofort behoben werden können, häufen sie sich an und werden damit leichte Beute für Angreifer.

Die Geschwindigkeit, mit der neue Probleme auftreten, unterstreicht, wie wichtig zuverlässige und resiliente Sicherheitsprozesse sind. Unternehmen benötigen zweifellos einen besseren Überblick über ihre Angriffsfläche und die Schwachstellen, aber zusätzlich sollten sie mehr Prozesse automatisieren, um die Fehlerbehebung zu beschleunigen und die Sicherheitsteams zu entlasten.

Lösungsmöglichkeit

Sicherheitsteams sind viel zu beschäftigt, als dass sie ständig Probleme derselben Kategorie beheben könnten. Eine effiziente Möglichkeit ist, ein Tool für das Angriffsflächenmanagement mit einer SOAR-Lösung (Security Orchestration, Automation and Response) zu kombinieren. Damit können neue Probleme automatisch identifiziert, priorisiert und entweder sofort behoben oder zusammen mit umfassenden Kontextdaten an einen entsprechenden Experten weitergeleitet werden.

Punkt 6: RDP- und Cloud-Schwachstellen sind persistent

Wie wichtig resiliente Sicherheitsprozesse sind, zeigen auch die neuen Daten zur Persistenz der Probleme in Angriffsflächen.

Bei RDP-Schwachstellen steigt das Risiko eines Cyberangriffs.

Öffentlich zugängliche RDP-Server gehören schon lange zu beliebten Zielen von Angreifern. Unit 42™ von Palo Alto Networks hat im Incident Response and Breach Report 2020 festgestellt, dass bei der Hälfte der Sicherheitsvorfälle ein öffentlich zugänglicher RDP-Server als Angriffsvektor ausgenutzt wurde. Im aktuellen Ransomware Threat Report 2022 von Unit 42 weist das Team zudem darauf hin, dass Brute-Force-Angriffe auf RDP-Server in allen untersuchten Fällen zu den drei häufigsten Zugriffsarten gehörten.

Vor diesem Hintergrund ist es besorgniserregend, dass in sieben der zwölf von Xpanse untersuchten Branchen RDP-Server im Durchschnitt mehr als sieben Tage pro Monat öffentlich zugänglich waren. In der Transport- und Logistikbranche betrug der Durchschnittswert sogar 13,5 Tage. In Anbetracht des Schadens und der Schwierigkeiten, die der oben aufgeführte Ransomwareangriff auf Maersk im Jahr 2017 verursacht hatte, würde man davon ausgehen, dass sich die gesamte Branche um eine Reduzierung der öffentlich zugänglichen RDP-Server bemühen würde.

Tabelle 1: Anzahl der RDP-Instanzen, die im Beobachtungszeitraum über das öffentliche Internet zugänglich waren, und die durchschnittliche Anzahl der Tage pro Monat mit einer öffentlich zugänglichen RDP-Instanz

Branche	Anzahl der erfassten öffentlich zugänglichen RDP-Instanzen	Durchschnittliche Anzahl der Tage, an denen RDP-Instanzen über das öffentliche Internet zugänglich waren
Transport und Logistik	24.113	13,49
Hightech	397.615	9,71
Versorgung und Energie	46.497	9,59
Medien und Unterhaltung	334.428	9,08
Business Services	154.238	8,36
Professional Services und Rechtsberatung	128.545	8,19
Finanzdienstleistungen	151.209	7,78
Versicherungswesen	38.102	5,78
Gesundheitswesen	112.525	5,58
Groß- und Einzelhandel	87.916	4,87
Telekommunikation	189.907	4,64
Pharmaindustrie und Biowissenschaften	53.808	4,13

In den fünf Branchen am Tabellenende ist die Lage nicht allzu dramatisch, aber auch dort waren RDP-Instanzen im Durchschnitt mindestens vier Tage pro Monat öffentlich zugänglich. Das ist nicht gerade ein Grund für Optimismus. Jede Offenlegung kann gravierende Konsequenzen haben. In Branchen wie dem Gesundheitswesen, in denen Menschenleben auf dem Spiel stehen, sind selbst 5,6 Tage pro Monat zu viel. Denn im Laufe von sechs Monaten wären es dann schon etwa 34 Tage, an denen Angreifer öffentlich zugängliche RDP-Server ausnutzen könnten.

Aktive Cloud-Probleme pro Monat

Wenn wir die Anzahl aller aktiven Cloud-Probleme pro Monat betrachten, fällt auch hier auf, dass viele davon persistent sind. Doch in diesem Fall scheint es eine deutliche Zweiteilung der Branchen zu geben.

In einigen Branchen lag der Medianwert der aktiven Cloud-Probleme pro Monat unter 200:

- Versorgung und Energie
- Finanzdienstleistungen
- Professional Services und Rechtsberatung
- Fertigung
- Versicherungswesen
- Business Services
- Hightech

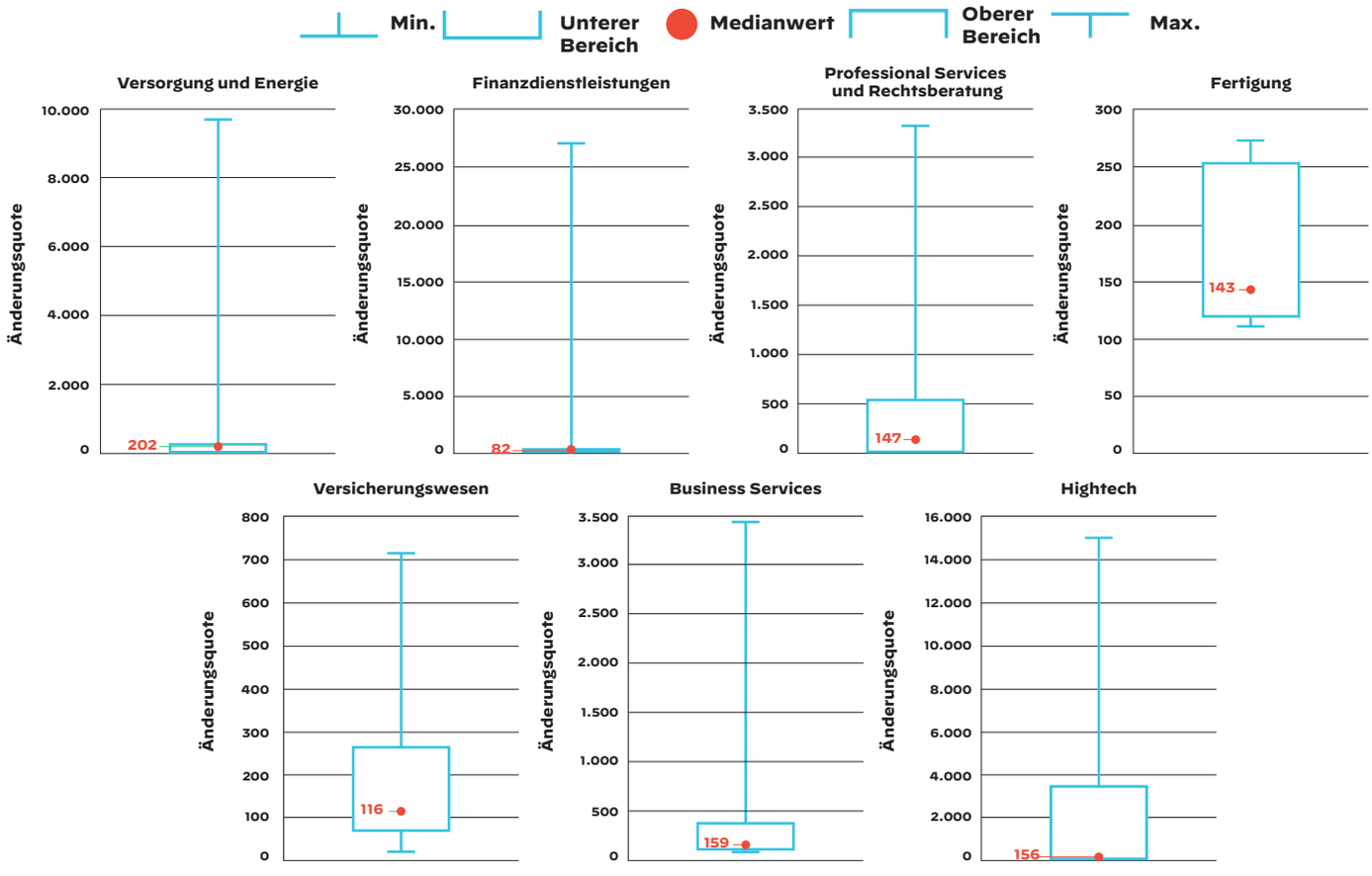

Abbildung 15: Anzahl der neuen Cloud-Probleme pro Monat nach Branche

In den übrigen Branchen hingegen lag der Medianwert der aktiven Cloud-Probleme pro Monat jeweils über 400:

- Gesundheitswesen
- Groß- und Einzelhandel
- Medien und Unterhaltung
- Telekommunikation
- Pharmaindustrie und Biowissenschaften

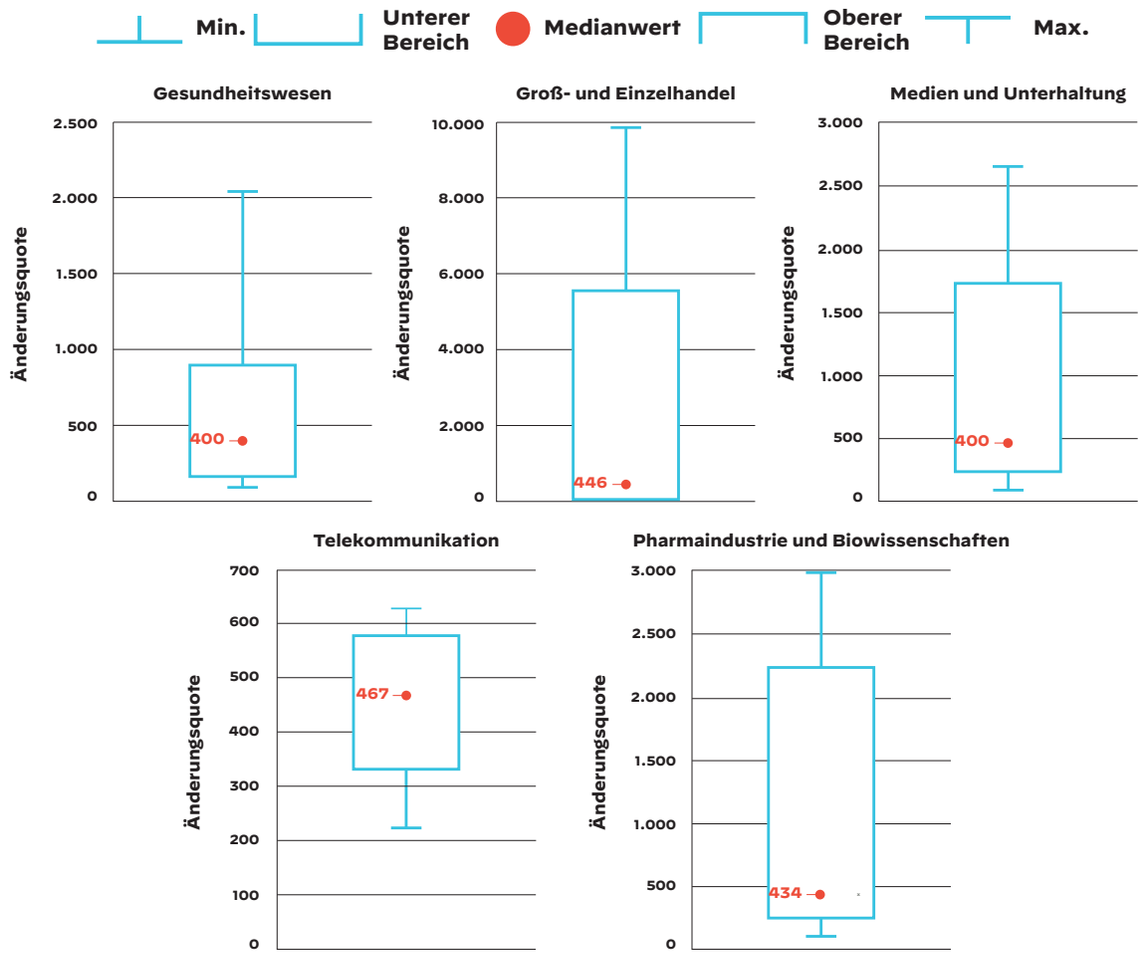

Abbildung 16: Anzahl der neuen Cloud-Probleme pro Monat nach Branche

Bei Hunderten aktiven Cloud-Schwachstellen pro Monat ist das Risiko natürlich wesentlich höher. Eine Redensart im Cybersicherheitsbereich lautet, dass Angreifer nur einmal Erfolg haben müssen, Sicherheitsteams hingegen fortlaufend erfolgreich sein müssen. Hunderte Schwachstellen pro Monat sind daher keine gute Bilanz.

Erwähnenswert sind angesichts dieser Daten außerdem die starken Schwankungen in einigen Branchen. Die Hightech-Branche lag mit einem Medianwert von 156 aktiven Cloud-Problemen pro Monat im unteren Bereich. Im 75. Perzentil stiegen diese jedoch auf 3.661 Probleme und im 90. Perzentil auf 15.381. Im Groß- und Einzelhandel war die Lage ähnlich: Der Medianwert für die aktiven Cloud-Probleme lag bei 446, stieg aber im 75. Perzentil auf 5.613 und im 90. Perzentil auf 9.954. Das auffälligste Beispiel waren die Finanzdienstleistungen, die den niedrigsten Medianwert aller Branchen hatten, im 90. Perzentil allerdings einen Höchstwert von 27.196 aktiven Cloud-Problemen aufwiesen.

Diese Extremwerte sind zwar nicht die Norm, aber sie zeigen, wie stark die Probleme jeden Monat variieren können. Diese Zahlen machen zudem deutlich, dass Sicherheitsteams weder die Zeit noch die Mittel haben, um jedes Problem einzeln zu beheben. Das ist natürlich kein Grund aufzugeben. Es heißt nur, dass es einen besseren Weg geben muss, als immer wieder manuell dieselben Prozesse zur Fehlerbehebung durchzuführen – was mit einem enormen Arbeitsaufwand für die Mitarbeiter verbunden ist.

Wie schon in den Punkten 2, 3 und 5 erläutert, handelt es sich bei den Schwachstellen nicht um exotische Zero-Day-Sicherheitslücken, sondern um gängige Probleme in weitverbreiteter Software und Services wie beispielsweise RDP-Servern oder öffentlich erreichbaren Anmeldeportalen für Administratoren. Können solche Probleme automatisch erkannt und behoben werden, sind nicht nur die SecOps-Prozesse wesentlich resilienter, sondern es werden auch die Sicherheitsteams entlastet, die sich dann um wichtigere Probleme kümmern können, statt von zeitaufwendigen Routineaufgaben aufgehalten zu werden.

Schlussfolgerung und Empfehlungen

Für Sicherheit zur sorgen, ist nicht einfach. Und darin besteht auch schon das ganze Problem. Sicherheitsteams versuchen, die vorhandenen Ressourcen und Daten optimal zu nutzen, aber häufig sind dazu ein umfassender Überblick über die Assets und resiliente Prozesse notwendig, um sicherzustellen, dass neue Probleme nicht persistent werden.

Wenn sie nicht wissen, wo sich eine Schwachstelle befindet, haben sie auch kaum eine Chance, das Problem zu beheben. In vielen Unternehmen werden Cloud- und RDP-Probleme persistent bleiben, aber die Anteile der Schwachstellen und Sicherheitslücken in der Angriffsfläche werden mit steigender Komplexität zunehmen.

Leider nutzen Angreifer auch die kleinste Schwachstelle aus. Für Sicherheitsteams ist es daher hilfreich zu wissen, wie ihre Angriffsfläche aussieht und was Angreifer sehen können. Dann lassen sich die zu behebenden Probleme wesentlich besser identifizieren und priorisieren.

Der Fokus sollte daher nicht zu sehr auf Kennzahlen wie der MTTD (Mean Time to Detect) und MTTR (Mean Time to Respond) liegen. Bei einem Sicherheitsvorfall sind diese Kennzahlen nützlich, aber in Bezug auf die Sicherheit sollte die Bedrohungsprävention höchste Priorität haben. Viel wichtiger ist daher MTTI (Mean Time to Inventory), da nur Assets geschützt werden können, die auch bekannt sind.

Moderne Angriffsflächen sind dynamisch. Ohne einen umfassenden Überblick über die aktuelle Lage und automatisierte Sicherheitsprozesse werden persistente Probleme und nicht verwaltete Assets schnell übersehen. Sicherheitsexperten benötigen aussagekräftige und zuverlässige Daten. Mit einer kontinuierlichen Erkennung und Überwachung können sie dann auch mit modernen, dynamischen Angriffsflächen Schritt halten und neue Schwachstellen zeitnah finden, priorisieren und beheben.

Möchten Sie wissen, wie Angreifer Ihre Angriffsfläche bzw. Ihr Netzwerk sehen? Kontaktieren Sie einen Mitarbeiter von Palo Alto Networks und vereinbaren Sie einen Termin, um sich selbst einen Eindruck zu verschaffen.

Methodik

Xpanse betreibt eine proprietäre Plattform, die kontinuierlich mehr als ein Petabyte pro Tag an Informationen zu allen öffentlich über das Internet zugänglichen Systemen erfasst, um zu ermitteln, wie Angreifer potenzielle Ziele sehen.

Anhand der extern zugänglichen Angriffsfläche weltweit agierender Unternehmen untersuchten und interpretierten Xpanse-Analysten Daten, um Sicherheitsteams zu helfen, ihre Angriffsfläche zu verstehen und Folgendes zu erreichen:

- Quantifizierung und Behebung öffentlich zugänglicher Sicherheitslücken
- Bereitstellung von Benchmarkmetriken zur Angriffsfläche für Sicherheitsteams
- Optimierung der Bedrohungsmodellierung
- Beschreibung der Bedrohungslage für Zielgruppen mit und ohne Technikkenntnissen
- Bereitstellung proaktiver Sicherheitsmaßnahmen

Im Rahmen dieser Analyse hat Xpanse Daten aus dem Jahr 2021 (Anfang März bis Ende September) und dem Jahr 2022 (Anfang Dezember 2021 bis Anfang Juni 2022) von über 100 Mandanten in diversen Branchen ausgewertet. Daten zu den einzelnen Branchen wurden in diesem Bericht nur dann angegeben, wenn Informationen von mindestens sieben Unternehmen aus der jeweiligen Branche vorlagen. Die Beobachtungen zu wichtigen CVEs (Common Vulnerabilities and Exposure) basieren auf den analysierten Daten von Januar und Februar 2022.

Die meisten Kennzahlen in diesem Bericht sind Medianwerte. Das liegt daran, dass es bei globalen Daten zu Internetassets häufig Ausreißer gibt, die den Mittel-/Durchschnittswert für eine Problemkategorie oder Branche stark verzerren. Medianwerte helfen, ein unverzerrtes Bild darzustellen.

Über Cortex Xpanse

Cortex® Xpanse™, eine Plattform für das automatisierte Angriffsflächenmanagement (Attack Surface Management, ASM), erstellt eine vollständige und korrekte Bestandsliste aller über das Internet erreichbaren Ressourcen und Fehlkonfigurationen eines Unternehmens, sodass dieses Sicherheitslücken in seiner externen Angriffsfläche kontinuierlich erfassen, bewerten und reduzieren kann. Zu den Xpanse-Kunden gehören führende Fortune-500-Unternehmen sowie US-Behörden und alle fünf US-Teilstreitkräfte.

paloalto® NETWORKS

Oval Tower, De Entrée 99–197
1101 HE Amsterdam, Niederlande

Telefon: +31 20 888 1883
Vertrieb: +800 7239771
Support: +31 20 808 4600

www.paloaltonetworks.de

cortex_xpanse-attack-surface-threat-report_071222-de