



BENUTZERNAME/PASSWORT

BENUTZERNAME/PASSWORT

APP-SICHERHEIT GEHT VOR

CREDENTIAL STUFFING

EINE SICHERHEITSEPIDEMIE

BENUTZERNAME/PASSWORT

BENUTZERNAME/PASSWORT

BENUTZERNAME/PASSWORT

EINFÜHRUNG

Für das Jahr 2016 hat die Welt einen neuen Rekord für Datenschutzverletzungen verzeichnet und mit mehr als 4,2 Milliarden¹ offengelegten Datensätzen den bisherigen Rekord von 1,1 Milliarden aus dem Jahr 2013 übertroffen. Doch so schlimm 2016 auch war, 2017 dürfte noch schlimmer werden.. Allein in den ersten sechs Monaten des Jahres 2017 wurden 2.227 Verstöße gemeldet, bei denen mehr als 6 Milliarden Datensätze offengelegt und unzählige

Konten gefährdet wurden.² Von all diesen gestohlenen Datensätzen enthält die große Mehrheit Benutzernamen und Passwörter, die laut 2017 Verizon Data Breach Investigations Report in 81 Prozent der mit Hacking in Verbindung stehenden Datenpannen verwendet werden.³ Angesichts der immer größer werdenden Bedenken in Bezug auf die Anwendungs- und Datenintegrität müssen Organisationen dem Identitätsschutz in ihren Sicherheitsstrategien Priorität

verleihen. Tatsächlich könnte die Sicherung der Identität von Benutzern und die Verwaltung ihrer Zugriffsberechtigungen für kritische Geschäftsanwendungen 2017 die größte Herausforderung für Organisationen darstellen.

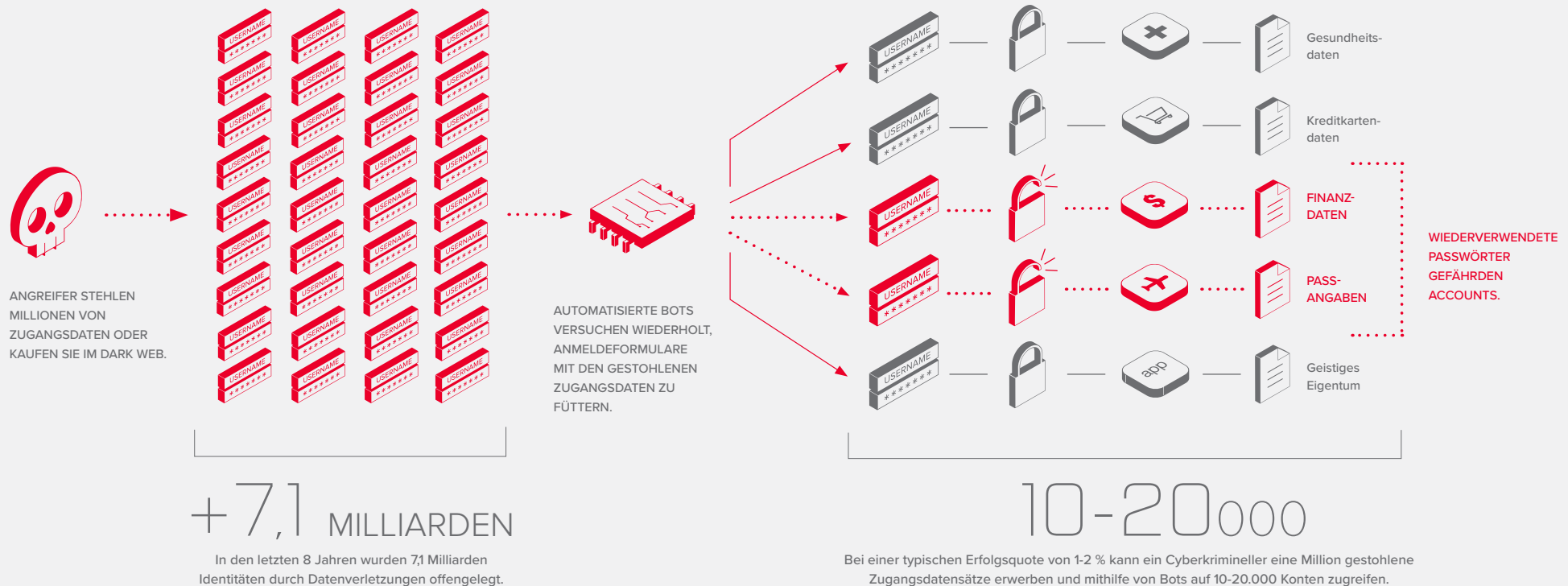
¹ <https://pages.riskbasedsecurity.com/hubfs/Reports/2016%20Year%20End%20Data%20Breach%20QuickView%20Report.pdf>

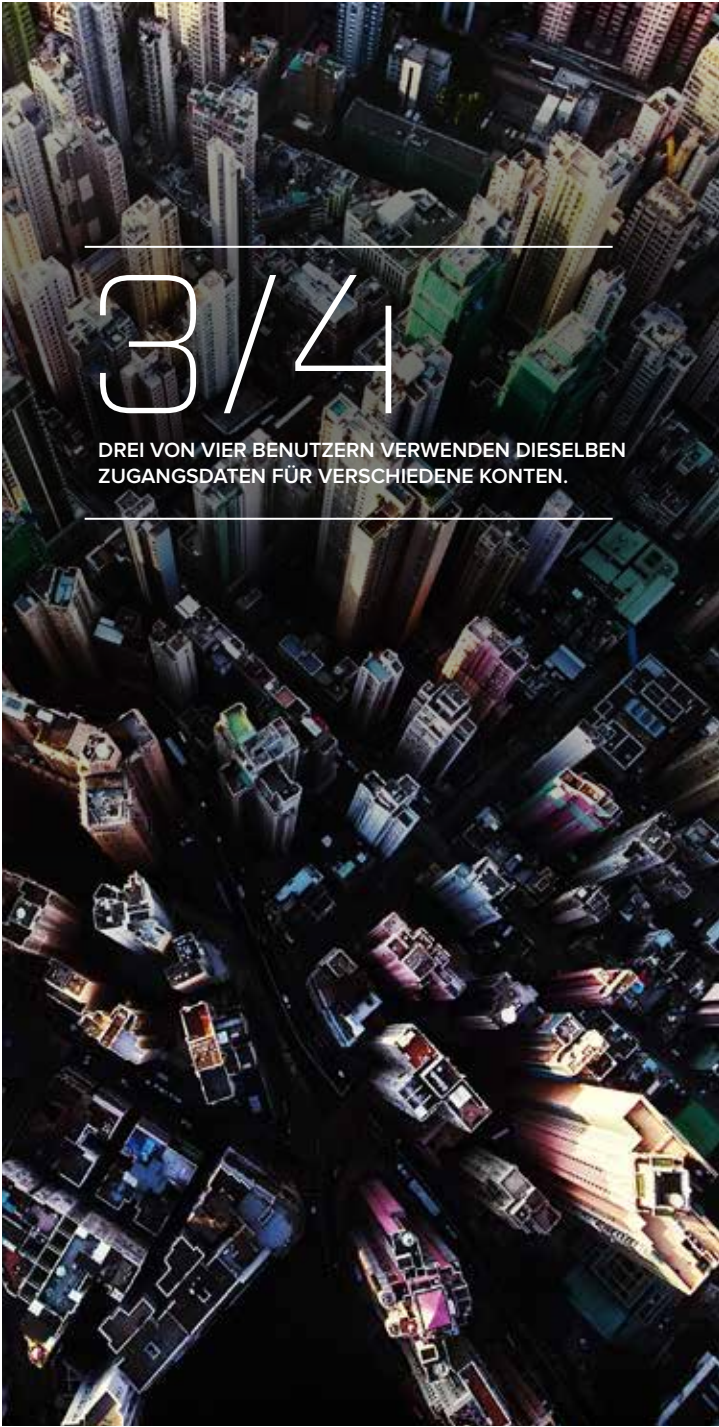
² <https://pages.riskbasedsecurity.com/hubfs/Reports/2017%20MidYear%20Data%20Breach%20QuickView%20Report.pdf>

³ <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/>

ANATOMIE EINES CREDENTIAL-STUFFING-ANGRIFFS

Bei einem Credential-Stuffing-Angriff nutzen Cyberkriminelle gestohlene Zugangsdaten und versuchen wiederholt, Zugriff auf Konten von Firmenbenutzern oder Kunden zu erlangen.





3/4

DREI VON VIER BENUTZERN VERWENDEN DIESELBEN ZUGANGSDATEN FÜR VERSCHIEDENE KONTEN.

DAS PROBLEM DES CREDENTIAL STUFFING

Bei einem Credential-Stuffing-Angriff kaufen Cyberkriminelle gestohlene Benutzernamen und Passwörter im Dark Web. Anschließend versuchen sie mit automatisierten Tools wiederholt, die Login-Felder anderer Websites mit den Zugangsdaten zu füttern, um Zugriff auf Konten von Firmenbenutzern oder Kunden zu erlangen. Wenn das gelingt, nutzt der Angreifer das Konto für betrügerische Zwecke. Die Erfolgsquote beträgt üblicherweise 1 bis 2 Prozent. Das bedeutet, dass ein Cyberkrimineller, der 1 Million gestohlene Zugangsdatensätze erwirbt (die im Dark Web jeweils für Bruchteile eines Cent angeboten werden⁴), in der Regel Zugriff auf 10.000 bis 20.000 Konten erlangen kann.

FAST 17 % ALLER KONTEN WURDEN 2016 NOCH IMMER MIT DEM PASSWORT „123456“ GESICHERT.

Diese Angriffe wären nicht erfolgreich, wenn die Benutzer für jede Website oder Anwendung, auf die sie zugreifen, andere Benutzernamen und Passwörter verwenden würden. Doch fast drei von vier Benutzern machen sich nicht die Mühe, für jedes ihrer vielen Konten eigene Zugangsdaten zu erstellen, sondern verwenden dieselben Zugangsdaten für mehrere Konten.⁵

Tatsächlich kann die Sicherheit Ihrer Organisation noch so stark sein, wenn Ihre Benutzer oder Kunden ihre Passwörter wiederverwenden – und davon können Sie ausgehen –, ist die Wahrscheinlichkeit groß, dass ihre Zugangsdaten bereits gestohlen wurden. Die explosionsartige Zunahme des Diebstahls von Zugangsdaten und die relative Leichtigkeit, mit der Cyberkriminelle mithilfe automatisierter Tools die Kontrolle über Benutzerkonten erlangen können, geben Organisationen berechtigten Anlass zur Sorge um die Sicherheit ihrer Anwendungen und Daten.

Die Frage ist, wie Sie diese Angriffe verhindern oder zumindest entschärfen können.

⁴ https://www.nytimes.com/2016/12/15/technology/hacked-yahoo-data-for-sale-dark-web.html?_r=0

⁵ <https://www.entrepreneur.com/article/246902>

EIN LEITFADEN FÜR DIE BEKÄMPFUNG DES DIEBSTAHLS VON ZUGANGSDATEN

Die schlechte Nachricht zuerst: Es gibt keinen Schalter, den Sie einfach nur umlegen müssen, um Ihre Organisation vor Credential-Stuffing-Angriffen zu schützen. Sie können jedoch verschiedene Maßnahmen ergreifen, um die Wahrscheinlichkeit, Opfer eines Angriffs zu werden, drastisch zu reduzieren. Schulen Sie Ihre Benutzer in der Verwendung sichererer Passwortpraktiken und verbessern Sie gleichzeitig die Sicherheit auf Unternehmensebene.

MITARBEITER UND RICHTLINIEN: SCHULEN, MELDEN, VERSTÄRKEN

Nach der Beschaffung und Nutzung gestohlener Anmeldeinformationen ist Phishing der beste Weg für Cyberkriminelle, an Zugangsdaten für das Credential Stuffing zu gelangen. Durch Schulungen und Fortbildungen können Sie das Bewusstsein Ihrer Mitarbeiter für Phishing schärfen. Auch wenn damit die Gefahr eines erfolgreichen Phishing-Angriffs noch nicht gebannt ist, kann fundiertes Wissen über die Arbeitsweise von Cyberkriminellen den Benutzern helfen, sich selbst und das Unternehmen besser zu schützen.

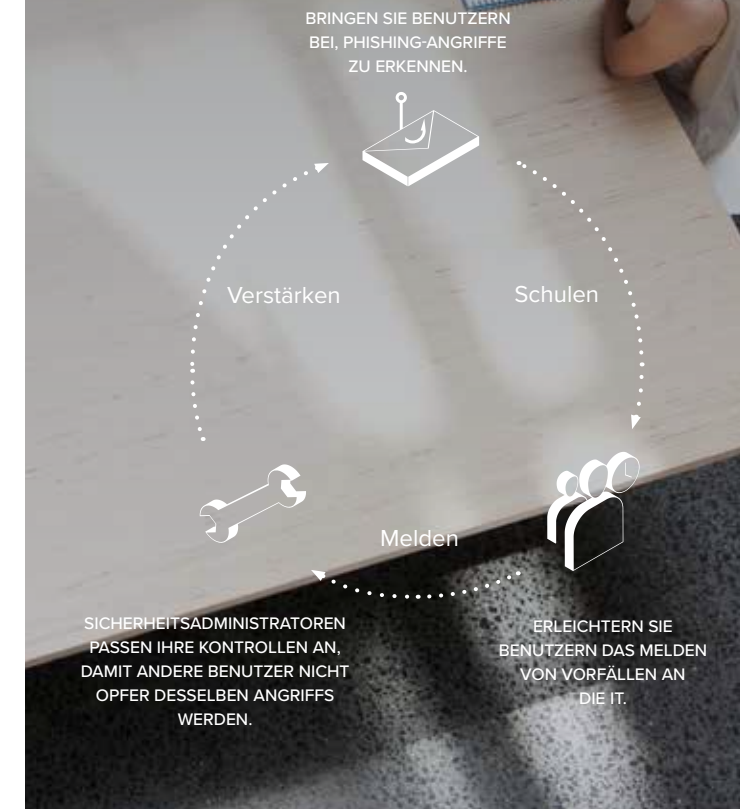
Bringen Sie Ihren Benutzer zunächst einmal bei, Phishing-Angriffe zu erkennen. Sie können Ihre eigenen Tests entwickeln oder einen kostenlosen Online-Test verwenden.⁶ Dann können Sie den Benutzern einige bewährte Verfahren zur Passwortverwaltung an die Hand geben. Vor allem muss Ihren Mitarbeitern klar werden, dass sie ihre Netzwerkzugangsdaten niemals für die Anmeldung bei irgendeiner externen Website verwenden dürfen, weil Cyberkriminelle sonst nach einem erfolgreichen Angriff auf diese Website Zugang zu Ihrem Unternehmensnetzwerk und allen seinen

Anwendungen erhalten könnten. Wenn Sie erfahren, dass Mitarbeiter ihre Firmenzugangsdaten auf anderen Websites verwendet haben, sorgen Sie dafür, dass sie diese unverzüglich ändern. Gehen Sie außerdem davon aus, dass ein Teil Ihrer Benutzer Passwörter mehrfach wiederverwendet, und erzwingen Sie nach einem groß angelegten Datenklau wie dem Yahoo!- oder LinkedIn-Angriff einen Reset sämtlicher Benutzerpasswörter.

Denken Sie daran, dass selbst die am besten geschuldeten Mitarbeiter immer noch menschlich sind und der Diebstahl von Zugangsdaten daher möglich bleibt. Legen Sie Richtlinien fest, die es den Benutzern erleichtern, einen Vorfall sofort der IT zu melden, wenn sie befürchten, dass sie in einer Phishing-E-Mail auf einen Malware-Link geklickt oder ihre Zugangsdaten fälschlicherweise weitergegeben haben. Wenn die Meldung rasch bei der IT eingeht, kann ein Sicherheitsadministrator dabei helfen, das System zu bereinigen, Passwörter zurückzusetzen, andere Mitarbeiter vor dem Betrug zu warnen und vor allem die Sicherheitsmaßnahmen Ihres Unternehmens anzupassen, damit andere Benutzer nicht Opfer desselben Angriffs werden.

⁶ <http://resources.infosecinstitute.com/top-9-free-phishing-simulators/>

WENN DIE IT UMGEHEND
EINE MELDUNG ÜBER EINEN
VORFALL ERHÄLT, KANN SIE DIE
SICHERHEITSMASSNAHMEN
ANPASSEN, DAMIT ANDERE
BENUTZER NICHT OPFER
DESSELBEN ANGRIFFS WERDEN.



TECHNOLOGIE: FÜR JEDEN ANWENDUNGSFALL DIE PASSENDE VERTEIDIGUNG

Beim Aufbau Ihrer Anwendungssicherheitsstrategie zur Abwehr von Credential-Stuffing-Angriffen müssen Sie zwei Benutzertypen berücksichtigen: Ein Mitarbeiter eines Konzerns wird – begeistert oder widerwillig – auch aufwändigere Prozesse wie die Multifaktor-Authentifizierung (MFA) umsetzen. Ein E-Commerce- oder Einzelhandelskunde hingegen dürfte Maßnahmen, die den Anmeldevorgang komplizieren, deutlich weniger bereitwillig tolerieren. Sie können einige Schritte unternehmen, um sowohl engagierte Mitarbeiter als auch eher gelegentliche Benutzer zu schützen.

Sichern und verschlüsseln

Eine robuste Web Application Firewall (WAF) ist Ihre erste Verteidigungslinie gegen Credential-Stuffing-Angriffe. Eine moderne, komplett ausgestattete WAF kann hochentwickelte Bot-Erkennung und -Vorbeugung bieten. Das ist

entscheidend, weil die meisten Angriffe mit automatisierten Programmen geführt werden. Durch die Analyse von Merkmalen wie der IP-Adresse, der Uhrzeit und der Verbindungsversuche pro Sekunde kann eine WAF Ihrem Sicherheitsteam helfen, Anmeldeversuche zu erkennen, die nicht über einen Browser erfolgen. Erwünschte Bots (z. B. Suchmaschinen-Bots) lassen sich dank der Signaturprüfung Ihrer WAF ganz einfach in die Whitelist aufnehmen, sodass sie Zugang zu Ihrer Website erhalten.

Außerdem kann eine WAF Benutzernamen und Passwörter mit einer bekannten Liste gestohlener Zugangsdaten vergleichen, um die Erkennung böswilliger Anmeldeversuche weiter zu vereinfachen. Darüber hinaus ermöglicht Ihre WAF dem Sicherheitsteam, potenzielle Credential-Stuffing-Angriffe anhand der Anzahl fehlgeschlagener Anmeldeversuche in einem bestimmten Zeitraum frühzeitig zu erkennen.

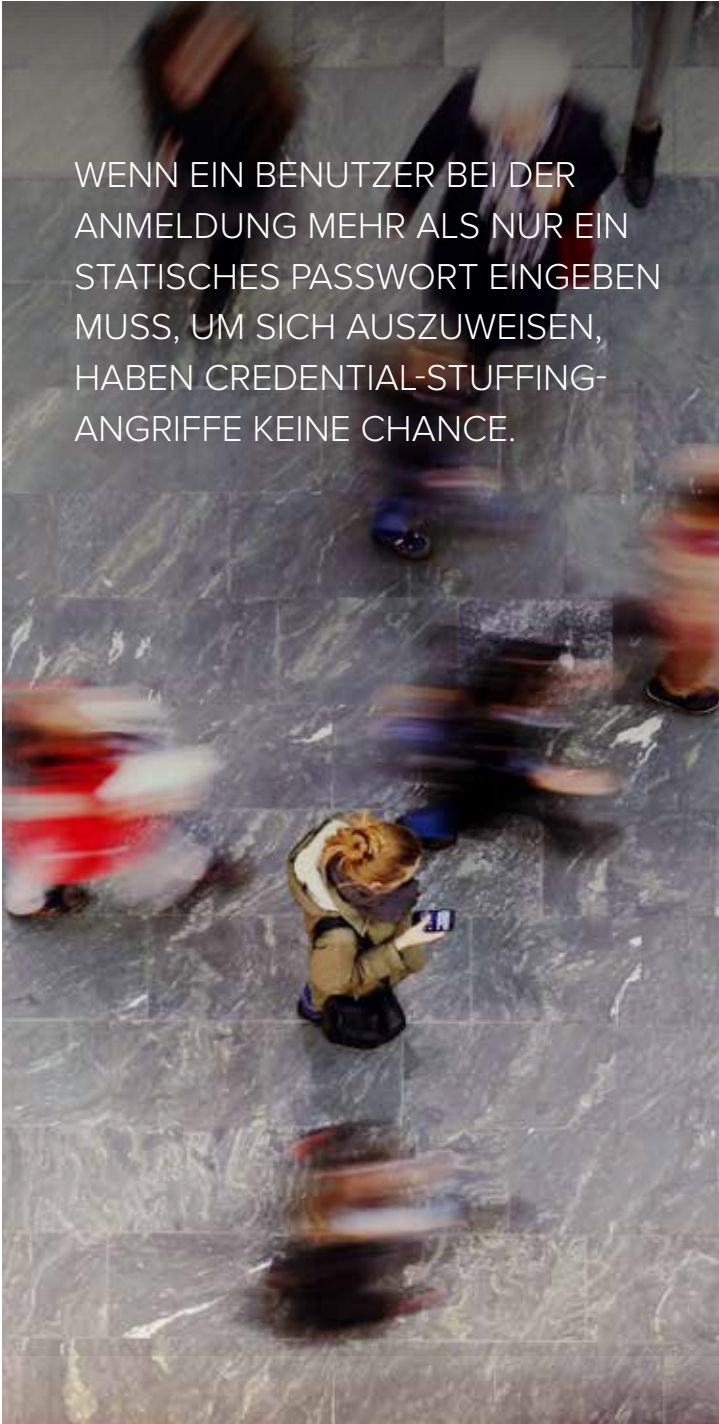
Für eine proaktive Verteidigung sollten Sie Ihre WAF so einstellen, dass sie nicht mehr als x Anmeldeversuche innerhalb von x Sekunden zulässt. Das kann einen Angriff von außen verlangsamen und Ihnen Zeit geben, Ihre Sicherheitseinstellungen anzupassen.

Eine weitere Maßnahme zur Verkleinerung Ihrer Angriffsfläche besteht darin, Verbindungen aus bestimmten IP-Adressbereichen oder geografischen Regionen herauszufiltern. Sobald Sie einen Angreifer erkannt haben, sollten Sie "böse" IP-Adressen und Gerätekennungen anderen Sicherheitslösungen über einen Threat-Feed zur Verfügung stellen, damit diese solche Aktivitäten gegebenenfalls erkennen und blockieren können. Denken Sie aber daran, dass dies meist nur eine sehr kurzfristige Lösung ist, da viele Bot-Betreiber die IP-Adressen immer wieder wechseln.

WAF-SCHUTZ

Eine moderne, komplett ausgestattete WAF kann hochentwickelte Bot-Erkennung und -Vorbeugung bieten. Das ist entscheidend, weil die meisten Angriffe mit automatisierten Programmen geführt werden.





WENN EIN BENUTZER BEI DER ANMELDUNG MEHR ALS NUR EIN STATISCHES PASSWORT EINGEBEN MUSS, UM SICH AUSZUWEISEN, HABEN CREDENTIAL-STUFFING-ANGRIFFE KEINE CHANCE.

Die dynamische Verschleierung von Eingabemasken kann einem Angreifer das Aufspüren des Anmeldeformulars Ihrer Website erheblich erschweren. Statt die Eingabefelder mit erkennbaren Bezeichnungen wie „passwd“ oder „usrnme“ zu versehen, wandelt die dynamische Feldverschleierung die Feldnamen in lange, undurchschaubare und ständig wechselnde Zeichenfolgen um und macht es dem Bot eines Angreifers damit unmöglich, die gestohlenen Zugangsdaten in die richtigen Felder einzufügen.

Schließlich können Sie auch die Datenübertragungen des Browsers und Ihrer Anwendungen verschlüsseln. Damit sind die von den Benutzern verschickten Informationen geschützt und eventuell abgefangene Daten wertlos. Als zusätzliche Sicherheitsmaßnahme können Sie dafür sorgen, dass die Formularparameter auf Client-Seite verschlüsselt werden. Dadurch wären automatisierte Credential Stuffing Tools gezwungen, die Seite korrekt auszuführen, damit die Formularfelder verschlüsselt und die korrekten Secure Channel Cookies versendet werden. Wenn die Bots unverschlüsselte Zugangsdaten übermitteln, wird Ihr Sicherheitsteam durch einen Systemalarm darüber informiert, dass möglicherweise gerade ein Credential-Stuffing-Angriff stattfindet.

Autorisierung steuern

Während eine WAF erheblich zur Abwehr von Credential-Stuffing-Angriffen beiträgt, können Sie die Angriffsfläche der Anwendung durch die Einführung Token-basierter Autorisierung noch weiter verringern. Dieses so genannte OAuth-Verfahren (Open Authorization) ermöglicht es den Benutzern, auf eine Anwendung zuzugreifen, ohne ihre Zugangsdaten an

die Anwendung selbst zu übermitteln. Nachdem sich der Benutzer einmal bei einer Website wie Facebook, Google, Microsoft Azure oder auch Ihrem eigenen Autorisierungsserver identifiziert hat, wird ein einmaliges, kurzlebiges Zugriffstoken für die Anwendung ausgestellt, mit der er sich verbindet. Die Anwendung benötigt dann keine weiteren Zugangsdaten und ist für den Benutzer damit höchst komfortabel. Außerdem sorgt der „Autorisierungsserver“ als vertrauenswürdige Quelle für eine sichere Authentifizierung, was die Wirksamkeit von Credential-Stuffing-Angriffen erheblich einschränkt.

Auch für den Schutz Ihrer APIs vor Credential-Stuffing-Angriffen ist die Token-basierte Autorisierung eine großartige Lösung. Da APIs von Haus aus für den programmgesteuerten Zugriff (von Software auf Software) ausgelegt und deshalb ein bevorzugtes Ziel dieser Angriffe sind, ist die Auslagerung der Autorisierung auf einen OAuth-Server hier besonders wichtig. Für den API-Zugriff per OAuth müssen die Entwickler keine Zugangsdaten in die Anwendung einprogrammieren, was die Sicherheit der API erhöht. Zudem lassen sich Token so programmieren, dass sie nicht nur den Vollzugriff erlauben oder verweigern, sondern auch verschiedene Berechtigungsebenen unterstützen.

Die meisten Unternehmen haben mehrere Anwendungen mit jeweils eigenen Benutzeranmeldungen oder APIs. Und da OAuth an sich keine native Sicherheit bietet, besteht die Gefahr einer unsicheren Implementierung.

Dieses Risiko können Sie jedoch minimieren, indem Sie den Zugriff auf Anwendungen, Netzwerkressourcen

und APIs mit einem zentralen Zugangsgateway verwalten, das die OAuth-Autorisierung für die Anwendung rückübersetzen kann. Auf diese Weise können Sie alle Zugriffsentscheidungen von einem einzigen Punkt aus steuern, das Risiko einer unsicheren OAuth-Implementierung minimieren und beim Aufbau des Autorisierungsframeworks wertvolle Entwicklungszeit einsparen.

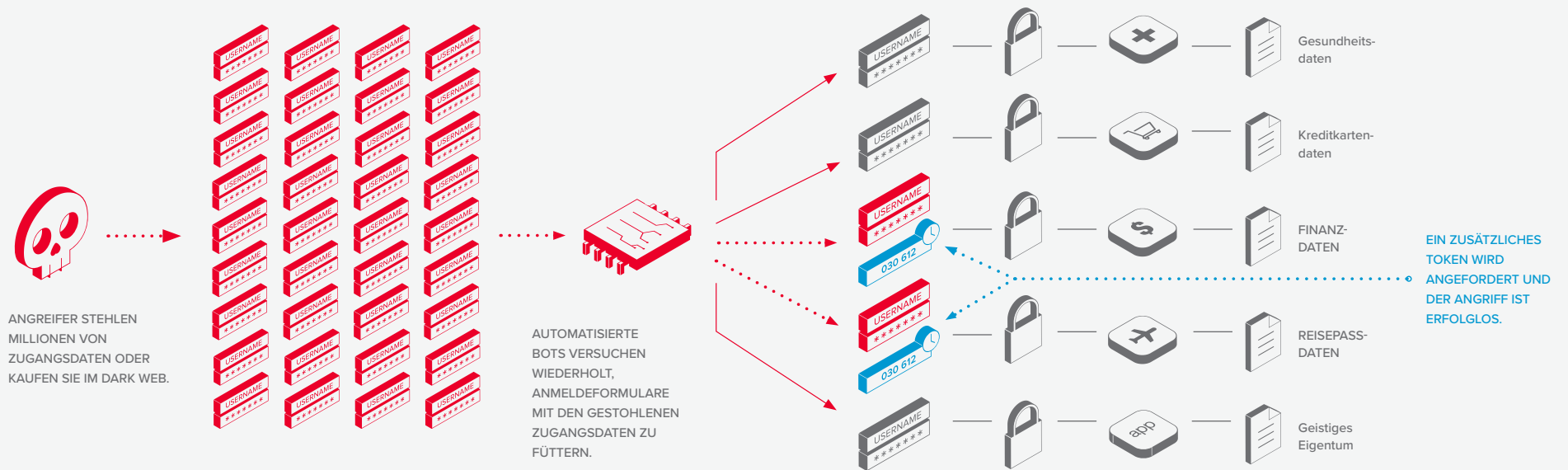
Insbesondere für Mitarbeiter in Unternehmen bietet die Einrichtung eines sicheren Zugangsgateways noch weitere Sicherheitsvorteile. Indem Sie alle Authentifizierungs- und

Zugriffsanfragen über ein einziges leistungsstarkes Gateway abwickeln, können Sie eine einheitliche Plattform für Ihre Benutzer bereitstellen und so die Gefahr verringern, dass diese auf Phishing-Versuche hereinfliegen. Ein solches Gateway beinhaltet auch weitere wichtige Bestandteile einer Identitätssicherheitslösung wie Single Sign-On und risiko-basierte MFA. Denn auch wenn alle Authentifizierungs- und Zugriffsanfragen über das zentrale Zugangsgateway eingehen, sind doch nicht alle Anfragen gleich. Authentifizierungsanforderungen und Zugriffsentscheidungen können von

verschiedenen Risikofaktoren abhängen, etwa von der Rolle des Benutzers, dem Gerät, dem geografischen Standort, der Tageszeit und nicht zuletzt von der Vertraulichkeit der Daten innerhalb der Anwendung. Kommen mehrere Risikofaktoren zusammen, kann das Gateway die Identitätsprüfung um einen zweiten oder gar einen dritten Faktor erweitern, bevor es dem Benutzer Zugang gewährt. Wenn ein Benutzer bei der Anmeldung mehr als nur ein statisches Passwort eingeben muss, um sich auszuweisen, haben Credential-Stuffing-Angriffe keine Chance.

MEHRFAKTOR-AUTHENTIFIZIERUNG

Zum Schutz vor einem Credential-Stuffing-Angriff muss ein Benutzer mehr als nur sein statisches Passwort eingeben, um sich auszuweisen.



IDENTITÄTSSICHERHEIT = UNTERNEHMENSSICHERHEIT

Da Identitäten mehr und mehr zum bevorzugten Ziel von Cyberkriminellen werden, müssen Unternehmen erkennen, dass die Identitäts- und Zugriffssicherheit für die Integrität ihrer Anwendungen und Daten entscheidend ist. Mit einer Kombination aus Benutzerschulungen, starken und einheitlichen Unternehmensrichtlinien, einer robusten Web Application Firewall und einem zentralen Authentifizierungs- und Autorisierungsgateway können Organisationen die immer mächtigeren und hartnäckigeren Credential-Stuffing-Angriffe von heute verhindern oder zumindest entschärfen.

Weitere Informationen zum Anwendungsschutz finden Sie unter f5.com/security.



EINE UMFASSENDE SICHERHEITS-
STRATEGIE KANN DIE MÄCHTIGEN
UND HARTNÄCKIGEN CREDENTIAL-
STUFFING-ANGRIFFE VON HEUTE
VERHINDERN ODER ZUMINDEST
ENTSCHÄRFEN.



BENUTZERSCHULUNG



EINHEITLICHE
UNTERNEHMENSRICHTLINIEN



WEB APPLICATION FIREWALL



ZENTRALES AUTHENTIFIZIERUNGS-
UND AUTORISIERUNGSGATEWAY



APP-SICHERHEIT GEHT VOR

Ständig verfügbare und vernetzte Anwendungen können Ihr Unternehmen stärken und transformieren – sie können aber auch die Schwachstelle sein, die den Zugang zu Daten hinter Ihrer Firewall ermöglichen. Da die meisten Angriffe auf der App-Ebene stattfinden, schützen Sie Ihre geschäftlichen Funktionen am besten, indem Sie die Apps schützen, die diese Funktionen bereitstellen.

