Cisco 2018
Annual Cybersecurity Report

Inhaltsverzeichnis

Zusammenfassung

Stellen Sie sich vor, wir könnten in die Zukunft sehen und wüssten somit, wann ein Angriff bevorsteht. Dann könnte dieser aufgehalten oder zumindest die Auswirkungen auf ein Minimum reduziert werden, und man hätte die Gewissheit, dass alle wichtigen Systeme geschützt sind. Tatsache ist: Wir *können* in die Zukunft sehen. Es gibt viele – und eindeutige – Hinweise.

Gegner und staatliche Akteure verfügen über die nötigen Kenntnisse und Tools, um kritische Infrastrukturen und Systeme zu zerstören und ganze Regionen lahmzulegen. Immer wieder gelangen neue, zerstörerische Angriffe an die Öffentlichkeit, wie dies im vergangenen Jahr z. B. in der Ukraine aber auch im Rest der Welt der Fall war. Einige Sicherheitsexperten glauben dennoch, dass für ihre Unternehmen kein Risiko besteht, weil ihr Markt, ihre Region oder ihre Technologie bisher nicht betroffen war.

Wer diese scheinbar weit entfernten Kampagnen nicht beachtet oder von den täglichen Auseinandersetzungen mit Angreifern zu sehr vereinnahmt wird, der übersieht vielleicht, mit welcher Geschwindigkeit und in welchem Ausmaß sich die Gegner und ihre Angriffsstrategien weiterentwickeln.

Seit Jahren warnt Cisco bereits vor einer Eskalation der cyberkriminellen Aktivitäten weltweit. Im Cisco Annual Cybersecurity Report 2018 finden Sie Daten und Analysen der Cisco Bedrohungsforscher sowie von einigen unserer Technologiepartner über das beobachtete Angreiferverhalten in den vergangenen 12 bis 18 Monaten. Viele der im Bericht behandelten Themen lassen sich in drei allgemeinen Feststellungen zusammenfassen:

1. **Die Raffinesse und Effektivität von Malware nimmt immer mehr zu.**

   Die Malware-Entwicklung (Seite 6) gehörte 2017 zu den bedeutendsten Entwicklungen in der Bedrohungslandschaft. Netzwerkbasierte Ransomware-Kryptowürmer machen den menschlichen Faktor beim Start von Ransomware-Kampagnen praktisch überflüssig. Einigen Gegnern geht es dabei nicht um das Lösegeld, sondern vielmehr um die Auslöschung von Systemen und Daten, wie dies bei Nyetya, einer als Ransomware getarnten Wiper-Malware, der Fall war (siehe Seite 6). Malware, die sich eigenständig ausbreitet, ist gefährlich und hat den Cisco Bedrohungsforschern zufolge das Potenzial, das Internet zum Erliegen zu bringen.

2. **Die Ausweichmanöver der Gegner werden immer ausgeklügelter, und sie nutzen Cloud-Services und andere Technologien mit einem ursprünglich legitimen Zweck, um Schaden zu verursachen.**

   Es entstehen zum einen immer mehr Bedrohungen, die **auch fortschrittliche Sandboxing-Umgebungen umgehen können** (Seite 22). Zum anderen kommen vermehrt **Verschlüsselungstechnologien zum Einsatz, um unentdeckt zu bleiben** (Seite 9). Verschlüsselungstechniken sollen die Sicherheit erhöhen, aber sie sind auch eine wirkungsvolle Methode für Angreifer zum Verbergen von Command-and-Control-Aktivitäten (C2). So haben diese mehr Zeit, um Angriffe durchzuführen und Schaden anzurichten.

   Cyberkriminelle übernehmen auch **C2-Kanäle, die auf legitime Internetservices** wie Google, Dropbox, und GitHub setzen (siehe Seite 24). Das macht es fast unmöglich, den Malware-Datenverkehr zu identifizieren.

   Viele Angreifer starten jetzt auch **mehrere Kampagnen von einer einzelnen Domain aus** (Seite 26), um möglichst viel Kapital daraus zu schlagen. Auch Infrastrukturressourcen, wie z. B. E-Mail-Adressen von sich registrierenden Personen, ASNs (autonome Systemnummern) und Namenserver, werden dafür genutzt.

3. **Nicht verteidigte Sicherheitslücken, die heute oftmals durch die Erweiterung des Internet of Things (IoT) und die Nutzung von Cloud-Services entstehen, sind das Ziel vieler Angreifer.**

   Neue IoT-Geräte werden derzeit in einem rasenden Tempo bereitgestellt. Dabei wird aber der Sicherheit dieser Systeme oft kaum Beachtung geschenkt. **Werden IoT-Geräte nicht regelmäßig gepatcht und überwacht,** stellen Sie für Angreifer eine willkommene Möglichkeit dar, um ins Netzwerk einzudringen (Seite 34). Organisationen mit angriffsgefährdeten IoT-Geräten wirken laut Forschungsergebnissen auch häufig **nicht motiviert, die Problembehebung zu beschleunigen** (Seite 42). Noch schlimmer: In den IT-Umgebungen dieser Unternehmen gibt es womöglich noch viel mehr anfällige IoT-Geräte, von denen sie gar nichts wissen.

Inzwischen breiten sich **IoT-Botnets mit dem** Wachstum des IoT aus und werden auch immer ausgereifter und automatisierter. Diese Situation nutzen Angreifer aus, um fortschrittliche DDoS-Angriffe (Distributed Denial of Service) zu starten (Seite 31).

Auch von der Tatsache, dass Sicherheitsteams **Schwierigkeiten mit dem Schutz von IoT- und Cloud-Umgebungen haben, profitieren die Angreifer**. Ein Grund dafür ist der mangelnde Überblick, wer genau für den Schutz dieser Umgebungen zuständig ist (siehe Seite 42).

Empfehlungen für Verteidiger

Die Frage lautet heute nicht, ob, sondern wann eine Organisation einem Cyberangriff ausgesetzt sein wird. Daher ist es für die Unternehmen wichtig, vorbereitet zu sein und sich von dem Angriff schnell wieder zu erholen. Ergebnisse der **Cisco Security Capabilities Benchmark Study 2018** – die Einblicke in die Sicherheitspraktiken von über 3.600 Befragten in 26 Ländern gewährt – zeigen, dass es für die Verteidiger viele Herausforderungen zu bewältigen gibt (siehe Seite 46).

Durch strategische Sicherheitsverbesserungen und die Verfolgung von gängigen Best-Practices können Risiken reduziert, Angreifer aufgehalten und mehr Einblicke in die Bedrohungslandschaft gewährt werden. Wir empfehlen:

- die Implementierung skalierbarer Tools für die erste Verteidigungslinie, wie z. B. Cloud-Security-Plattformen.
- die Einhaltung von Unternehmensrichtlinien und Praktiken für das Patching von Anwendungen, Systemen und Appliances.
- die Bereitstellung von Netzwerksegmentierung zur Reduzierung von Outbreaks.
- die Einführung von Tools der nächsten Generation zur Überwachung von Endgerätprozessen.
- den Zugriff auf aktuelle und genaue Threat-Intelligence-Daten und Prozesse zur Einbindung dieser Daten in die Sicherheitsüberwachung.
- die Durchführung detaillierter und fortschrittlicher Analysen.
- die Prüfung und Übung von Sicherheitsverfahren.
- regelmäßige Daten-Backups und Prüfung der Wiederherstellungsprozesse, was wichtige Prozesse im Umgang mit schnellen, netzwerkbasierten Ransomware-Würmern und anderen schädlichen Cyberangriffen darstellt.
- die Wirksamkeitsprüfung von Sicherheitstechnologien von Drittanbietern zur Reduzierung des Risikos von Angriffen gegen die Lieferkette.
- die Durchführung von Sicherheitsscans von Mikroservices, Cloud-Services und Systemen für das Anwendungsmanagement.
- die Prüfung der Sicherheitssysteme sowie der Einsatzmöglichkeiten von SSL-Analytik und (sofern möglich) SSL-Entschlüsselung.

Für die Abwehr von Angriffen sollte auch der Einsatz fortschrittlicher Sicherheitstechnologien in Erwägung gezogen werden, die Funktionen für maschinelles Lernen und künstliche Intelligenz bieten. Die Malware kommuniziert versteckt über den verschlüsselten Web-Datenverkehr und Netzwerkeindringlinge übertragen vertrauliche Daten mithilfe der geschäftlichen Cloud-Systeme. Um zu verhindern, dass die Verschlüsselung zur Tarnung betrügerischer Aktivitäten genutzt wird, oder um diese Nutzung aufzudecken, benötigen die Sicherheitsteams effektive Tools.

Über den Report

Der ***Cisco Annual Cybersecurity Report 2018*** stellt unsere aktuellen Erkenntnisse zu den Fortschritten in der Sicherheitsbranche vor, die Unternehmen und Endnutzer dabei unterstützen, sich vor Angriffen zu schützen. Wir untersuchen auch die Techniken und Strategien, die Angreifer nutzen, um diese Abwehrmaßnahmen zu umgehen und dabei unentdeckt zu bleiben.

Darüber hinaus geben wir einen Überblick über die wichtigsten Ergebnisse der **Cisco Security Capabilities Benchmark Study 2018**, in deren Rahmen wir den Sicherheitsstatus von Unternehmen sowie deren Sicht auf die Effektivität ihrer Maßnahmen zur Abwehr von Cyberangriffen untersuchen.

Teil I:
Die Bedrohungslandschaft

Teil I: Die Bedrohungslandschaft

Die Raffinesse und Effektivität von Malware nimmt immer mehr zu. Die steigende Anzahl und Vielfalt an Malware-Typen und -Familien erzeugt weiterhin Chaos in der Bedrohungslandschaft, denn sie erschweren die Bedrohungseindämmung durch die Verteidiger.

DIE MALWARE-ENTWICKLUNG

Eine der wichtigsten Entwicklungen in der Bedrohungslandschaft im Jahr 2017 war die der Ransomware. Netzwerk-basierte Ransomware-Würmer machen den menschlichen Faktor beim Start von Ransomware-Kampagnen praktisch überflüssig. Einigen Gegnern geht es dabei nicht um das Lösegeld, sondern um die Zerstörung von Systemen und Daten. Wir erwarten im kommenden Jahr weitere ähnliche Aktivitäten.

Die Bedrohung ist real: 2018 lauern neue, sich eigenständig verbreitende, netzwerkbasierte Bedrohungen

2017 wurden wir von einer Ransomware-Welle überrollt – und das obwohl diese Welle sogar vorhergesagt wurde. Im März 2016 begegneten wir der SamSam-Kampagne[1] – dem ersten groß angelegten Angriff, der Netzwerkvektoren zur Verbreitung von Ransomware nutzte und dadurch den Benutzer für den Infektionsprozess überflüssig machte. Danach war den Cisco Bedrohungsforschern klar, dass es nur noch eine Frage der Zeit war, bis es Angreifern gelingen würde, diese Technik zu automatisieren. Die Angreifer erweiterten den Wirkungsgrad ihrer Malware sogar noch, indem sie sie mit „wurmähnlichen" Funktionen kombinierten, um möglichst viel Schaden anzurichten.

Diese Entwicklung ging schnell voran. Im Mai 2017 dann WannaCry – ein Ransomware-Kryptowurm, der sich wie ein Lauffeuer im Internet ausbreitete.[2] Für seine Verbreitung nutzte er eine Sicherheitslücke von Microsoft Windows namens EternalBlue, die von der Hackergruppe Shadow Brokers Mitte April 2017 offenbart wurde.

Die WannaCry-Erpresser haben zum Zeitpunkt des Wallet-Cash-out 143.000 US-Dollar an Bitcoin-Zahlungen kassiert. Anhand der Dauer des Vorfalls und der Wertzunahme der Bitcoins, die mit einen ursprünglichen Gesamtwert von 93.531 US-Dollar in die Wallets eingezahlt wurden, schätzen Cisco Bedrohungsforscher, dass ungefähr 312 Lösegeldzahlungen geleistet wurden. Zum Vergleich: Als das Exploit-Kit Angler aktiv war, wurden damit ca. 100 Mio. US-Dollar pro Jahr eingenommen, was dem Umsatz eines globalen Unternehmens entspricht.

WannaCry verfolgte nicht nach, wem durch die Verschlüsselung Schäden entstanden und welche betroffenen Benutzer Zahlungen leisteten. Auch die Anzahl der Benutzer, die nach Eingang der Zahlungen Entschlüsselungsschlüssel erhielten, ist nicht bekannt. (WannaCry breitet sich immer noch aus und Benutzer zahlen Lösegelder, leider umsonst.) Da WannaCry als Ransomware finanziell weniger erfolgreich ist, glauben die US-Regierung und viele Sicherheitsforscher, dass die Lösegeldkomponente lediglich ein Deckmantel für den tatsächlichen Zweck von WannaCry ist, nämlich die Auslöschung von Daten.

Im Juni 2017 erschien Nyetya (auch bekannt als NotPetya) auf der Bildfläche.[3] Diese Wiper-Malware war ebenfalls als Ransomware getarnt und nutzte die Schwachstelle der Remote-Codeausführung, auch „EternalBlue" genannt, und die Schwachstelle der Remote-Codeausführung „EternalRomance" (die ebenfalls von den Shadow Brokers veröffentlicht wurde) sowie andere Vektoren, welche die Erfassung von Anmeldedaten erlaubten.

1 *SamSam: The Doctor Will See You, After He Pays the Ransom,* Cisco Talos-Blog, März 2016: blog.talosintelligence.com/2016/03/samsam-ransomware.html.
2 *Player 3 Has Entered the Game: Say Hello to 'WannaCry,'* Cisco Talos-Blog, Mai 2017: blog.talosintelligence.com/2017/05/wannacry.html.
3 *New Ransomware Variant 'Nyetya' Compromises Systems Worldwide,* Cisco Talos-Blog, Juni 2017: blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html.

Das geschah aber unabhängig von der Shadow Broker-Veröffentlichung.[4] Nyetya verbreitete sich über Software-Updatesysteme eines Steuer-Softwarepakets, das bei mehr als 80 Prozent der Unternehmen in der Ukraine im Einsatz war und auf über 1 Million Computern installiert war.[5] Die ukrainische Cyberpolizei bestätigte, dass mehr als 2.000 ukrainische Unternehmen betroffen waren.[6]

Bevor Malware sich wie heute eigenständig ausbreiten konnte, wurde sie auf die folgenden drei Arten eingeschleust: als Drive-By-Download, per E-Mail oder über physische Medien, wie z. B. ein schädliches USB-Speichergerät. Alle Methoden erforderten aber irgendeine Form menschlichen Eingriffs, damit ein Gerät oder System sich überhaupt mit Ransomware infizierte. Da die Angreifer jetzt neue Angriffsvektoren nutzen, benötigen sie lediglich eine nicht gepatchte, aktive Workstation, um eine netzwerkbasierte Ransomware-Kampagne zu starten.

Einige Sicherheitsexperten betrachten Würmer zwar als eine veraltete Bedrohungsart, weil die Zahl wurmähnlicher CVEs (Common Vulnerabilities and Exposures) zurückgegangen ist und sich die Sicherheitsprodukte allgemein verbessert haben. Allerdings ist die sich eigenständig ausbreitende Malware nicht nur eine relevante Gefahr, sie hat laut Cisco Bedrohungsforschern auch das Potenzial, das ganze Internet lahmzulegen. WannaCry und Nyetya sind nur ein Vorgeschmack auf das, was noch kommt, deshalb sollten Verteidiger auf der Hut sein.

WannaCry und Nyetya hätten verhindert oder ihre Auswirkungen abgemildert werden können, wenn mehr Organisationen grundlegende Best-Practices für die Sicherheit angewendet hätten, etwa das Patching von Schwachstellen, die Festlegung geeigneter Prozesse und Richtlinien für die Reaktion auf Vorfälle und der Einsatz von Netzwerksegmentierung.

Weitere Tipps zur richtigen Reaktion auf automatisierte netzwerkbasierte Ransomware-Würmer können Sie im Cisco Talos-Blog *Back to Basics: Worm Defense in the Ransomware Age* nachlesen.

Sicherheitsschwachstelle: die Lieferkette

Die Nyetya-Kampagne war auch einer von vielen Angriffen gegen die Lieferkette, welche die Cisco Bedrohungsforscher 2017 beobachteten. Ein Grund, weshalb Nyetya so viele Systeme so schnell infizieren konnte, ist die Tatsache, dass Benutzer automatische Software-Updates nicht als Sicherheitsrisiko betrachteten oder in einigen Fällen nicht einmal bemerkten, dass sie schädliche Updates empfingen.

Bei einem weiteren derartigen Angriff im September 2017 waren die Download-Server beteiligt, die von einem Softwarehersteller zur Verteilung eines legitimen Softwarepakets namens CCleaner genutzt wurden.[7] CCleaner-Binärdateien, die eine Backdoor für Trojaner enthielten, wurden mit einem gültigen Zertifikat signiert und ließen den Benutzer in dem Glauben, dass die verwendete Software sicher war. Das Ziel der Akteure hinter dieser Kampagne waren große Technologieunternehmen, die diese Software legitim oder als Teil ihrer Schatten-IT nutzten.

Die Geschwindigkeit und Komplexität von Lieferkettenangriffen scheint zuzunehmen. Sie können Computer massiv beeinträchtigen und Monate oder sogar Jahre überdauern. Verteidiger sollten sich der potenziellen Risiken bewusst sind, wenn sie Software und Hardware von Organisationen nutzen, die keinen zuverlässigen Sicherheitsstatus vorweisen können. Suchen Sie nach Herstellern, die Informationen zu CVEs herausgeben, schnell auf Schwachstellen reagieren und konsequent dafür sorgen, dass ihre Build-Systeme nicht kompromittiert werden können. Außerdem sollten sich Benutzer Zeit nehmen, neue Software vor dem Herunterladen zu scannen, um sicherzustellen, dass sie keine Malware enthält.

Die Netzwerksegmentierung von Software, die nicht durch umfassende Sicherheitspraktiken gestützt ist, kann dabei helfen, Schäden aus Lieferkettenangriffen einzudämmen und zu verhindern, dass sie sich in der gesamten Organisation ausbreiten.

4 Ibid.
5 *Ukraine scrambles to contain new cyber threat after 'NotPetya' attack,* von Jack Stubbs und Matthias Williams, Reuters, Juli 2017: reuters.com/article/us-cyber-attack-ukraine-backdoor/ukraine-scrambles-to-contain-new-cyber-threat-after-notpetya-attack-idUSKBN19Q14P.
6 *The MeDoc Connection,* Cisco Talos-Blog Juli 2017: blog.talosintelligence.com/2017/07/the-medoc-connection.html.
7 *CCleaner Command and Control Causes Concern,* Cisco Talos-Blog, September 2017: blog.talosintelligence.com/2017/09/ccleaner-c2-concern.html.

Die Bedeutung der Integrität für das Threat-Intelligence-Reporting

Alle Organisationen, die Kunden oder der Öffentlichkeit Bedrohungsinformationen über beliebige Kanäle mitteilen, sollten Richtlinien anwenden, um die Korrektheit der Berichte sicherzustellen. Selbst wenn nicht alle Fakten eindeutig sind, können Organisationen doch weitergeben, was sie wissen und Spekulationen außen vor lassen. Aber richtige Informationen sind wichtiger als schnelle Informationen.

Als die Umstände der WannaCry-Kampagne im Mai 2017 bekannt wurden, herrschte innerhalb der Security-Community zunächst Unklarheit darüber, wie der Ransomware-Wurm in Systeme eindringen konnte. Mehrere Organisationen im öffentlichen und privaten Sektor meldeten, dass der Angriff aus einer Phishing-Kampagne und einem schädlichen E-Mail-Anhang hervorging. Tatsächlich suchte die netzwerkbasierte Bedrohung aber nach anfälligen, öffentlichen SMB-Ports (Server Message Block) von Microsoft Windows und infizierte diese.

Cisco Bedrohungsforscher alarmierten umgehend die Security-Community, dass die E-Mails, die ihrer Meinung nach mit der WannaCry-Kampagne in Zusammenhang standen, wahrscheinlich Spam-Mails des Necurs-Botnet waren, welche die Jaff-Ransomware verbreiteten. Es dauerte einige Tage, bis die Security-Community ebenfalls zustimmte, dass die verdächtigen E-Mails Jaff, und nicht WannaCry, enthielten. Während dieses Zeitraums reagierten die Benutzer also auf Basis falscher Informationen und konnten die sich schnell ausbreitende WannaCry-Kampagne nicht aufhalten.

Das Chaos, das die WannaCry-Kampagne hinterlassen hat, ist eine Warnung. Die Security-Community muss in Zukunft vermeiden, falsche Fakten über den Ursprung und die Wirkung von Cyberangriffen zu verbreiten. Zu Beginn einer Kampagne kann der große Wunsch, die Gegner schnell zu stoppen und die Benutzer zu schützen, sehr schnell dazu führen, dass Informationen (insbesondere über soziale Netzwerke) geteilt werden, die zu Verunsicherung führen und die Benutzer sogar daran hindern können, ihre Systeme zu verteidigen.

Weitere Informationen zu diesem Thema finden Sie im Beitrag ***On Conveying Doubt*** im Cisco Talos-Blog.

VERSCHLÜSSELTER, SCHÄDLICHER WEB-DATENVERKEHR

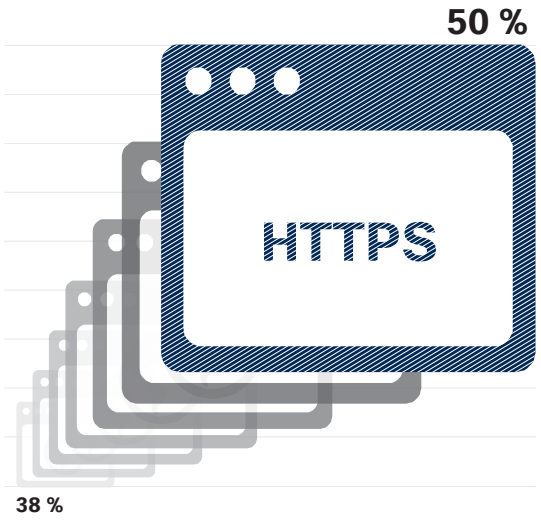
Das zunehmende Volumen an verschlüsseltem Web-Datenverkehr (sowohl legitim, als auch schädlich) sorgt für noch mehr Herausforderungen und Verwirrung bei der Identifizierung und Überwachung potenzieller Bedrohungen durch die Verteidiger. Verschlüsselungstechniken sollen die Sicherheit erhöhen, aber sie sind auch eine wirkungsvolle Methode für Angreifer zum Verbergen von Command-and-Control-Aktivitäten (C2). So haben diese mehr Zeit, um Angriffe durchzuführen und Schaden anzurichten. Cisco Bedrohungsforscher rechnen damit, dass Jahr 2018 auf der gegnerischen Seite verstärkt Verschlüsselungsfunktionen eingesetzt werden. Um da mithalten zu können, müssen Verteidiger neben dem Bedrohungsschutz, Erkennungs- und Problembehebungslösungen zusätzlich mehr Automatisierungslösungen und fortschrittliche Tools z. B. für maschinelles Lernen und künstliche Intelligenz einsetzen.

Im toten Winkel der Verteidiger: verschlüsselter, schädlicher Web-Datenverkehr

Laut Forschungsergebnissen von Cisco war seit Oktober 2017 50 Prozent des globalen Web-Datenverkehrs verschlüsselt. Das entspricht im Vergleich zum November 2016 einer Zunahme um 12 Prozentpunkte (siehe Abbildung 1). Ein Grund für diese Zunahme ist die Verfügbarkeit von kostengünstigen oder auch kostenlosen SSL-Zertifikaten. Ein weiterer ist, dass Google Chrome verstärkt auf unverschlüsselte Websites hinweist, die vertrauliche Informationen wie Kreditkartendaten von Kunden „nicht sicher“ handhaben. Unternehmen werden dazu motiviert, die HTTPS-Verschlüsselungsanforderungen von Google zu erfüllen, andernfalls könnten sie im Ranking bei der Google-Suche sehr weit zurückfallen.

Während der globale verschlüsselte Web-Datenverkehr weiter zunimmt, scheinen auch die Gegner vermehrt von der Verschlüsselung Gebrauch zu machen, um ihre C2-Aktivitäten zu verschleiern. Wir haben beobachtet, dass sich die in untersuchten Malware-Stichproben genutzte, verschlüsselte Netzwerkkommunikation in einem Zeitraum von 12 Monaten verdreifacht hat (siehe Abbildung 2). Unsere Analyse von mehr als 400.000 schädlichen Binärdateien hat ergeben, dass seit Oktober 2017 rund 70 Prozent wenigstens eine Verschlüsselungsform nutzten.

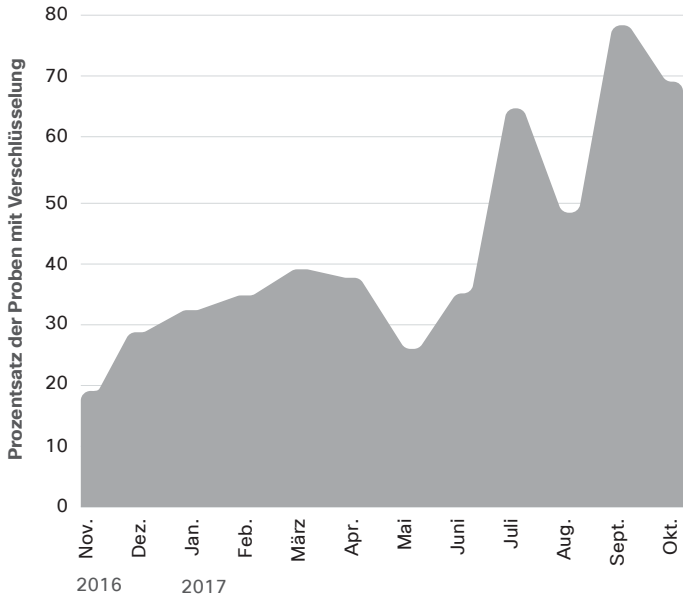
Abbildung 1 Zunehmendes Volumen an verschlüsseltem Web-Datenverkehr weltweit



Zunahme des globalen Web-Datenverkehrs von Nov. 2016 bis Okt. 2017 um 12 Prozentpunkte

Quelle: Cisco Security Research

Abbildung 2 Steigende Anzahl schädlicher Binärdateien, die verschlüsselte Netzwerkkommunikation nutzen



Quelle: Cisco Security Research

Grafiken für 2018 hier herunterladen: cisco.com/go/acr2018graphics

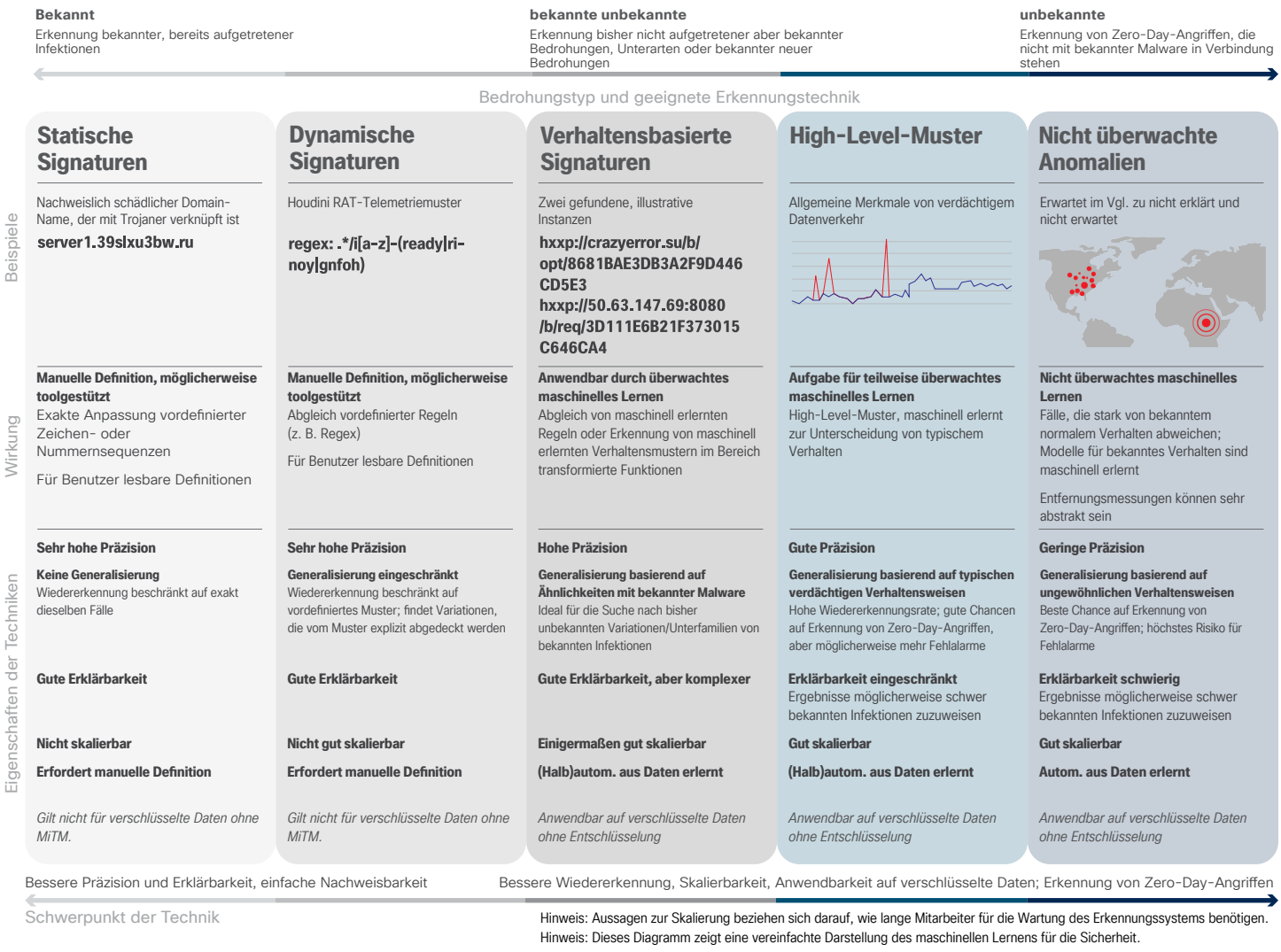
Beschleunigte Bedrohungserkennung durch maschinelles Lernen

Um mehr und bessere Einblicke in die Verschlüsselung zu erhalten und den Handlungsspielraum der Angreifer zu verringern, untersuchen immer mehr Unternehmen die Möglichkeiten, die sich ihnen durch maschinelles Lernen und künstliche Intelligenz bieten. Diese erweiterten Funktionen können die Netzwerksicherheit verbessern und mit der Zeit „lernen“, wie ungewöhnliche Muster im Web-Datenverkehr, die möglicherweise auf schädliche Aktivitäten hinweisen, automatisch erkannt werden können.

Maschinelles Lernen ist ein nützliches Mittel für die automatische Erkennung von bekannten Bedrohungen, also denen, die schon einmal aufgetreten sind (siehe Abbildung 3). Der wahre Wert dieser Lösung liegt, insbesondere bei der Beobachtung von verschlüsseltem Web-Datenverkehr, aber in ihrer Fähigkeit, bekannte unbekannte Bedrohungen (bisher nicht dagewesene Variationen bekannter Bedrohungen, Malware-Unterfamilien oder verwandte neue Bedrohungen) und unbekannte Bedrohungen (brandneue Malware) zu erkennen. Die Technologie kann lernen, ungewöhnliche Muster in großen Volumen an verschlüsseltem Web-Datenverkehr zu identifizieren und Sicherheitsteams automatisch darüber zu informieren, dass hier weitere Untersuchungen erforderlich sind.

Letzteres ist ganz besonders wichtig, da der Fachkräftemangel in vielen Organisationen für die Verbesserung von Sicherheitsmaßnahmen hinderlich ist, wie den Ergebnissen der Cisco Security Capabilities Benchmark Study 2018 (siehe Seite 35) zu entnehmen ist. Automatisierung und intelligente Tools wie maschinelles Lernen und künstliche Intelligenz helfen Verteidigern dabei, mangelnde Fähigkeiten und Ressourcen auszugleichen, und machen die Identifizierung und Reaktion auf bekannte und neue Bedrohungen effektiver.

Abbildung 3 Maschinelles Lernen im Bereich Netzwerksicherheit: Taxonomie



Hinweis: Aussagen zur Skalierung beziehen sich darauf, wie lange Mitarbeiter für die Wartung des Erkennungssystems benötigen.
Hinweis: Dieses Diagramm zeigt eine vereinfachte Darstellung des maschinellen Lernens für die Sicherheit.

Quelle: Cisco Security Research

Grafiken für 2018 hier herunterladen: cisco.com/go/acr2018graphics

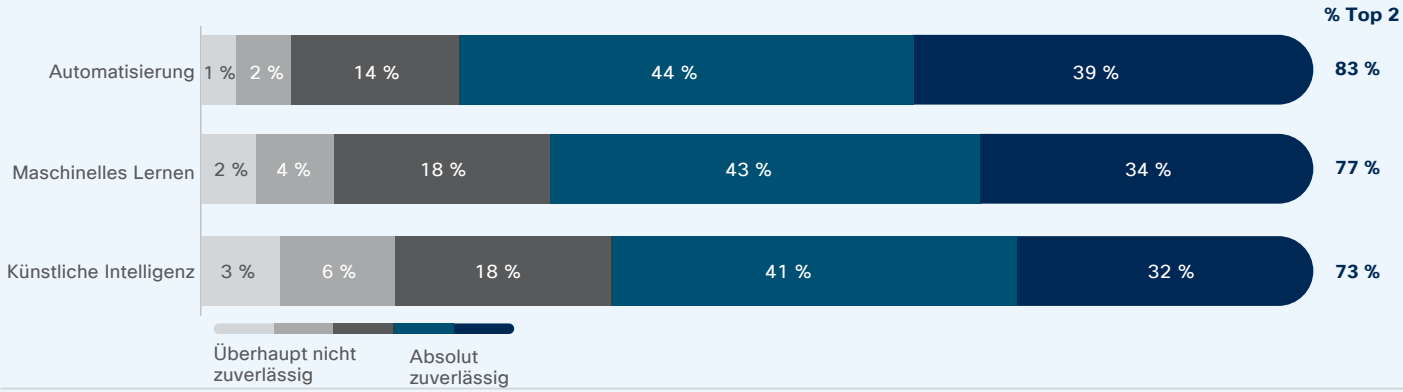
Cisco Security Capabilities Benchmark Study 2018: Verteidiger setzen vermehrt auf Automatisierung und künstliche Intelligenz

Die für die Cisco Security Capabilities Benchmark Study 2018 befragten CISOs (Chief Information Security Officers) gaben an, dass sie gerne Tools kaufen würden, die künstliche Intelligenz und maschinelles Lernen nutzen. Sie glauben außerdem, dass ihre Sicherheitsinfrastruktur immer fortschrittlicher und intelligenter wird. Allerdings frustriert sie die Zahl der Fehlalarme, die solche Systeme ausgeben, weil diese den Arbeitsaufwand für die Sicherheitsteams erhöhen. Diese Bedenken sollten sich jedoch mit der Zeit legen, da diese beiden Technologien immer ausgereifter werden und lernen, was in den von ihnen überwachten Netzwerkumgebungen als „normale“ Aktivität zu betrachten ist.

Auf die Frage, auf welche automatisierten Technologien sich ihre Organisationen am meisten verließen, antworteten 39 Prozent der Sicherheitsexperten, dass sie sich voll auf die Automatisierung verlassen; 34 Prozent setzen auf maschinelles Lernen und 32 Prozent auf künstliche Intelligenz (Abbildung 4).

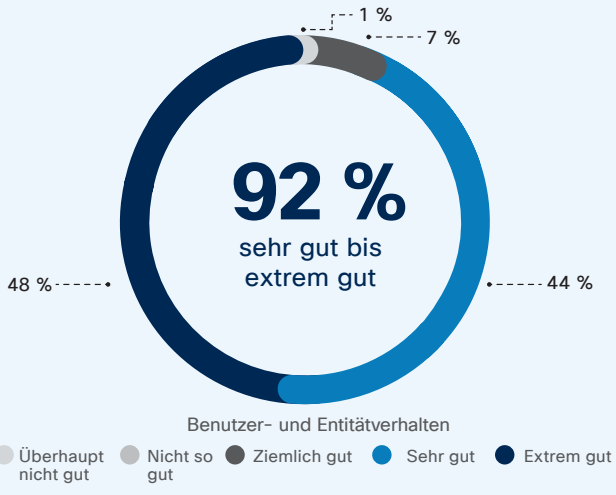
Tools für die Verhaltensanalyse werden ebenfalls als nützlich betrachtet, wenn es um das Auffinden von Angreifern im Netzwerk geht. 92 Prozent der Sicherheitsexperten sagen, dass diese Tools extrem gut funktionieren (Abbildung 5).

Abbildung 4 Organisationen setzen stark auf Automatisierung, maschinelles Lernen und künstliche Intelligenz



Quelle: Cisco Security Capabilities Benchmark Study 2018

Abbildung 5 Die meisten Sicherheitsexperten begreifen den Nutzen von Tools für die Verhaltensanalyse



(n=3617)

Extrem gut
69 %

2/3 der Gesundheitseinrichtungen glauben, dass Verhaltensanalysen/Forensik die Identifizierung von Angreifern unterstützen.

(n=358)

Extrem gut
38–39 %

Im Transportwesen und Regierungsbereich sind weniger der Ansicht, dass Verhaltensanalysen/Forensik extrem gut funktionieren.

(Transport: n=175; Regierung: n=639)

Quelle: Cisco Security Capabilities Benchmark Study 2018

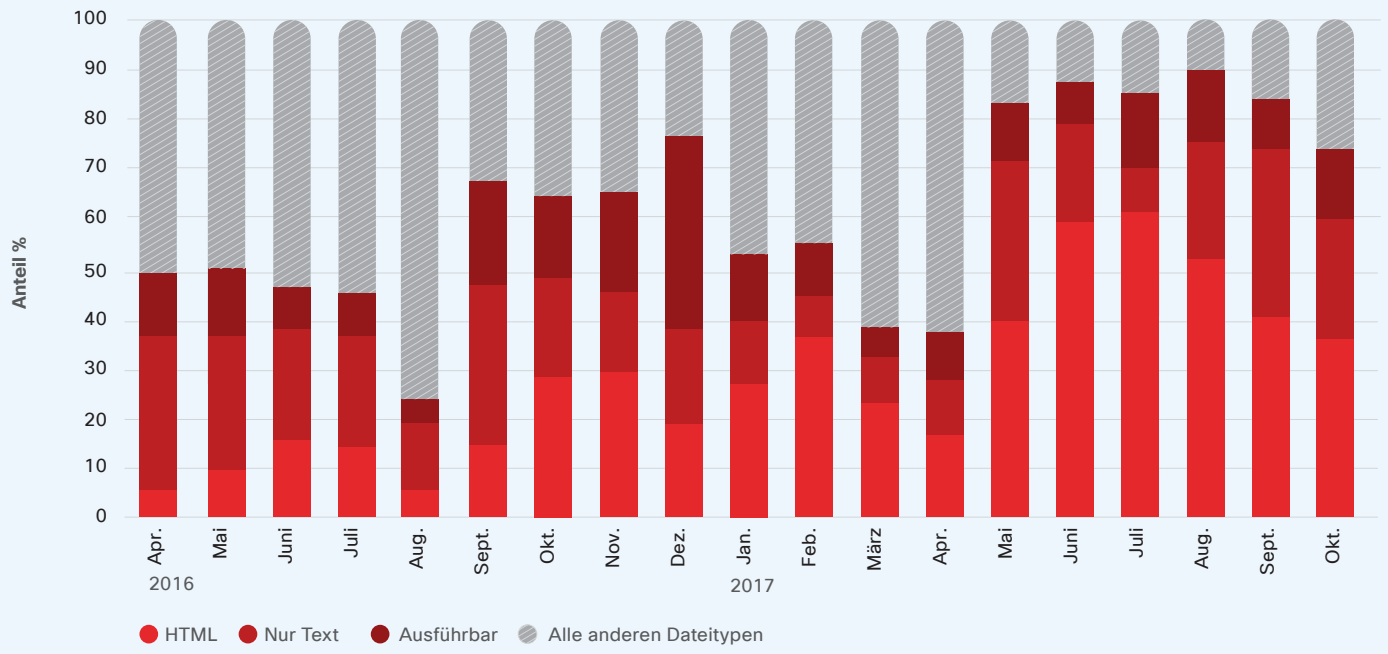
Grafiken für 2018 hier herunterladen: cisco.com/go/acr2018graphics

Web-Angriffsmethoden zeigen, wie intensiv sich Angreifer auf die Kompromittierung von Browsern konzentrieren

Eine Analyse der Web-Angriffsmethoden über einen Zeitraum von 18 Monaten (April 2016 bis Oktober 2017) zeigt, dass Gegner vermehrt schädliche Webinhalte nutzen (Abbildung 6). Dieser Trend geht mit aggressiven Angriffen gegen den Webbrowser Microsoft Internet Explorer mit immer noch aktiven Exploit-Kits einher.

Cisco Bedrohungsforscher haben beobachtet, dass die Anzahl der Erkennungen von schädlichen JavaScript-Webinhalten in dieser Zeit auffällig und konsistent war. Dies unterstreicht die Wirksamkeit dieser Strategie, bei der anfällige Browser infiziert werden sollen, um andere illegale Aktivitäten wie Browserumleitungen oder Downloads von Trojanern zu vereinfachen.

Abbildung 6 Malware-bezogene Blockierungsaktivität nach Inhaltstyp, April 2016 – Oktober 2017

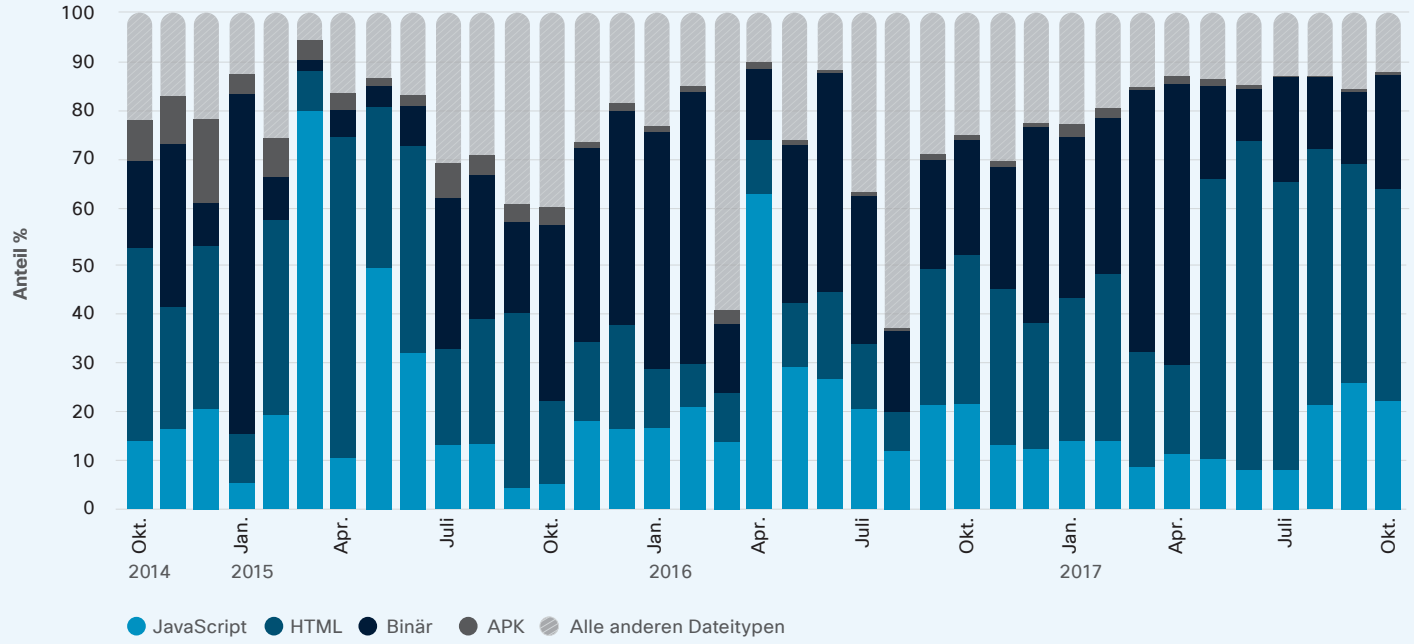


Quelle: Cisco Security Research

Abbildung 7 bietet einen Überblick über die Web-Angriffsmethoden im Verlauf von drei Jahren (Oktober 2014 bis Oktober 2017). Die Gegner verwendeten während dieses Zeitraums konsequent verdächtige Binärdateien, um vor allem Adware und Spyware einzuschleusen. Wie im *Cisco Midyear Cybersecurity Report 2017* behandelt, können diese Arten von potenziell unerwünschten Anwendungen (PUA) Sicherheitsrisiken darstellen. Dazu zählen z. B. erhöhte Malware-Infektionen und Diebstahl von Benutzer- oder Unternehmensdaten.[8]

Die Drei-Jahres-Ansicht in Abbildung 7 zeigt außerdem, dass das Volumen an schädlichen Webinhalten im Verlauf der Zeit schwankt, da Angreifer Kampagnen starten und beenden sowie ihre Taktiken ändern, um nicht entdeckt zu werden.

Abbildung 7 Malware-bezogene Blockierungsaktivität nach Inhaltstyp, Oktober 2014 – Oktober 2017



Quelle: Cisco Security Research

Grafiken für 2018 hier herunterladen: cisco.com/go/acr2018graphics

8 *Cisco Midyear Cybersecurity Report 2017*: cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

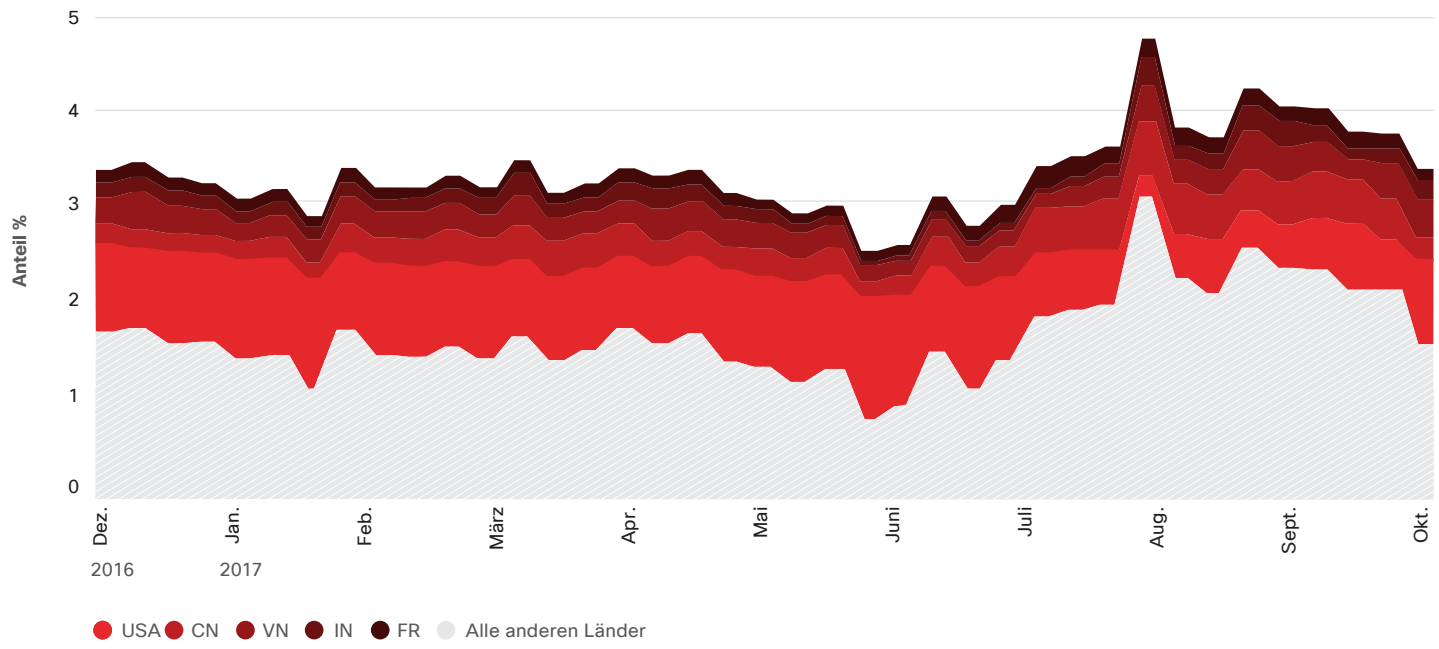
E-MAIL-BEDROHUNGEN

Trotz der Veränderungen in der Bedrohungslandschaft, bleiben schädliche E-Mails und Spam weiterhin ein wichtiges Mittel zur Verbreitung von Malware, weil sich die Bedrohung direkt gegen das Endgerät richtet. Die Angreifer wenden eine Mischung unterschiedlicher Social-Engineering-Techniken an (Phishing, schädliche Links und Anhänge), und warten dann einfach ab, bis ein nichtsahnender Benutzer die Exploits aktiviert.

Schwankende Spam-Botnet-Aktivitäten beeinflussen das Spam-Gesamtaufkommen

Ende 2016 beobachteten Cisco Bedrohungsforscher eine merkliche Zunahme bei Spam-Kampagnen, die anscheinend mit einem Rückgang von Exploit-Kit-Aktivitäten einherzugehen schien. Als führende Exploit-Kits wie Angler plötzlich vom Markt verschwanden, wandten sich viele Benutzer dieser Kits dem E-Mail-Vektor zu bzw. kehrten zu diesem zurück, um weiterhin Profite zu erzielen.[9] Nach diesem ersten Ansturm zurück zur E-Mail ging das globale Spam-Aufkommen zurück und pendelte sich in der ersten Jahreshälfte 2017 wieder ein. Ende Mai und Anfang Juni 2017 ging das globale Spam-Aufkommen dann erneut zurück, um im Hoch- bis Spätsommer wieder anzuziehen (siehe Abbildung 8).

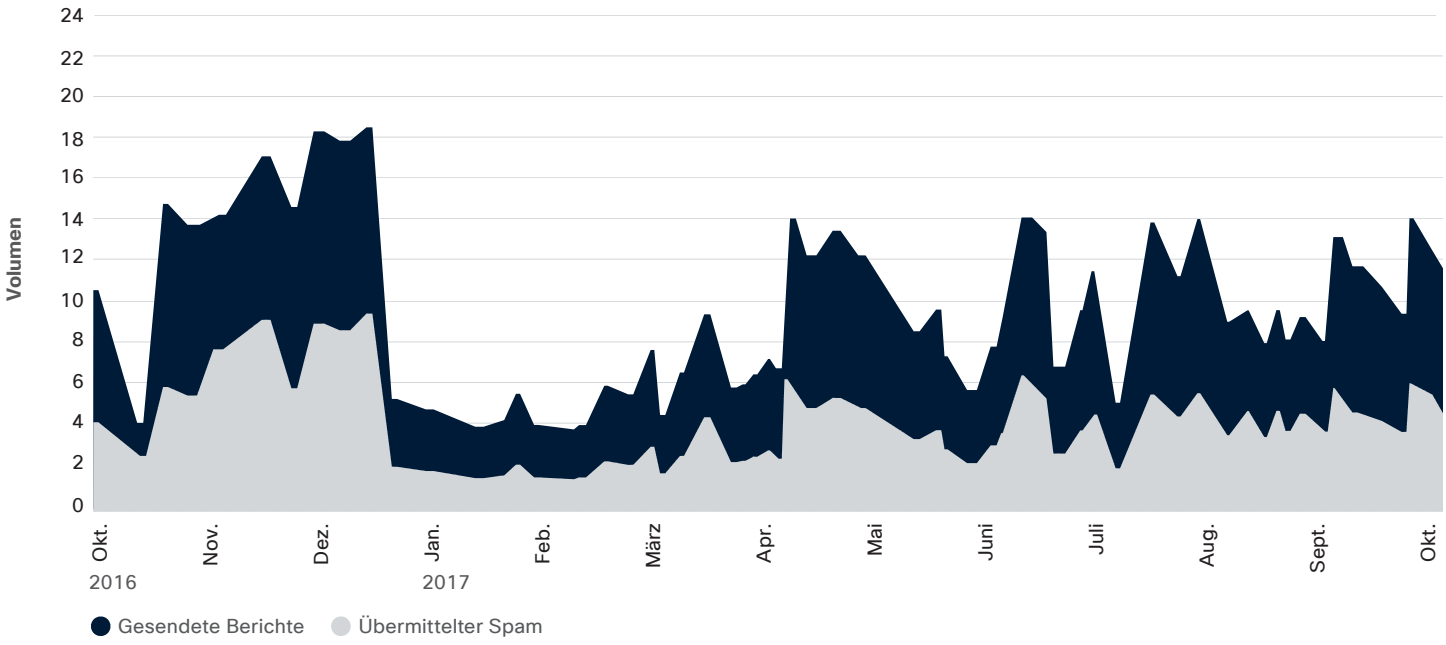
Abbildung 8 Blockierte IP-Reputation nach Land, Dezember 2016 – Oktober 2017



Quelle: Cisco Security Research

9 Siehe Abschnitt „Rückgang der Exploit-Kit-Aktivität wirkt sich wahrscheinlich auf globale Spam-Trends aus“ S. 18, *Cisco Midyear Cybersecurity Report 2017*: cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

Abbildung 9 Spam-Botnet-Aktivitäten, Oktober 2016 – Oktober 2017



Quelle: Cisco SpamCop

Grafiken für 2018 hier herunterladen: cisco.com/go/acr2018graphics

Das geringere Spam-Aufkommen von Januar bis April 2017 fällt mit einer Flaute bei Spam-Botnet-Aktivitäten zusammen, wie ein internes Diagramm vom Cisco® SpamCop-Service zeigt (Abbildung 9).

Cisco Bedrohungsforscher berichten, dass das Necurs-Botnet, das entscheidend zum globalen Spam-Gesamtaufkommen beiträgt, zwar aktiv war, aber zwischen Januar und April weniger Spam verteilte. Im Mai verbreitete das Botnet Jaff-Ransomware mithilfe von massiven Spam-Kampagnen. Die Kampagnen enthielten eine PDF-Datei mit einem eingebetteten schädlichen Microsoft Office-Dokument und ein Downloadprogramm für die Jaff-Ransomware.[10] Sicherheitsforscher entdeckten eine Schwachstelle in Jaff, welche die Erstellung einer Entschlüsselungsmethode ermöglichte. Somit waren die Nutzer von Necurs dazu gezwungen, wieder auf die Locky-Ransomware zurückzugreifen.[11] Der Zeitraum, den die Akteure hinter Necurs für die Rückkehr zu Locky benötigten, fällt mit dem deutlichen Rückgang des globalen Spam-Aufkommens während der ersten zwei Juniwochen zusammen (Abbildung 9).

10 *Jaff Ransomware: Player 2 Has Entered the Game,* von Nick Biasini, Edmund Brumaghin und Warren Mercer mit Beiträgen von Colin Grady, Cisco Talos-Blog, Mai 2017: blog.talosintelligence.com/2017/05/jaff-ransomware.html.

11 *Player 1 Limps Back Into the Ring—Hello Again, Locky!* von Alex Chiu, Warren Mercer und Jaeson Schultz mit Beiträgen von Sean Baird und Matthew Molyett, Cisco Talos-Blog, Juni 2017: blog.talosintelligence.com/2017/06/necurs-locky-campaign.html.

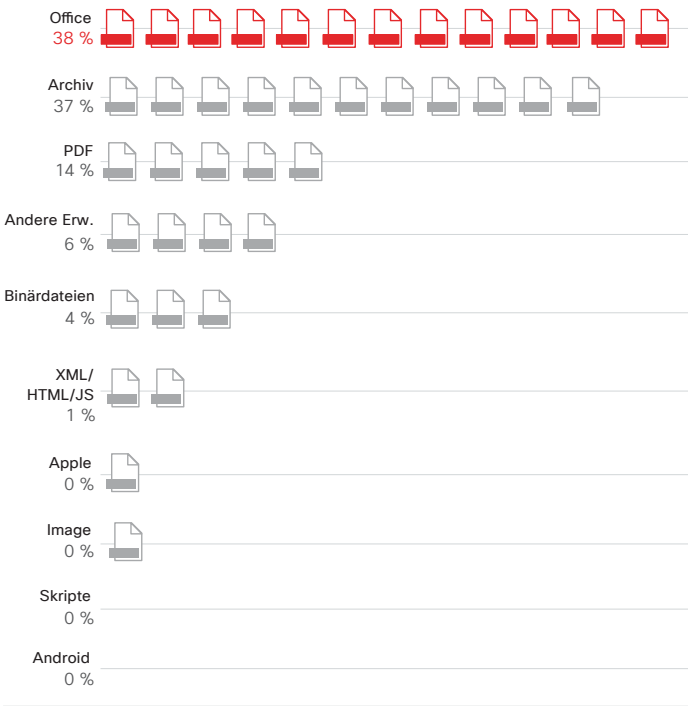
Schädliche Dateierweiterungen in E-Mails: die 10 wichtigsten Tools von gängigen Malware-Familien

Cisco Bedrohungsforscher analysierten die E-Mail-Telemetriedaten von Januar bis September 2017, um die Arten schädlicher Dateierweiterungen zu ermitteln, welche von gängigen Malware-Familien am häufigsten genutzt wurden. Die Analyse ergab eine Top-10-Liste, in der vor allem Microsoft Office-Formate wie Word, PowerPoint und Excel mit schädlichen Dateierweiterungen (38 Prozent) auffielen (siehe Abbildung 10).

Archivdateien wie.zip und.jar machten 37 Prozent aller untersuchten schädlichen Dateierweiterungen aus. Es ist wenig überraschend, dass Gegner verstärkt auf Archivdateien setzen, schließlich sind diese schon lange bevorzugte Verstecke für Malware. Benutzer müssen Archivdateien öffnen, um deren Inhalt anzuzeigen, und das ist für viele Bedrohungen ein wichtiger Schritt in der Infektionskette. Schädliche Archivdateien sind häufig auch bei der Täuschung von automatisierten Analysetools erfolgreich; vor allem, wenn sie Bedrohungen enthalten, die eine Aktivierung durch den Benutzer erfordern. Auch eher unbekannte Dateitypen wie.7z und.rar werden von den Gegnern verwendet, um einer Entdeckung zu entgehen.

Auf Platz drei landeten nach unserer Analyse schädliche PDF-Dateierweiterungen. Sie machten fast 14 Prozent der untersuchten schädlichen Dateierweiterungen aus. (Hinweis: Die Kategorie „Sonstige Erweiterungen“ bezieht sich auf in unserer Studie untersuchte Erweiterungen, die nicht so einfach bekannten Dateitypen zugeordnet werden konnten. Einige Malware-Arten sind dafür bekannt, dass sie zufällige Dateierweiterungen verwenden.)

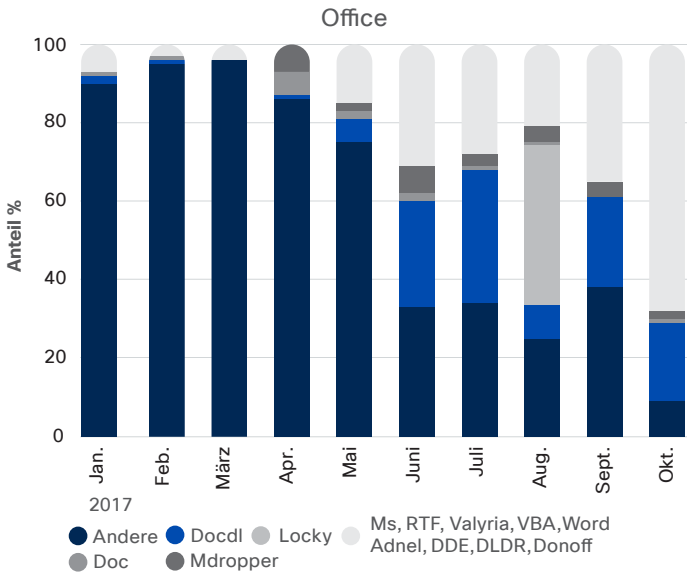
Abbildung 10 Top 10 der schädlichen Dateierweiterungen, Januar – September 2017



Quelle: Cisco Security Research

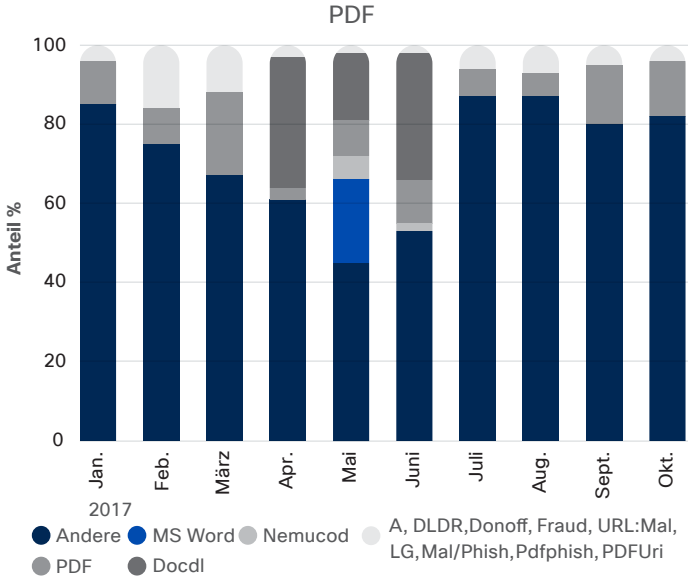
Die Abbildungen 11a-c bieten einen Überblick über die Malware-Familien in unserer Untersuchung, die mit den drei schädlichsten Dateierweiterungstypen zusammenhingen: MS Office-Dateien, Archivdateien und PDFs. Abbildung 12 zeigt den Prozentsatz der Erkennungen nach Familien, die eine Dateierweiterung mit schädlicher Payload enthielten. Die Aktivitätsspitzen fallen laut den Cisco Bedrohungsforschern mit Spam-Kampagnen zusammen, die während dieser Monate beobachtet wurden. Im Spätsommer gab es beispielsweise große Kampagnen, bei denen Nemucod und Locky verbreitet wurden – zwei Bedrohungen, die oft zusammenarbeiten. Nemucod versendet bekanntermaßen schädliche Payloads in Archivdateien wie.zip, die wie normale. doc-Dateien aussehen, aber schädliche Skripte enthalten. („Dwnldr“, auch in Abbildung 12 zu sehen, ist wahrscheinlich eine Variante von Nemucod.)

Abbildung 11a Top 3 der schädlichen Dateierweiterungen und Beziehungen zwischen Malware-Familien



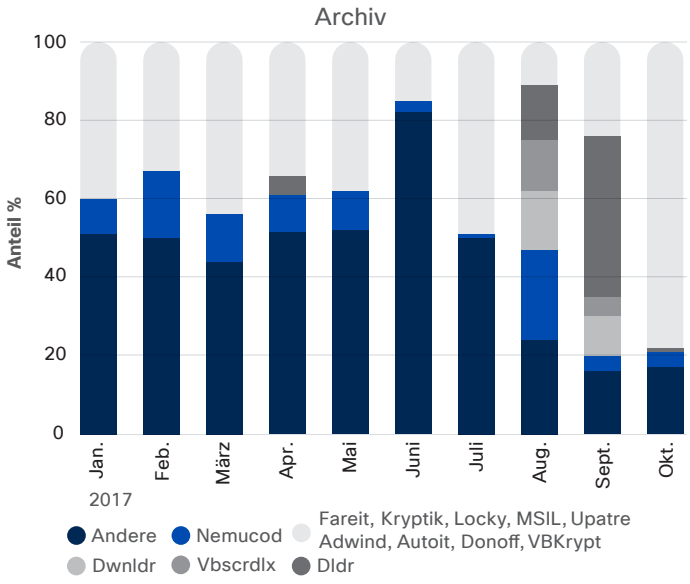
Quelle: Cisco Security Research

Abbildung 11b Top 3 der schädlichen Dateierweiterungen und Beziehungen zwischen Malware-Familien



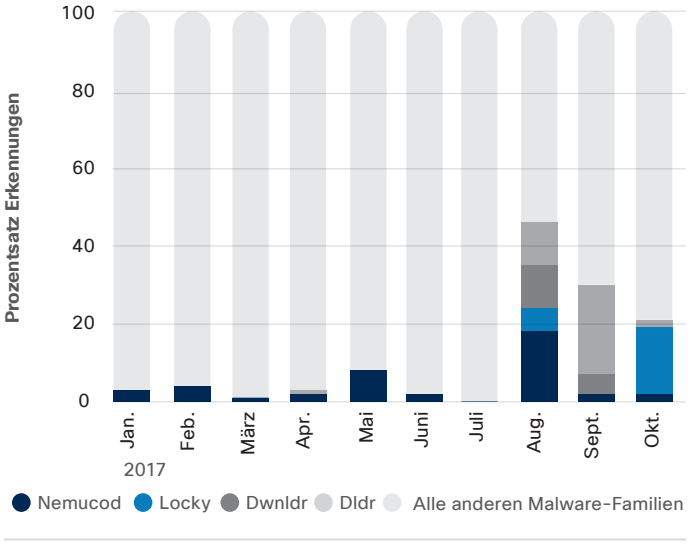
Quelle: Cisco Security Research

Abbildung 11c Top 3 der schädlichen Dateierweiterungen und Beziehungen zwischen Malware-Familien



Quelle: Cisco Security Research

Abbildung 12 Muster der häufigsten Malware-Familien, Januar – Oktober 2017



Quelle: Cisco Security Research

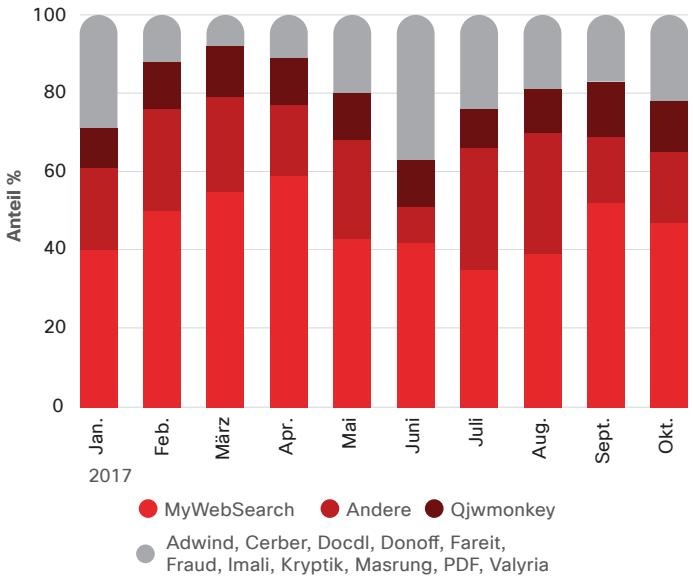
MyWebSearch-Spyware ist aktivster Nutzer der sonstigen Erweiterungen

Die Gruppe „Sonstige Erweiterungen“ in unserer Studie enthält einige wohlbekannte Malware-Typen. Aber MyWebSearch, eine schädliche Adware-Software und ein Browser-Hijacker, der sich als nützliche Symbolleiste ausgibt, ist am aktivsten (siehe Abbildung 13). Sie nutzt ausschließlich.exe-Dateierweiterungen, manchmal nur einen Typ pro Monat. Die potenziell unerwünschte Anwendung (PUA) gibt es schon seit Jahren und sie infiziert verschiedene Browsertypen. Häufig kommt sie als Paket mit betrügerischen Softwareprogrammen daher und kann Benutzer dem Malvertising aussetzen.

Unsere Analyse der schädlichen Dateierweiterungstypen zeigt, dass die E-Mail selbst noch immer ein wichtiger Kanal für die Verteilung von Malware ist, selbst in dieser heute so komplexen Bedrohungsumgebung. Zu den grundlegenden Abwehrstrategien für Unternehmen gehören:

- Implementierung leistungsfähiger und umfassender E-Mail-Sicherheitsmaßnahmen
- Aufklärung von Benutzern über die Bedrohung durch schädliche Anhänge und Links in Phishing-Mails und Spam

Abbildung 13 MyWebSearch ist aktivster Nutzer im Bereich der „sonstigen Erweiterungen“



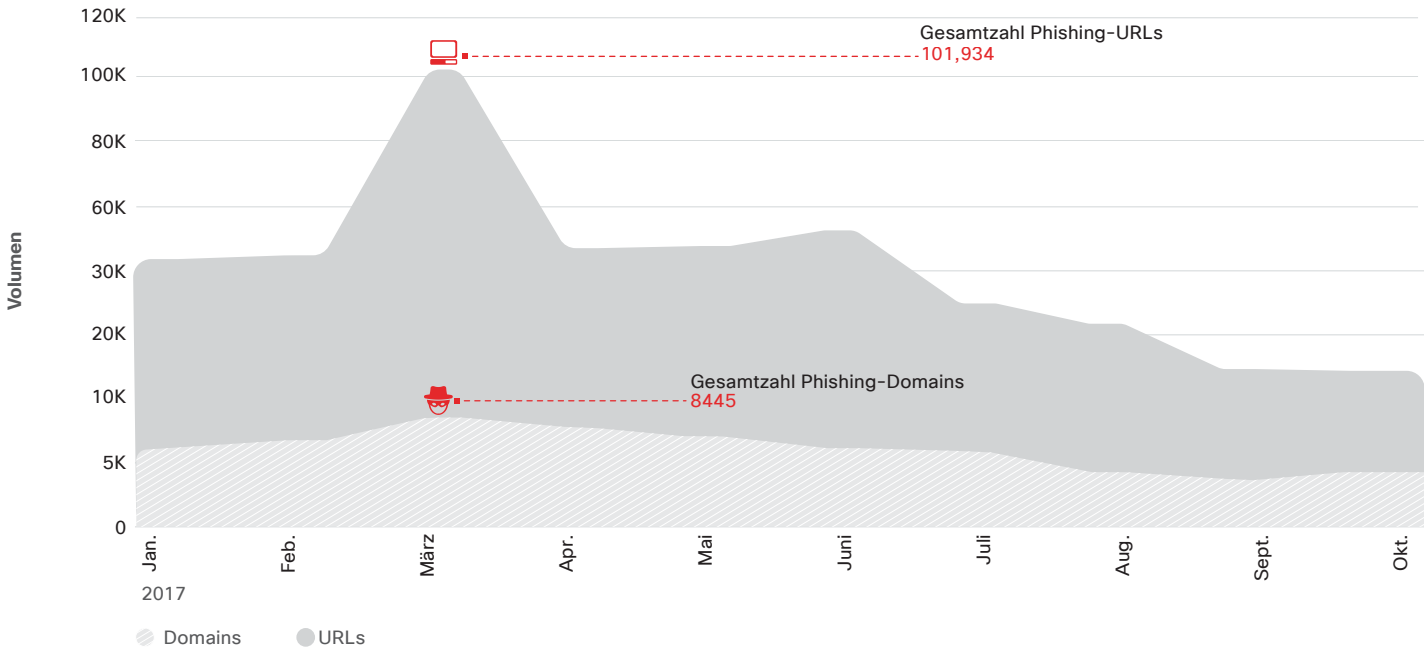
Quelle: Cisco Security Research

Social Engineering immer noch ein entscheidender Ausgangspunkt für E-Mail-Angriffe

Phishing und Spear Phishing werden häufig genutzt, um Anmeldeinformationen und andere vertrauliche Informationen von Benutzern zu stehlen. Dabei sind sie äußerst effektiv. Tatsächlich waren Phishing- und Spear-Phishing-E-Mails an einigen der größten und schlagzeilenträchtigsten Sicherheitsverletzungen der letzten Jahre beteiligt. Zwei Beispiele aus dem Jahr 2017 sind der ausgedehnte Angriff auf Gmail-Nutzer[12] und der Hackerangriff auf irische Energienetze.[13]

Um die tatsächliche Häufigkeit von Phishing-URLs und -Domains zu beurteilen, prüften Cisco Bedrohungsforscher Daten aus Quellen, die potenziell verdächtige E-Mails untersuchen. Diese wurden von Benutzern über Community-basierte Antiphishing-Threat-Intelligence eingesendet. Abbildung 14 zeigt die Anzahl der Phishing-URLs und Phishing-Domains, die im Zeitraum von Januar bis Oktober 2017 beobachtet wurden.

Abbildung 14 Anzahl der beobachteten Phishing-URLs und Domains pro Monat



Quelle: Cisco Security Research

Die Spitzen im März und Juni können auf zwei verschiedene Kampagnen zurückgeführt werden. Die erste schien auf Nutzer eines großen Telekommunikations-Service-Provider abzuzielen. Diese Kampagne:

- betraf 59.651 URLs mit Subdomains unter aaaainfomation[dot]org.
- enthielt Subdomains, die zufällige Zeichenfolgen mit 50-62 Buchstaben enthielt.

Jede Subdomain-Länge (50 - 62) enthielt etwa 3.500 URLs, die eine programmatische Verwendung der Subdomains erlaubte (z. B.: Cewekonuxykysowegulukozapojygepuqybyteqe johofopefogu[dot]aaaainfomation[dot]org).

Die Gegner nutzten einen preiswerten Privacy-Service, um die in dieser Kampagne beobachteten Domains zu registrieren.

12 *Massive Phishing Attack Targets Gmail Users,* von Alex Johnson, NBC News, Mai 2017: nbcnews.com/tech/security/massive-phishing-attack-targets-millions-gmail-users-n754501.
13 *Hackers target Irish energy networks amid fears of further cyber attacks on UK's crucial infrastructure,* von Lizzie Deardon, *The Independent*, Juli 2017: independent.co.uk/news/world/europe/cyber-attacks-uk-hackers-target-irish-energy-network-russia-putin-electricity-supply-board-nuclear-a7843086.html.

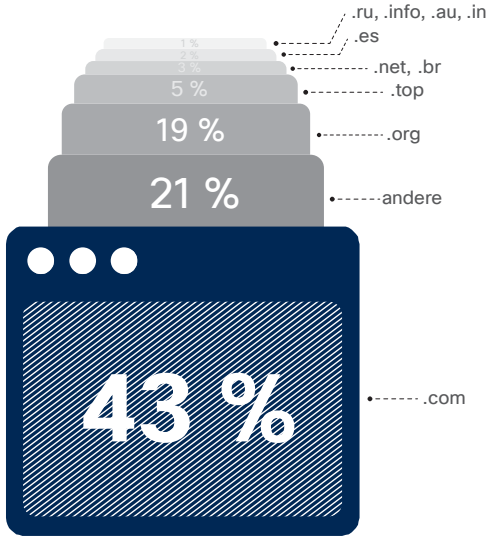
In der zweiten Kampagne, die im Juni besonders aktiv war, verwendeten Angreifer den Namen einer legitimen Steuerbehörde in Großbritannien, um ihre Aktionen zu verschleiern. Sie verwendeten 12 TLDs (Top-Level-Domains). Elf der Domains waren URLs mit sechs zufälligen Strings aus sechs Zeichen (z. B.: jyzwyp[dot]top). Neun der Domains wurden mehr als 1.600 Phishing-Websites zugeordnet.

Wie bei der Kampagne im März registrierten Gegner die Domains mit einem Privacy-Service, um Domain-Registrierungsdaten zu verbergen. Nach zwei Tagen hatten sie alle Domains registriert. Am zweiten Tag konnten knapp 19.000 mit der Kampagne verknüpfte URLs festgestellt werden, die alle innerhalb von fünf Stunden erfasst wurden (für weitere Informationen dazu, wie schnell Angreifer neu registrierte Domains einsetzen, siehe „Böswilliger Einsatz von legitimen Ressourcen für Backdoor-C2-Zwecke“ auf Seite 24).

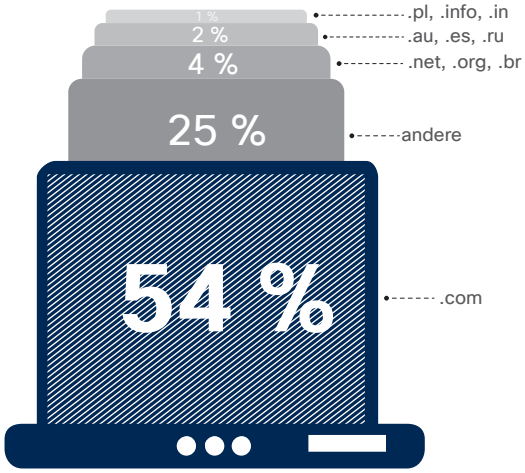
TLD-Verteilung auf bekannten Phishing-Websites

Unsere Analyse der Phishing-Websites von Januar bis August 2017 ergab, dass Angreifer 326 eindeutige TLDs für diese Aktivitäten verwendeten, darunter.com,.org,.top (hauptsächlich wegen der Kampagne bei der britischen Steuerbehörde) sowie länderspezifische TLDs (siehe Abbildung 15). Die Verwendung weniger bekannter TLDs kann für Gegner von Vorteil sein, denn diese Domains sind in der Regel erschwinglich und bieten oft eine günstige Möglichkeit, unentdeckt zu bleiben.

Abbildung 15 TLD-Verteilung auf bekannten Phishing-Websites



Prozentsatz aller Websites mit TLDs (alle Daten)



Prozentsatz der Websites mit TLDs
(Ausgenommen bestimmte TLDs aus zwei Kampagnen gegen Steuerbehörde und Telekommunikationsunternehmen)

Quelle: Cisco Security Research

Verteidiger sollten bei der Überwachung dieser „alten“ Bedrohung wachsam sein

Im Jahr 2017 wurden den Community-basierten Antiphishing-Threat-Intelligence-Services aus unserer Analyse pro Monat zehntausende Phishing-Versuche gemeldet. Zu den gängigen Taktiken und Tools, die von Gegnern für die Durchführung von Phishing-Kampagnen genutzt werden, gehörte Folgendes:

- **Domain Squatting:** Domains werden ähnlich wie gültige Domains benannt (Beispiel: cisc0[dot]com).
- **Domain Shadowing:** Einer gültigen Domain werden ohne das Wissen des Eigentümers Subdomains hinzugefügt (Beispiel: badstuff[dot]cisco[dot]com).
- **Böswillig registrierte Domains:** Eine Domain, die für schädliche Zwecke erstellt wurde (Beispiel: viqpbe[dot]top).
- **URL-Shortener:** Eine schädliche URL, die durch einen URL-Shortener getarnt ist (Beispiel: bitly[dot]com/random-string).

  Hinweis: Bei den von uns untersuchten Daten war Bitly.com das URL-Shortening-Tool, das Gegner am häufigsten nutzten. Zu schädlichen Zwecken verkürzte URLs machten 2 Prozent der Phishing-Websites in unserer Studie aus. Diese Zahl erreichte im August 3,1 Prozent.
- **Subdomain-Services:** Eine Website, die unter einem Subdomain-Server erstellt wird (Beispiel: mybadpage[dot]000webhost[dot]com).

Angreifer, die Phishing und Spear Phishing nutzen, verfeinern laufend ihre Social-Engineering-Methoden, um Benutzer dazu zu bewegen, auf schädliche Links zu klicken, betrügerische Webseiten zu besuchen oder Anmeldeinformationen und andere wertvolle Daten preiszugeben. Benutzerschulungen und -verantwortlichkeiten und die Anwendung von E-Mail-Sicherheitstechnologien bleiben weiterhin wichtige Strategien für den Kampf gegen diese Bedrohungen.

TAKTIKEN ZUR SANDBOX-UMGEHUNG

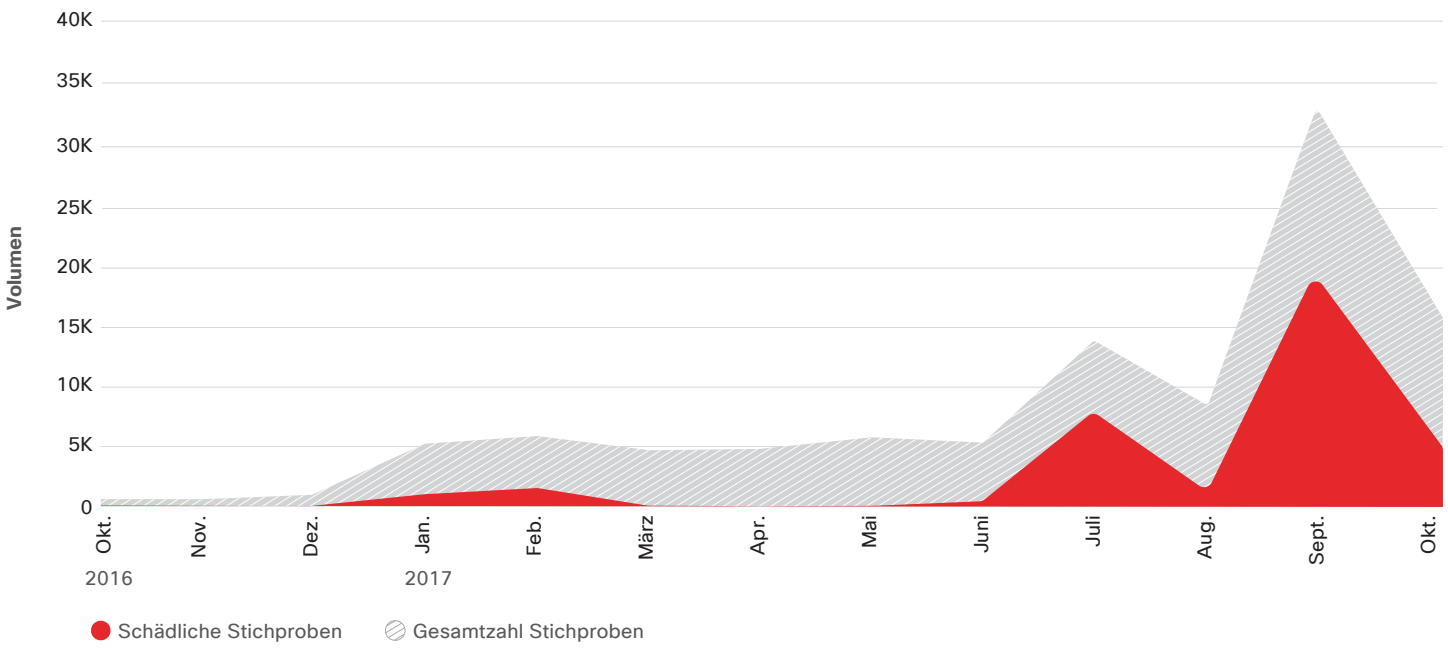
Gegner entwickeln immer fortschrittlichere Bedrohungen, die immer ausgefeiltere Sandbox-Umgebungen umgehen können. Als Cisco Bedrohungsforscher schädliche, mit verschiedenen Taktiken zur Sandbox-Umgehung ausgerüstete E-Mail-Anhänge analysierten, stellten sie fest, dass die Anzahl der schädlichen Stichproben mit spezieller Sandbox-Umgehung auffällige Spitzenwerte erzielte und dann schnell abfiel. Dies ist ein weiteres Beispiel dafür, wie schnell Angreifer ihre Bemühungen intensivieren, um Verteidigungslinien zu durchbrechen, sobald sie eine effektive Technik gefunden haben.

Die Tricks der Malware-Entwickler zur Sandbox-Umgehung

Im September 2017 stellten Cisco Bedrohungsforscher ein hohes Aufkommen von Stichproben fest, bei denen nach dem Schließen eines Dokuments schädliche Payloads verteilt werden (Abbildung 16). In diesem Fall wird die Malware durch das Ereignis „document_close“ aktiviert. Die Methode funktioniert deshalb, weil Dokumente nach dem Öffnen und Analysieren in der Sandbox häufig nicht geschlossen werden. Da die Sandbox das Dokument nicht explizit schließt, werden die Anhänge von der Sandbox als sicher betrachtet und den vorgesehenen Empfängern zugestellt. Wenn ein Empfänger das angehängte Dokument öffnet und es später schließt, wird die schädliche Payload eingeschleust. Sandboxes, die Aktionen beim Schließen von Dokumenten nicht ordnungsgemäß erfassen, können mithilfe dieser Technik umgangen werden.

Für Angreifer ist das Ereignis „document_close“ eine clevere Option. Sie nutzt nicht nur die in Microsoft Office integrierten Makrofunktionen, sondern auch die Neigung der Benutzer, möglicherweise relevante Anhänge zu öffnen. Sobald Benutzer feststellen, dass der Anhang nicht relevant ist, schließen sie das Dokument und aktivieren die Makros, die in der Malware verborgen sind.

Abbildung 16 Hohe Zahl an schädlichen Microsoft Word-Dokumenten mit Funktionsaufruf „Schließen“ (beobachtet im September 2017)

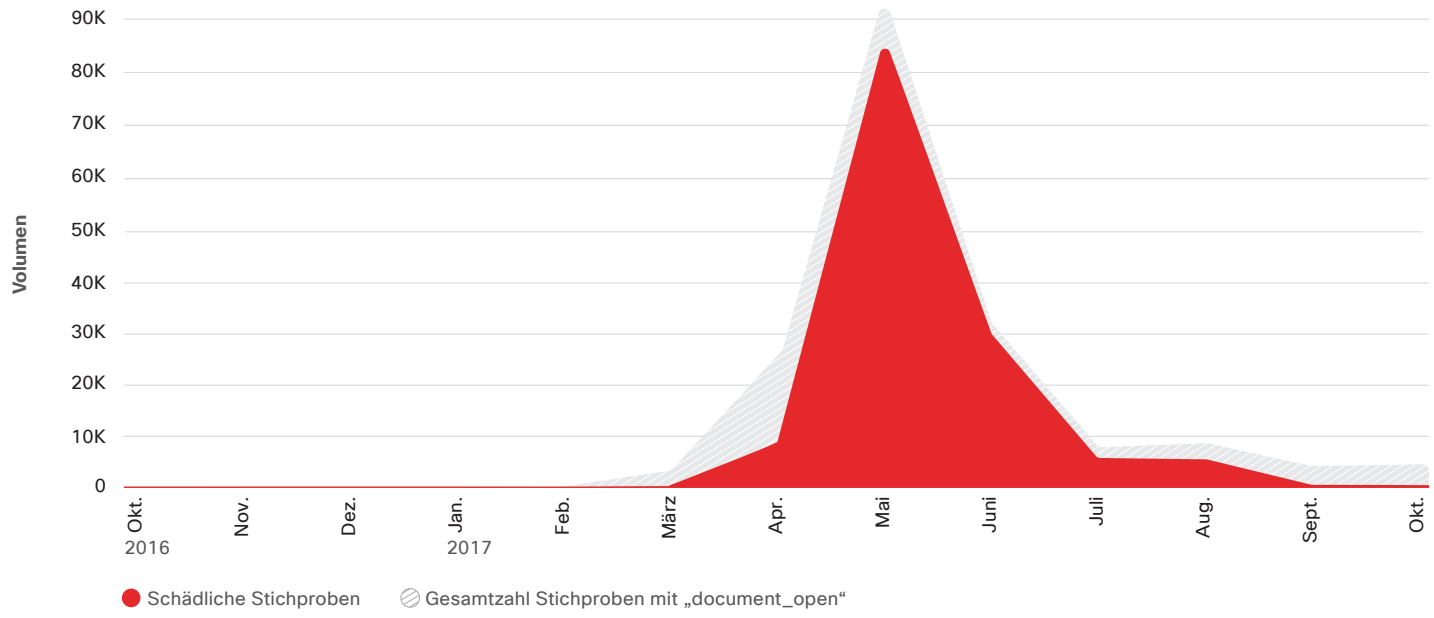


Quelle: Cisco Security Research

Einige Angreifer umgehen das Sandboxing, indem sie den Dokumententyp verschleiern, der die schädliche Payload enthält. Wie in Abbildung 17 zu sehen, verzeichneten wir im Mai 2017 einen erheblichen Angriff, der auf schädlichen Word-Dokumenten basierte, die in PDF-Dokumente eingebettet wurden. Die Dokumente könnten Sandboxes umgehen, die lediglich die PDF-Datei erkennen und öffnen, anstatt auch das eingebettete Word-Dokument zu öffnen und zu analysieren. Das PDF-Dokument enthielt typischerweise einen Anreiz für Benutzer, das Word-Dokument anzuklicken und zu öffnen, was dann ein schädliches Verhalten auslösen würde. Sandboxes, die in PDFs eingebettete Dokumente nicht öffnen und analysieren, können auf diese Weise umgangen werden.

Nachdem sie sich die Spitzen mit schädlichen PDF-Stichproben angesehen hatten, verfeinerten unsere Bedrohungsforscher die Sandbox-Umgebung. Daraufhin untersuchte die Sandbox, ob PDF-Dateien Aktionen oder Anreize zum Öffnen von Word-Dokumenten enthielten.

Abbildung 17 Groß angelegter Angriff im Mai 2017 mit PDFs, die schädliche eingebettete Word-Dokumente enthielten



Quelle: Cisco Security Research

Die Spitzen mit schädlichen Stichproben, welche andere Sandbox-Umgehungstechniken nutzen, weisen darauf hin, dass Angreifer einer Methode folgen möchten, die für sie – und andere Angreifer – zu funktionieren scheint. Wenn Gegner sich schon die Mühe machen, Malware und eine zugehörige Infrastruktur zu entwickeln, möchten sie daraus auch Kapital schlagen. Sollten sie feststellen, dass die Malware den Tests der Sandbox entgehen kann, werden sie ihre Angriffe intensivieren und diese gegen mehr Benutzer richten.

Cisco Forscher empfehlen die Verwendung einer Sandboxing-Methode, die inhaltsorientiert arbeitet. Dies soll sicherstellen, dass Malware mit den obigen Umgehungstaktiken nicht an der Sandbox-Analyse vorbeikommt. Die Sandboxing-Technologie sollte die Metadaten in den zu analysierenden Stichproben erkennen und bestimmen können, ob Stichproben eine Aktion nach dem Schließen eines Dokuments beinhalten.

MISSBRAUCH VON CLOUD-SERVICES UND ANDEREN LEGITIMEN RESSOURCEN

Da immer mehr Anwendungen, Daten und Identitäten in die Cloud verschoben werden, müssen Sicherheitsteams das Risiko eines Kontrollverlusts über den herkömmlichen Netzwerkperimeter eindämmen. Angreifer profitieren von der Tatsache, dass Sicherheitsteams Schwierigkeiten damit haben, dynamische und stetig wachsende Cloud- und IoT-Umgebungen zu verteidigen. Ein Grund dafür ist der mangelnde Überblick darüber, wer genau für den Schutz dieser Umgebungen zuständig ist.

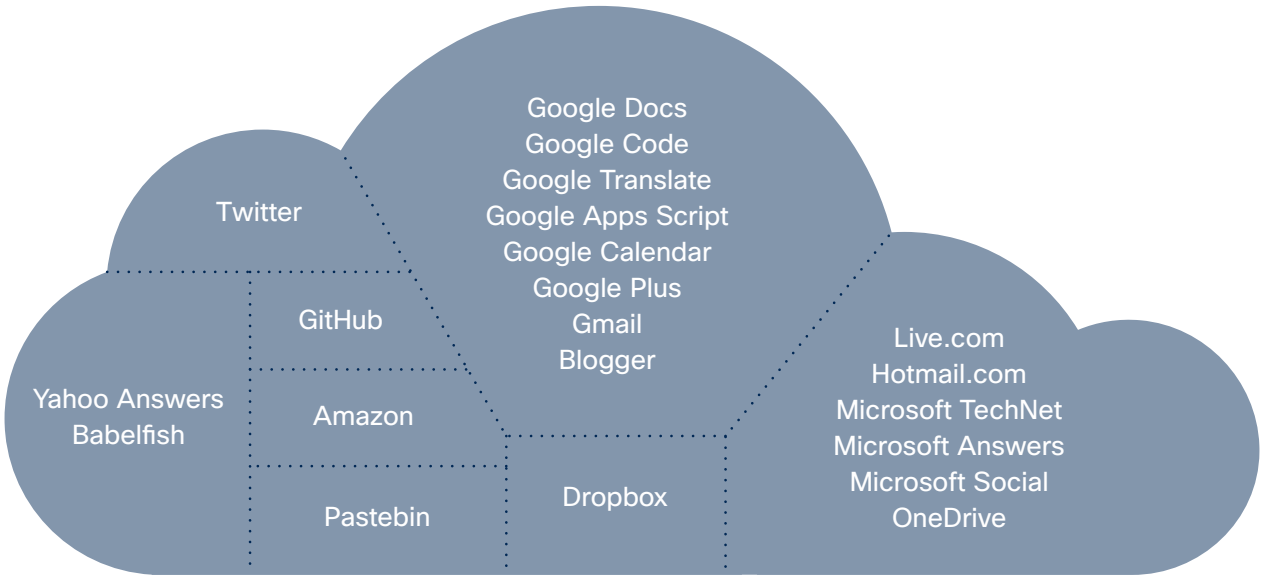
Um diese Herausforderung zu meistern, werden Unternehmen – je nachdem, welche Services sie für ihre Geschäfte nutzen und wie sich Bedrohungen in diesem Bereich weiterentwickeln – eine Kombination aus Best-Practices, modernen Sicherheitstechnologien wie maschinelles Lernen und sogar experimentelle Methoden anwenden müssen.

Böswillige Verwendung von legitimen Ressourcen für Backdoor-C2

Wenn Angreifer legitime Services für C2-Aktivitäten (Command-and-Control) verwenden, wird es für Sicherheitsteams beinahe unmöglich, Malware-Netzwerkverkehr zu identifizieren, weil dieser das Verhalten von legitimem Netzwerkverkehr nachahmt. Gegner können die vielen „Hintergrundgeräusche" des Internets als Deckung nutzen, da sich viele Benutzer heutzutage auch für die Arbeit auf Services wie Google Docs oder Dropbox verlassen, egal, ob diese vom Arbeitgeber angeboten oder systematisch unterstützt werden.

Abbildung 18 zeigt diverse bekannte legitime Services. Forscher von Anomali, einem Cisco Partner und Anbieter von Threat-Intelligence, stellten fest, dass diese in den letzten Jahren für Malware-Backdoor-C2-Schemata[14] verwendet wurden. (Hinweis: Bei dieser Art von Service gestaltet sich die Missbrauchsbekämpfung schwierig. Denn wenn die Einrichtung von Benutzerkonten und ihre Verwendung erschwert werden, kann sich das negativ auf den Umsatz auswirken.)

Abbildung 18 Beispiele für legitime Services, die von Malware für C2-Aktionen missbraucht werden



Quelle: Anomali

14 Anomali definiert ein C2-Schema als die Gesamtheit von IP-Adressen, Domains, legitimen Services und allen Remote-Systemen, die Teil der Kommunikationsarchitektur von Malware sind.

Laut den Untersuchungen von Anomali zählten Angreifer, die Advanced Persistent Threats (APT) durchführen, und staatlich geförderte Gruppen zu den Gegnern, die als erste legitime Services für C2-Aktionen nutzten. Allerdings wird diese Vorgehensweise nun auch von anderen raffinierten Akteuren in der Schattenwirtschaft übernommen. Die Verwendung von legitimen Services für C2-Aktivitäten ist für Angreifer aus folgenden Gründen attraktiv:

- Sie können neue Konten für diese Services registrieren.
- Sie können eine Webseite im öffentlich zugänglichen Internet einrichten.
- Sie können C2-Protokolle widerrechtlich verschlüsseln. (Anstatt C2-Server zu verschlüsseln oder Verschlüsselungsmethoden in Malware zu integrieren, können Angreifer einfach das SSL-Zertifikat eines legitimen Services übernehmen.)
- Sie können Ressourcen spontan anpassen und transformieren. (Angreifer können beispielsweise Malware-Implantate für andere Angriffe wiederverwenden, ohne dieselben DNS- oder IP-Adressen zu nutzen.)
- Sie können die Wahrscheinlichkeit reduzieren, Spuren in der Infrastruktur zu hinterlassen. (Gegner, die legitime Services für C2-Aktivitäten nutzen, brauchen keine hartcodierte Malware mit IP-Adressen oder Domains. Wenn der Vorgang abgeschlossen ist, deaktivieren sie einfach ihre Seiten mit legitimen Services und keiner wird jemals die IP-Adressen herausfinden.)
- Diese Technik verschafft den Angreifern mehr Vorteile, da sie ihren Aufwand reduzieren und mehr Kapital daraus schlagen können.

Die Nutzung legitimer Services für C2-Aktivitäten durch die Gegner erzeugt bei den Verteidigern große Herausforderungen:

Legitime Services sind schwer zu blockieren.
Können Organisationen rein wirtschaftlich betrachtet überhaupt eine teilweise Blockierung von legitimen Internet-Services wie Twitter oder Google in Erwägung ziehen?

Legitime Services sind häufig verschlüsselt und generell schwer zu untersuchen.
Die SSL-Entschlüsselung ist teuer und auf Unternehmensebene nicht immer möglich. Daher versteckt Malware ihre Kommunikation im verschlüsselten Datenverkehr und macht es für Sicherheitsteams schwer, oder gar unmöglich, schädlichen Datenverkehr zu identifizieren.

Die Nutzung legitimer Services unterwandert Domain- und Zertifikatsinformationen und erschwert die Zuordnung.
Gegner müssen keine Domains registrieren, weil das Konto für den legitimen Service als erste C2-Adresse betrachtet wird. Sie werden wahrscheinlich auch keine weiteren SSL-Zertifikate registrieren oder selbstsignierte SSL-Zertifikate für C2-Schemata verwenden. Beide Trends werden sich natürlich negativ auf Indikator-Feeds für die Reputationsfilterung und Indikator-Blacklists auswirken, die auf neu erstellten und neu registrierten Domains und den damit verbundenen Zertifikaten und IP-Adressen basieren.

Die Verwendung von legitimen Services für C2-Aktivitäten ist schwer zu erkennen. Die Bedrohungsforscher von Anomali empfehlen Verteidigern, den Einsatz einiger experimenteller Methoden zu erwägen. Wer Malware aufspüren möchte, die legitime Services für C2-Aktivitäten nutzt, muss nach Folgendem Ausschau halten:

- Nach nicht auf Browsern oder Apps basierenden, legitimen Services
- Nach einzigartigen oder niedrigen Antwortpaketgrößen von legitimen Services
- Nach einem hohen Zertifikataustausch bei legitimen Services
- Nach Bulk-Sandboxing-Beispielen mit verdächtigen DNS-Aufrufen von legitimen Services

Bei diesen einzigartigen Verhaltensweisen lohnt es sich, die Quellprogramme und Prozesse näher zu untersuchen.[15]

15 Wenn Sie weitere Informationen zu diesen experimentellen Vorgehensweisen erhalten möchten und mehr Details zur Nutzung legitimer Services für C2-Aktivitäten benötigen, laden Sie den Forschungsbericht von Anomali, *Rise of Legitimate Services for Backdoor Command and Control*, unter folgender Adresse herunter. anomali.cdn.rackfoundry.net/files/anomali-labs-reports/legit-services.pdf.

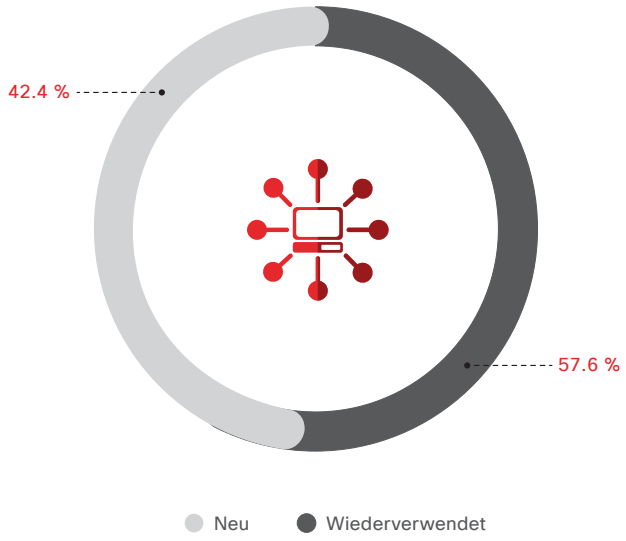
Ressourcen optimal nutzen

Cisco Security-Forscher analysierten erstmals beobachtete, einzigartige, mit DNS-Abfragen zusammenhängende Abfragenamen (Domains), die im August 2017 innerhalb von sieben Tagen gemacht wurden. Beachten Sie, dass der Ausdruck „erstmals beobachtet“ für die Erstellung einer Domain keine Bedeutung hat; er bedeutet lediglich, dass eine Domain während des Beobachtungszeitraums erstmals von Cisco Cloud-Sicherheitstechnologien erkannt wurde.

Der Zweck dieser Untersuchung war, mehr Einblick darin zu erhalten, wie häufig Gegner RLDs (Registered-Level-Domains) für ihre Angriffe verwenden und wiederverwenden. Wenn Verteidiger das Verhalten von Angreifern auf der Domain-Ebene verstehen, kann ihnen dies bei der Identifizierung von schädlichen Domains und zugehörigen Subdomains nützlich sein, die mit Tools der ersten Verteidigungslinie – etwa Cloud-Security-Plattformen – blockiert werden sollten.

Damit sich unsere Forscher ausschließlich auf die Kerngruppe der einzigartigen RLDs konzentrieren können, das sind insgesamt etwa 4 Millionen, wurden Subdomains von der Stichprobe der erstmals beobachteten Domains ausgenommen. Nur ein kleiner Prozentsatz der RLDs in dieser Stichprobe wurde als schädlich eingestuft. Von den tatsächlich schädlichen RLDs wurden über die Hälfte (etwa 58 Prozent) wiederverwendet, wie Abbildung 19 zeigt.

Abbildung 19 Prozentsatz der neuen und wiederverwendeten Domains



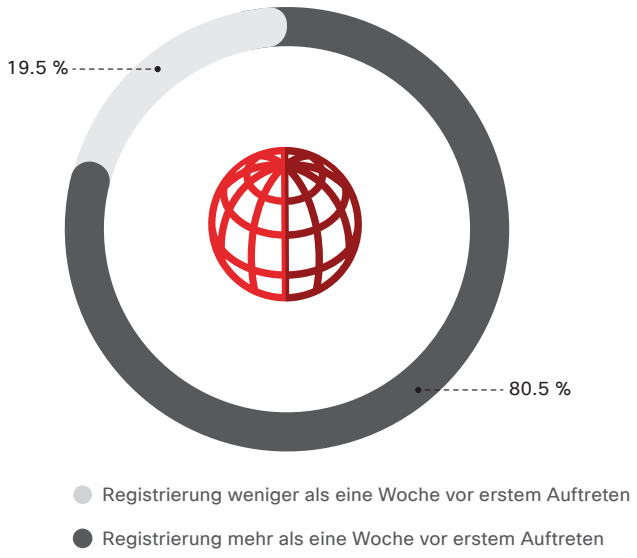
Quelle: Cisco Security Research

Das Ergebnis legt nahe, dass sich die meisten Angreifer bei der Erstellung neuer Domains für ihre Kampagnen vor allem für einen möglichst großen Gewinn interessieren, weshalb sie mehrere Kampagnen von einer einzelnen Domain aus starten. Die Domain-Registrierung kann kostspielig sein, wenn man bedenkt, wie viele die meisten Angreifer davon benötigen, um ihre Kampagnen durchzuführen und einer Entdeckung zu entgehen.

Ein Fünftel der schädlichen Domains kommt schnell zum Einsatz.

Gegner können tage-, monate- oder jahrelang nach der Registrierung auf ihren Domains ausharren und auf den richtigen Zeitpunkt warten. Allerdings stellten Cisco Bedrohungsforscher fest, dass ein bedeutender Prozentsatz der schädlichen Domains, etwa 20 Prozent, weniger als eine Woche nach der Registrierung für Kampagnen genutzt wurden (siehe Abbildung 20).

Abbildung 20 RLD-Registrierungszeiten

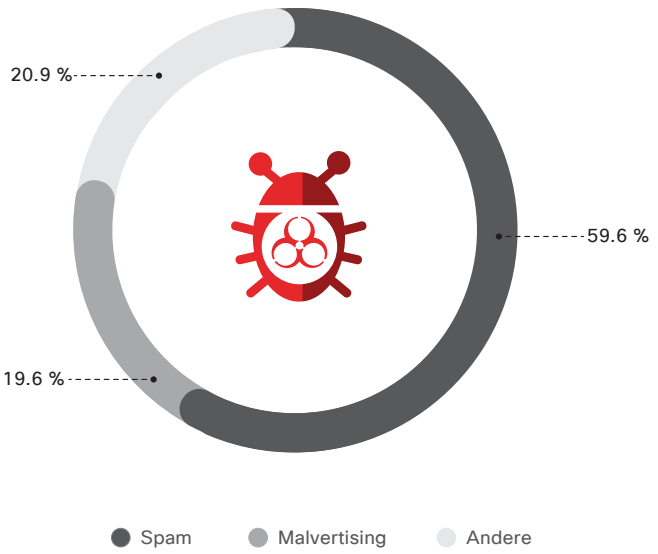


Quelle: Cisco Security Research

Viele neue Domains sind mit Malvertising-Kampagnen verbunden.

Die meisten von uns untersuchten schädlichen Domains (ca. 60 Prozent) hingen mit Spam-Kampagnen zusammen. Fast ein Fünftel der Domains waren mit Malvertising-Kampagnen verbunden (siehe Abbildung 21). Malvertising wird immer häufiger dazu eingesetzt, um Benutzer zu Exploit-Kits zu lotsen, auch solchen, die Ransomware verteilen.

Abbildung 21 Kategorisierung als schädlich



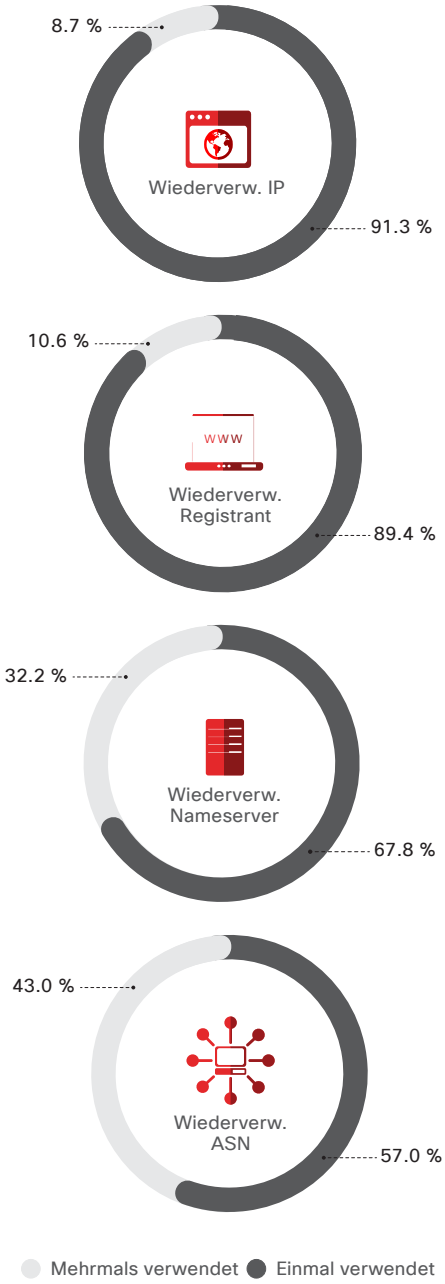
Quelle: Cisco Security Research

Zu den extrem häufig genutzten, domainspezifischen Techniken für die Erstellung von Malvertising-Kampagnen zählt das Domain Shadowing. Bei dieser Technik stehlen Angreifer legitime Domain-Anmeldeinformationen, um Subdomains zu erstellen, die auf schädliche Server verweisen. Eine andere Taktik ist der Missbrauch von kostenlosen, dynamischen DNS-Services zur Erstellung schädlicher Domains und Subdomains. So können schädliche Payloads von sich andauernd ändernden Hosting-IPs bereitgestellt werden, entweder infizierte Benutzercomputer oder kompromittierte öffentliche Websites.

Domains verwenden Infrastrukturressourcen wieder.

Die schädlichen RLDs in unserer Stichprobe schienen auch Infrastrukturressourcen wiederzuverwenden, wie E-Mail-Adressen von sich registrierenden Personen, IP-Adressen, autonome Systemnummern (ASNs) und Namenserver (siehe Abbildung 22). Dies ist laut unseren Forschern ein weiterer Beweis dafür, dass Gegner versuchen, ihre Investitionen in neue Domains voll auszuschöpfen und Ressourcen zu schonen. Eine IP-Adresse kann beispielsweise von mehr als einer Domain verwendet werden. Bei der Vorbereitung einer Kampagne können Angreifer so z. B. in einige IP-Adressen und verschiedene Domain-Namen investieren, anstatt teure Server anzuschaffen.

Abbildung 22 Wiederverwendung der Infrastruktur durch schädliche RLDs



Quelle: Cisco Security Research

Die von den RLDs wiederverwendeten Ressourcen liefern Hinweise dafür, ob die Domain möglicherweise schädlich ist. Werden beispielsweise E-Mail-Adressen von sich registrierenden Personen oder IP-Adressen selten wiederverwendet, weist ein Muster einer regelmäßigen Wiederverwendung auf verdächtiges Verhalten hin. Bei der Blockierung dieser Domains werden die Verteidiger wahrscheinlich auf keine Probleme treffen, da es keine negativen geschäftlichen Auswirkungen gibt.

Die statische Blockierung von ASNs und Namenservern dürfte in den meisten Fällen weniger leicht umzusetzen sein. Allerdings lohnt es sich, Muster für die Wiederverwendung von RLDs näher zu untersuchen, um festzustellen, ob bestimmte Domains blockiert werden sollten.

Wenn Sicherheitsteams Cloud-Security-Tools der ersten Verteidigungslinie verwenden, um potenziell schädliche Domains und Subdomains zu identifizieren und analysieren, können sie den Weg eines Angreifers nachverfolgen und beispielsweise folgende Fragen beantworten:

- In welche IP-Adresse wird die Domain aufgelöst?
- Welche ASN ist mit dieser IP-Adresse verknüpft?
- Wer hat die Domain registriert?
- Welche anderen Domains sind mit dieser Domain verknüpft?

Die Antworten können Verteidigern nicht nur dabei helfen, Sicherheitsrichtlinien zu verfeinern und Angriffe abzuwehren, sondern auch Benutzer davon abzuhalten, sich innerhalb des Unternehmensnetzwerks mit schädlichen Webseiten im Internet zu verbinden.

DevOps-Technologien bedroht durch Ransomware-Angriffe

Im Jahr 2017 traten mit einer Kampagne im Januar erstmals DevOps-Ransomware-Angriffe auf, die gegen die Open-Source-Datenbankplattform MongoDB gerichtet waren.[16] Die Angreifer verschlüsselten öffentliche MongoDB-Instanzen und verlangten Lösegeldzahlungen für Entschlüsselungsschlüssel und -software. Kurze Zeit später konzentrierten sie sich auf die Kompromittierung von Datenbanken, wie CouchDB und Elasticsearch, mit serverorientierter Ransomware.

Rapid7 ist ein Cisco Partner und Anbieter von Sicherheitsdaten- und Analytiklösungen. Wie Rapid7-Forscher in unserem *Cisco Midyear Cybersecurity Report 2017* erklärten, werden DevOps-Services häufig nicht ordnungsgemäß bereitgestellt oder absichtlich offen gelassen, damit legitime Benutzer bequemer darauf zugreifen können. Das macht diese Services anfällig für Angriffe.

Rapid7 führt regelmäßige Internetsuchen nach DevOps-Technologien durch und katalogisiert sowohl offene als auch gegen Lösegeld freigekaufte Instanzen. Einige der DevOps-Services, die sie dabei finden, können personenbezogene Daten enthalten, die auf Namen aus Tabellen basieren, die über das Internet verfügbar sind.

Zur Reduzierung des Risikos von DevOps-Ransomware-Angriffen sollten Organisationen, die öffentliche Internetinstanzen von DevOps-Technologien nutzen, Folgendes tun:

- Solide Standards für eine sichere Bereitstellung von DevOps-Technologien erstellen
- Ein aktives Bewusstsein der öffentlichen Infrastruktur bewahren, die vom Unternehmen genutzt wird
- DevOps-Technologien mit Patches auf dem neuesten Stand halten
- Prüfungen auf Schwachstellen durchführen

Weitere Informationen zur Untersuchung von Rapid7 finden Sie im Abschnitt „Setzen Sie Ihr Geschäft keinem Risiko durch DevOps-Technologien aus“ im *Cisco Midyear Cybersecurity Report 2017.*

16 *After MongoDB, Ransomware Groups Hit Exposed Elasticsearch Clusters,* von Lucian Constantin, IDG News Service, 13. Januar 2017: **pcworld.com/article/3157417/security/after-mongodb-ransomware-groups-hit-exposed-elasticsearch-clusters.html.**

Insider-Bedrohungen nutzen die Cloud

In früheren Security Reports haben wir über den Nutzen von OAuth-Berechtigungen und Superuser-Privilegien gesprochen, mit denen festgelegt wird, wer in das Netzwerk darf und wie auf Daten zugegriffen werden kann.[17] Um die Auswirkungen der Benutzeraktivität auf die Sicherheit weiter zu prüfen, untersuchten Cisco Bedrohungsforscher vor Kurzem die Trends beim Datendiebstahl. Sie wandten einen Algorithmus für maschinelles Lernen an, um Profile von 150.000 Benutzern in 34 Ländern zu erstellen, die alle zwischen Januar und Juni 2017 Cloud-Service-Provider nutzten. Der Algorithmus berücksichtigte nicht nur die Anzahl der heruntergeladenen Dokumente, sondern auch Variablen wie den Zeitpunkt des Downloads, IP-Adressen und Standorte.

Sechs Monate lang wurde das Benutzerverhalten überwacht. Danach untersuchten die Forscher eineinhalb Monate lang nach Auffälligkeiten und stellten bei 0,5 Prozent der Benutzer verdächtige Downloads fest. Das ist zwar nicht viel, aber diese Benutzer luden insgesamt über 3,9 Mio. Dokumente von unternehmenseigenen Cloud-Systemen herunter. Das sind pro Benutzer und Zeitraum durchschnittlich 5.200 Dokumente. Von den verdächtigen Downloads traten 62 Prozent außerhalb der üblichen Geschäftszeiten auf, 40 Prozent am Wochenende.

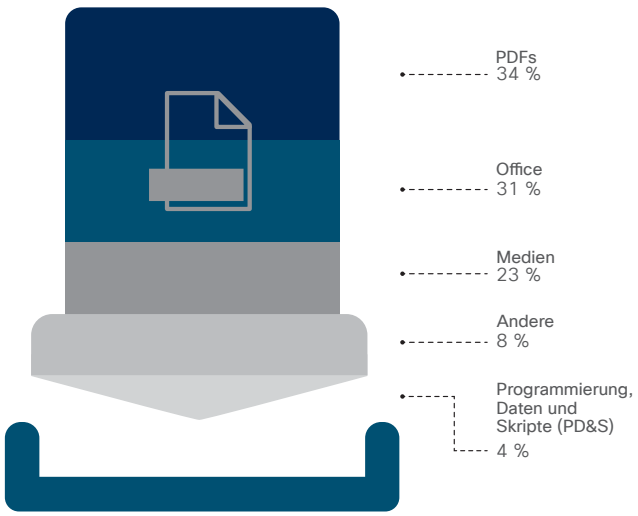
Cisco Forscher führten auch eine Text-Mining-Analyse von den Titeln der 3,9 Mio. heruntergeladenen verdächtigen Dokumente durch.

Eines der häufigsten Schlüsselwörter in den Dokumententiteln war „Daten“. Die Schlüsselwörter, die am häufigsten im Zusammenhang mit dem Wort „Daten“ auftauchten, waren „Mitarbeiter“ und „Kunde“. Bei den heruntergeladenen Dokumententypen handelte es sich bei 34 Prozent um PDFs und bei 31 Prozent um Microsoft Office-Dokumente (siehe Abbildung 23).

Die Anwendung von Algorithmen für maschinelles Lernen bietet einen differenzierten Blick auf Aktivitäten von Cloud-Benutzern, die über die Anzahl der Downloads hinausgeht. In unserer Analyse wurden 23 Prozent der untersuchten Benutzer mehr als dreimal wegen verdächtigen Downloads markiert; das fing normalerweise mit einer kleinen Dokumentenzahl an. Die Anzahl stieg jedes Mal langsam an, bis diese Benutzer schließlich plötzliche und auffällige Download-Spitzen erkennen ließen (Abbildung 24).

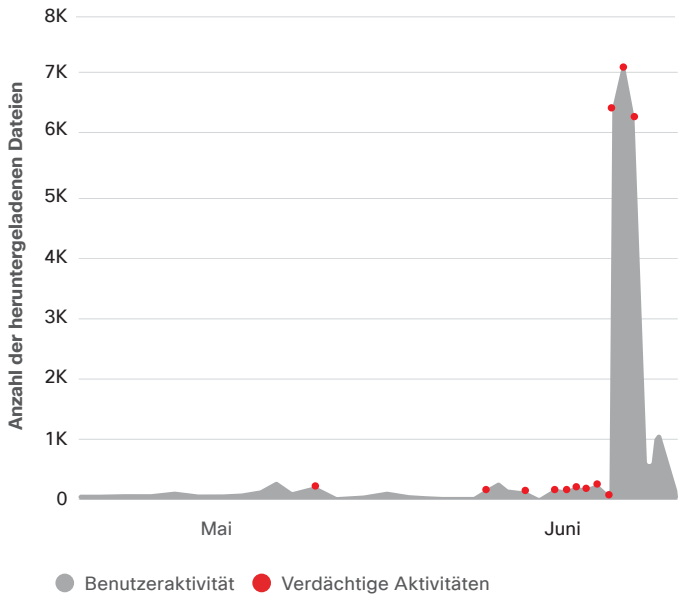
Algorithmen für maschinelles Lernen versprechen tiefere Einblicke in die Cloud und das Nutzerverhalten. Kann dieses Download-Verhalten vorhergesagt werden, sparen sich die Verteidiger den Aufwand für die Untersuchung des legitimen Verhaltens. Außerdem können sie einschreiten, um einen potenziellen Angriff oder einen Datendiebstahl zu vermeiden, bevor dieser eintritt.

Abbildung 23 Am häufigsten heruntergeladene Dokumente



Quelle: Cisco Security Research

Abbildung 24 Algorithmen für maschinelles Lernen erfassen verdächtiges Downloadverhalten von Benutzern



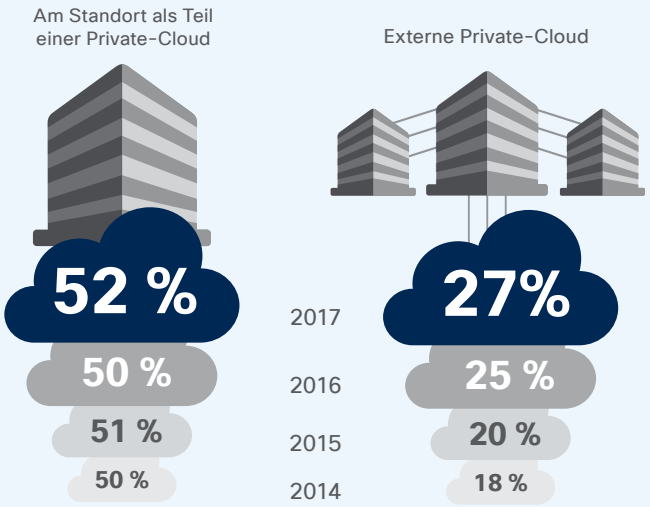
Quelle: Cisco Security Research

17 *Cisco Midyear Cybersecurity Report 2017*: cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

Cisco Security Capabilities Benchmark Study 2018: Sicherheit gilt als wichtiger Vorteil von Hosting-Netzwerken in der Cloud

Die Verwendung von On-premise- und Public-Cloud-Infrastrukturen nimmt laut der Cisco Security Capabilities Benchmark Study 2018 zu, obwohl viele Organisationen noch immer auf reine On-premise-Netzwerke setzen. In der Studie von 2017 gaben 27 Prozent der Sicherheitsexperten an, dass sie externe Private Clouds verwenden; 2016 waren es 25 Prozent und 2015 noch 20 Prozent (Abbildung 25). 52 Prozent erklärten, dass ihre Netzwerke on-premise als Teil der Private Cloud gehostet werden.

Abbildung 25 Mehr Unternehmen nutzen Private Clouds



2014 (n=1727), 2015 (n=2417), 2016 (n=2887), 2017 (n=3625)

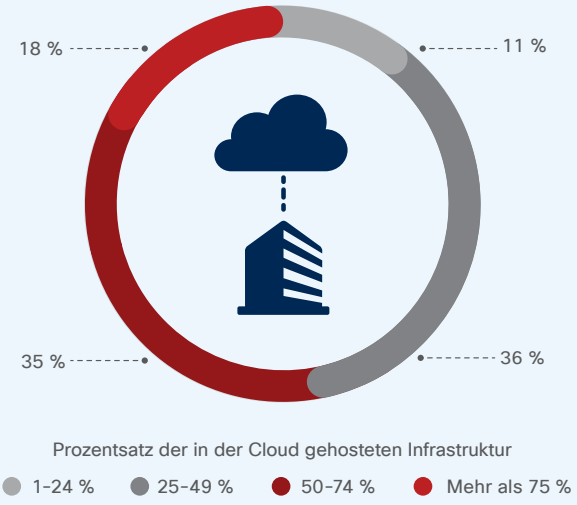
Quelle: Cisco Security Capabilities Benchmark Study 2018

Unter den Organisationen mit Cloud-Bereitstellungen hosten 36 Prozent 25 bis 49 Prozent ihrer Infrastruktur in der Cloud; 35 Prozent wiederum hosten 50 bis 74 Prozent ihrer Infrastruktur in der Cloud (Abbildung 26).

Dem befragten Sicherheitspersonal zufolge ist Sicherheit der Hauptvorteil von in der Cloud gehosteten Netzwerken. Unter ihnen gaben 57 Prozent an, dass sie Netzwerke wegen der besseren Datensicherheit in der Cloud hosten; 48 Prozent führen die Skalierbarkeit an und 46 Prozent die Benutzerfreundlichkeit (siehe Abbildung 27).

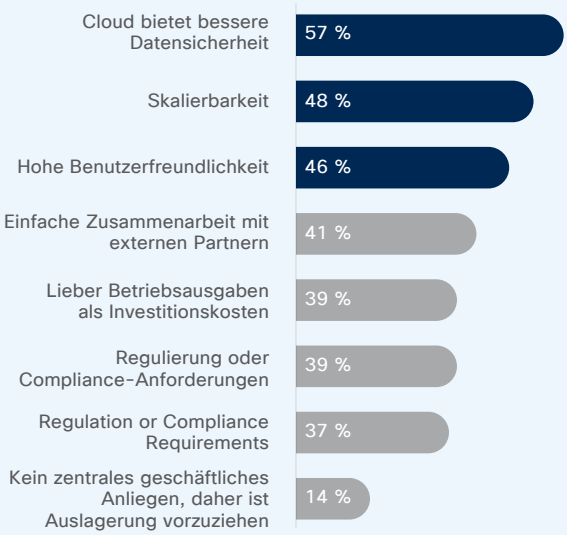
Die Befragten merkten außerdem an, dass sie mit der zunehmenden Verlegung der Infrastruktur in die Cloud überlegen, in CASBs (Cloud Access Security Broker) zu investieren, um die Cloud-Umgebungen noch sicherer zu machen.

Abbildung 26 53 Prozent der Organisationen hosten mindestens die Hälfte der Infrastruktur in der Cloud



Quelle: Cisco Security Capabilities Benchmark Study 2018

Abbildung 27 57 Prozent glauben, dass die Cloud eine bessere Datensicherheit bietet



Quelle: Cisco Security Capabilities Benchmark Study 2018

Grafiken für 2018 hier herunterladen: cisco.com/go/acr2018graphics

IoT- UND DDoS-ANGRIFFE

Das IoT steht noch immer am Beginn seiner Entwicklung. Aber bereits jetzt nutzen Angreifer die Sicherheitsschwachstellen in IoT-Geräten aus, um sich Zugang zu Systemen zu verschaffen. Dazu zählen auch Systeme zur Fertigungs- und Prozessautomatisierung, die eine kritische Infrastruktur unterstützen. IoT-Botnets nehmen an Größe und Wirkung zu und sind zunehmend in der Lage, heftige Angriffe zu verursachen, die das Internet stark beeinträchtigen könnten. Die Angreifer konzentrieren sich aktuell auf eine intensivere Ausnutzung der Anwendungsebene. Diese scheint ihr neues Ziel zu sein. Viele Sicherheitsexperten sind sich der Bedrohung durch IoT-Botnets nicht bewusst oder halten sie für nicht so wichtig. In vielen Organisationen werden der IT-Umgebung immer mehr IoT-Geräte hinzugefügt, ohne dabei groß (oder überhaupt!) an die Sicherheit zu denken. Sie nehmen sich auch nicht die Zeit, um zu prüfen, wie viele IoT-Geräte überhaupt mit ihrem Netzwerk verknüpft sind. Auf diese Weise machen sie es Gegnern leicht, die Kontrolle über das IoT zu übernehmen.

Nur wenige Unternehmen betrachten IoT-Botnets als unmittelbare Gefahr – das sollten sie aber

Genauso, wie sich das IoT immer weiter ausweitet und entwickelt, werden auch die IoT-Botnets immer ausgereifter und umfangreicher, um immer größere und intensivere DDoS-Angriffe zu starten. Radware, ein Cisco Partner, stellte für den *Cisco Midyear Cybersecurity Report 2017* eine Analyse der drei größten IoT-Botnets Mirai, BrickerBot und Hajime zur Verfügung. Auch in unserem aktuellen Bericht greifen wir das Thema erneut auf, um den Ernst dieser Bedrohung zu unterstreichen.[18] Die Untersuchungen unseres Partners zeigen, dass nur 13 Prozent der Organisationen glauben, dass IoT-Botnets im Jahr 2018 eine große Bedrohung für sie darstellen.

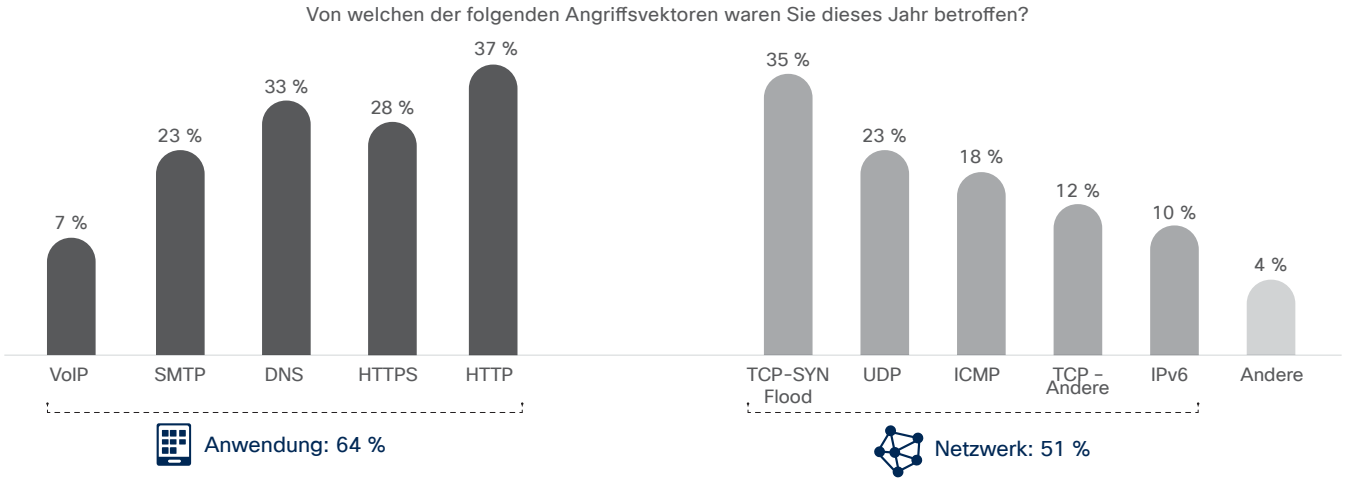
IoT-Botnets sind deshalb so erfolgreich, weil Organisationen und Benutzer schnell kostengünstige IoT-Geräte bereitstellen, ohne sich um den Sicherheitsaspekt zu kümmern. IoT-Geräte sind Linux- und Unix-basierte Systeme, deshalb sind sie häufig das Ziel von Binärdateien im ELF-Format (Executable and Linkable; ausführ- und verknüpfbar). Über sie lässt sich auch einfacher die Kontrolle übernehmen als über einen PC und das bedeutet, dass Gegner ganz einfach und schnell eine große Armee aufbauen können.

IoT-Geräte sind rund um die Uhr in Betrieb und können in kürzester Zeit aktiviert werden. Während die Gegner ihre IoT-Botnets weiter vergrößern, investieren sie in raffiniertere Codes und Malware und konzentrieren sich auf erweiterte DDoS-Angriffe.

DDoS-Angriffe auf Anwendungs- und Netzwerkebene

Angriffe auf Anwendungsebene nehmen zu, während Angriffe auf die Netzwerkschicht zurückgehen (siehe Abbildung 28). Radware-Forscher vermuten, dass diese Verschiebung auf die Zunahme von IoT-Botnets zurückzuführen ist. Ein bedenklicher Trend, da die Anwendungsschicht so vielfältig ist und über zahlreiche Geräte verfügt. Deshalb könnten Angriffe gegen diese Ebene möglicherweise große Teile des Internets zum Erliegen bringen.

Abbildung 28 Die Zahl der auf Anwendungen gerichteten DDoS-Angriffe nahm 2017 zu



Quelle: Radware

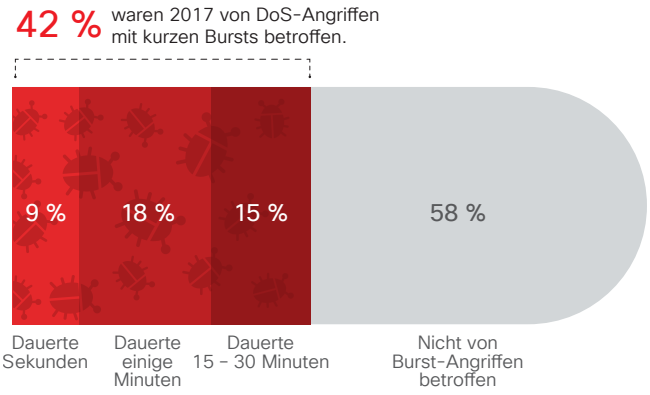
18 Weitere Informationen zu den Forschungsergebnissen über IoT-Botnets von Radware finden Sie im Abschnitt „Das Internet of Things (IoT) nimmt gerade erst Fahrt auf, aber die IoT-Botnets sind bereits zur Stelle" S. 39, *Cisco Midyear Cybersecurity Report 2017*: cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

Immer mehr Angreifer wenden sich der Anwendungsschicht zu, weil es laut Radware-Forschern auf der Netzwerkebene nur noch wenig zu holen gibt. Die Erstellung von IoT-Botnets ist auch weniger ressourcenintensiv als die von PC-Botnets. Das bedeutet, dass Gegner mehr Ressourcen in die Entwicklung von fortschrittlichen Codes und Malware investieren können, wie dies z. B. bei den Betreibern des Multivektor-Botnet Mirai der Fall war, das für seine erweiterten Anwendungsangriffe bekannt ist.

Komplexität, Häufigkeit und Dauer von „Burst-Angriffen“ nimmt zu

Einer der bedeutendsten DDoS-Angriffstrends, den Radware 2017 beobachtete, war die Zunahme von kurzen Burst-Angriffen, die immer komplexer, häufiger und andauernder werden. 42 Prozent der von Radware befragten Organisationen waren 2017 von dieser Art DDoS-Angriff betroffen (Abbildung 29). Bei den meisten Angriffen dauerten die wiederholten Bursts nur wenige Minuten an.

Abbildung 29 DDoS-Angriffe mit wiederkehrenden „Bursts“



Quelle: Radware

Burst-Taktiken richten sich typischerweise gegen Gaming-Websites und Service-Provider, weil diese Ziele stark von der Serviceverfügbarkeit abhängig sind und derartigen Angriffsmanövern nicht standhalten können. Pünktliche oder zufällige Bursts mit hohem Datenverkehrsaufkommen, die über mehrere Tage oder sogar Wochen auftreten, geben Organisationen keine Möglichkeit zu reagieren und sorgen für ernsthafte Serviceausfälle.

Radware-Forscher machen die folgenden Angaben zu Burst-Angriffen:

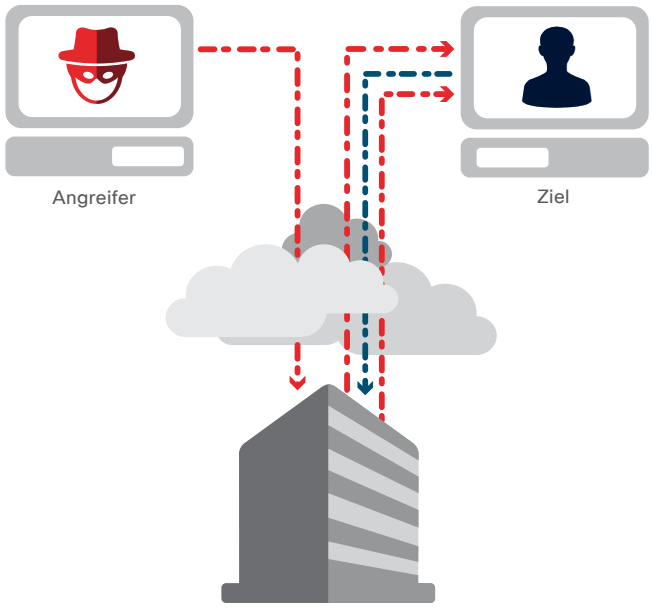
- Sie bestehen aus mehreren veränderlichen Vektoren. Die Angriffe sind geografisch verteilt und machen sich als eine Reihe präziser SYN-, ACK- und UDP-Floods (User Datagram Protocol) mit hohem Volumen an mehreren Ports bemerkbar.
- Sie kombinieren umfangreiche Angriffe mit variierenden Zeitspannen – zwei bis 50 Sekunden mit hohen Datenverkehrsspitzen in Intervallen von ca. fünf bis 15 Minuten.
- Sie werden häufig mit anderen länger andauernden DDoS-Angriffen kombiniert.

Zunahme von Reflection/Amplification-Angriffen

Ein weiterer DDoS-Trend, den Radware im Verlauf des Jahres 2017 beobachtete, ist die Zunahme von Reflection/Amplification-DDoS-Angriffen als bedeutender Vektor gegen ein breit gefächertes Servicespektrum. Laut Radware waren 2017 zwei von fünf Unternehmen von Reflection/Amplification-Angriffen betroffen. Ein Drittel dieser Organisationen berichtete, dass sie diese Angriffe nicht eindämmen konnten.

Ein Reflection/Amplification-Angriff nutzt eine potenziell legitime Komponente eines Drittanbieters, um Angriffsdatenverkehr an ein Ziel zu senden und so die Identität des Angreifers zu verschleiern. Angreifer senden Pakete an die Reflektor-Server mit einer Quell-IP-Adresse, die als IP-Adresse des Zielbenutzers gesetzt ist. Dadurch ist es möglich, das Ziel indirekt mit Antwortpaketen zu überhäufen und die vom Ziel genutzten Ressourcen zu erschöpfen (siehe Abbildung 30).

Abbildung 30 Reflection/Amplification-Angriff



Quelle: Radware

Damit Gegner erfolgreiche Reflection/Amplification-Angriffe durchführen können, brauchen sie eine höhere Bandbreitenkapazität als ihre Ziele. Möglich machen das die Reflektor-Server: Der Angreifer reflektiert einfach den Datenverkehr von einer oder mehreren Drittanbietersystemen. Da es sich bei diesen um gewöhnliche Server handelt, kann diese Art Angriff nur sehr schwer eingedämmt werden. Typische Beispiele hierfür sind:

DNS-Amplification/Reflection-Angriffe
Dieser raffinierte Denial-of-Service-Angriff nutzt das Verhalten eines DNS-Servers, um den Angriff zu verstärken. Eine standardmäßige DNS-Abfrage ist kleiner als das DNS-Antwortpaket. Bei einem DNS-Amplification/Reflection-Angriff wählt der Angreifer sorgfältig eine DNS-Abfrage, die zu langwierigen Antwortpaketen führt und bis zu 80 Mal länger dauert als die Abfrage (zum Beispiel „ANY"). Der Angreifer sendet diese Abfrage mit einem Botnet eines Drittanbieter-DNS-Servers und verschleiert die Quell-IP-Adresse mit der IP-Adresse des Zielbenutzers. Die Drittanbieter-DNS-Server senden daraufhin ihre Antwortpakete an die IP-Adresse des Ziels. Mit dieser Angriffstechnik kann ein relativ kleines Botnet eine wahre Flut an großen Antwortpaketen an das Ziel weiterleiten.

NTP-Reflection-Angriff
Bei dieser Art des Amplification-Angriffs werden öffentlich zugängliche NTP-Server (Network Time Protocol) ausgenutzt, um Verteidiger mit UDP-Datenverkehr zu überfluten und überlasten. NTP ist ein altes Netzwerkprotokoll für die Uhrzeitsynchronisierung zwischen Computersystemen über paketbasierte Netzwerke. Es wird im Internet immer noch weithin von Desktops, Servern und sogar Telefonen zur Uhrzeitsynchronisierung verwendet. Einige alte NTP-Serverversionen enthalten einen Befehl namens „monlist", mit dem die anfordernde Person eine Liste der letzten 600 Hosts beziehen kann, die sich mit dem abgefragten Server verbunden haben.

Ein einfaches Szenario: der Angreifer sendet wiederholt eine „get monlist"-Anfrage an einen beliebigen NTP-Server und verschleiert die Quell-IP-Adresse für den anfragenden Server als Zielserver. Die Antwortpakete des NTP-Servers werden dann an den Zielserver geleitet und sorgen für einen deutlichen Anstieg des UDP-Datenverkehrs am Quell-Port 123.

SSDP-Reflection-Angriff
Bei dieser Angriffsvariante wird das SSDP (Simple Service Discovery Protocol) ausgenutzt, das zur Suche nach UPnP-Geräten (Universal-Plug-and-Play) dient. Es ermöglicht außerdem die Erkennung und Ansteuerung von vernetzten Geräten und Diensten, wie Kameras, vernetzten Druckern und vielen anderen elektronischen Geräten.

Sobald sich ein UPnP-Gerät mit einem Netzwerk verbindet und eine IP-Adresse erhalten hat, kann es anderen Computern im Netzwerk seine Dienste mitteilen, indem es eine Nachricht über ein Multicast-IP-Protokoll versendet. Wenn ein Computer diese Nachricht über das Gerät erhält, sendet er eine Anforderung für eine vollständige Beschreibung der Gerätedienste. Das UPnP-Gerät reagiert dann umgehend auf diesen Computer und schickt eine vollständige Liste mit den angebotenen Diensten.

Wie bei NTP- und DNS-Amplification-DDos-Angriffen auch, kann der Angreifer ein kleines Botnet nutzen, um die letzte Dienstanfrage abzurufen. Der Angreifer verschleiert dann die Quell-IP-Adresse als IP-Adresse des Zielbenutzers und leitet die Antwortpakete direkt an das Ziel weiter.

Verteidiger müssen „Leak-Pfade“ beseitigen

Cisco Partner Lumeta definiert einen Leak-Pfad als eine Richtlinien- oder Segmentierungsverletzung oder als nicht autorisierte oder falsch konfigurierte Verbindung zum Internet in einem Unternehmensnetzwerk (auch zur Cloud), über die Datenverkehr an einen Ort im Internet – etwa eine schädliche Website – weitergeleitet werden kann. Diese unerwarteten Verbindungen können auch intern zwischen zwei verschiedenen Netzwerksegmenten auftreten, die nicht miteinander kommunizieren sollten. Beispielsweise könnte ein unerwarteter Leak-Pfad zwischen der Fertigungsebene und geschäftlichen IT-Systemen in kritischen Infrastrukturumgebungen auf schädliche Aktivitäten hinweisen. Leak-Pfade können auch eine Folge von fehlerhaft konfigurierten Routern und Switches sein.

Geräte, bei denen Berechtigungen nicht korrekt eingerichtet oder offen gelassen wurden, bzw. nicht verwaltet werden, sind anfällig für Angriffe. Geräte und Netzwerke, die zu einer nicht genehmigten IT oder einer Schatten-IT gehören, sind ebenfalls ein gefundenes Fressen für Gegner, weil diese in der Regel nicht verwaltet oder gepatcht werden. Lumeta schätzt, dass rund 40 Prozent der dynamischen Netzwerke, Endpunkte und Cloud-Infrastrukturen in Unternehmen zu erheblichen „blinden Flecken“ in der Infrastruktur führen, über die Sicherheitsteams keine Echtzeit-Einblicke erhalten.

Die Erkennung von vorhandenen Leak-Pfaden ist extrem wichtig, da diese jederzeit ausgenutzt werden können. Neu geschaffene Leak-Pfade müssen wiederum in Echtzeit erkannt werden, da sie umgehend Kompromittierungen erkennen lassen und mit raffinierten Angriffen (einschließlich Ransomware) im Zusammenhang stehen.

Die kürzlich von Lumeta durchgeführte Analyse der IT-Infrastruktur in über 200 Organisation und mehreren Ländern hebt die mangelnden Einblicke in die Endgeräte hervor. Sie zeigt außerdem, dass viele Unternehmen die Anzahl der Endgeräte in ihren IT-Umgebungen massiv unterschätzen (siehe Abbildung 31). Unkenntnis darüber, wie viele IP-fähige IoT-Geräte sich im Netzwerk befinden, ist häufig der Hauptgrund dafür, dass die Zahl der Endpunkte zu gering geschätzt wird.

Abbildung 31 Überblick über blinde Flecken in der Infrastruktur in verschiedenen Branchen

Tatsächliche Lumeta-Kunden	Behörden/ Verwaltung	Gesundheit	Tech	Finanzwesen
Angenommene Endpunkte	150,000	60,000	8000	600,000
Erkannte Endpunkte	170,000	89,860	14,000	1,200,000
Mangelnde Transparenz bei Endpunkten	12 %	33 %	43 %	50 %
Nicht verwaltete Netzwerke	3278	24	5	771
Nicht autorisierte oder ungesicherte Geräte für Weiterleitung	520	75	2026	420
Bekannte aber nicht erreichbare Netzwerke	33,256	4	16,828	45
Bei Bereitstellung identifizierte Leak-Pfade zum Internet	3000	120	9400	220

Quelle: Lumeta

Die Forscher von Lumeta vermuten, dass Leak-Pfade insbesondere in Cloud-Umgebungen häufiger auftreten werden, wo die Netzwerktransparenz eingeschränkt ist und weniger Sicherheitsmaßnahmen vorgesehen sind.

Angreifer nutzen die Leak-Pfade, die sie selbst erstellen oder finden, aber nicht immer sofort. Sie kehren oft auch erst nach einiger Zeit zu diesen Kanälen zurück und verwenden sie zur Installation von Malware oder Ransomware, um Informationen oder andere Daten zu stehlen. Der Grund, weshalb Leak-Pfade häufig unerkannt bleiben, liegt laut Lumeta darin, dass Angreifer bei der Verschlüsselung und Verschleierung ihrer Aktivitäten geschickt vorgehen, indem sie beispielsweise den Tor-Browser nutzen. Außerdem verwenden sie die Leaks sehr diskret, um Sicherheitsteams nicht auf sich aufmerksam zu machen.

Die Forschungsergebnisse von Lumeta besagen, dass die Qualifikationsdefizite in Sicherheitsteams und insbesondere der Mangel an grundlegenden Netzwerkkenntnissen daran schuld sind, dass Organisationen Leak-Pfade nicht rechtzeitig untersuchen und beseitigen können. Eine bessere Zusammenarbeit zwischen den Sicherheits- und Netzwerkteams kann dabei helfen, die Untersuchung und Beseitigung von Leak-Pfaden zu beschleunigen.

Automatisierungstools, die einen Netzwerkkontext bieten, gewähren Sicherheitsexperten ebenfalls Einblicke in mögliche Leak-Pfade. Darüber hinaus kann die Implementierung geeigneter Segmentierungsrichtlinien Sicherheitsteams dabei helfen zu entscheiden, ob eine unerwartete Kommunikation zwischen Netzwerken oder Geräten schädlich ist.

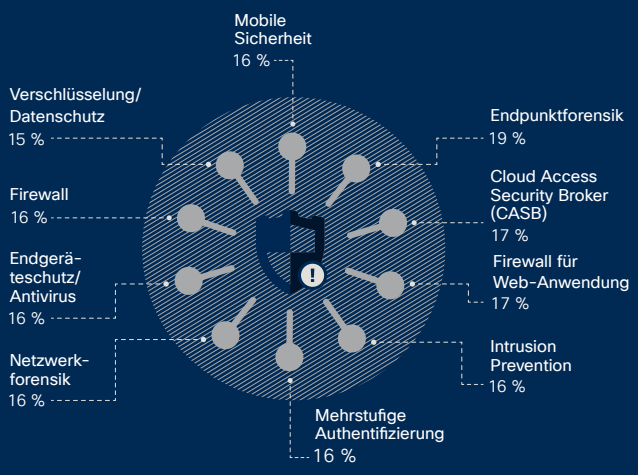
Cisco Security Capabilities Benchmark Study 2018: Mangel an Sicherheitspersonal hindert viele Organisationen daran, neue Cyberfunktionen zu implementieren

Ernst zu nehmende, personelle Engpässe bleiben für Verteidiger weiterhin ein großes Problem. Wie oben bereits erwähnt, können Qualifikationsdefizite eine Organisation daran hindern, bestimmte Arten von Bedrohungen zu untersuchen und zu beheben.

Ohne geeignetes Personal sind Verteidiger auch nicht in der Lage, neue Technologien und Prozesse bereitzustellen, die eine Stärkung des Sicherheitsstatus fördern (Abbildung 32).

Viele der für die Cisco Security Capabilities Benchmark Study 2018 befragten Sicherheitsexperten sagten, dass sie im Idealfall mehr routinemäßige Aktivitäten automatisieren oder auslagern würden, damit sich das Personal auf kritischere Aufgaben konzentrieren kann.

Abbildung 32 Wichtige Funktionen, die Verteidiger hinzufügen würden, wenn mehr Personal zur Verfügung stünde



Quelle: Cisco Security Capabilities Benchmark Study 2018

Grafiken für 2018 hier herunterladen: cisco.com/go/acr2018graphics

Systeme zur Fertigungs- und Prozessautomatisierung stellen Risiko für kritische Infrastrukturen dar

Systeme zur Fertigungs- und Prozessautomatisierung (ICS; Industrial Control System) sind das Kernstück aller Fertigungs- und Prozesssteuerungssysteme. Sie verbinden sich mit anderen elektronischen Systemen, die Teil eines Steuerungsprozesses sind, und bilden ein umfassend vernetztes System aus anfälligen Geräten, auf das es viele Angreifer abgesehen haben.

Laut TrapX Security, einem Cisco Partner und Hersteller von Cybersicherheitslösungen mit Deception-Technologie, stellen Angreifer, die auf Systeme zur Fertigungs- und Prozessautomatisierung abzielen, um die kritische Infrastruktur lahmzulegen, aktiv Recherchen an und erstellen Backdoor-Ausgangspunkte, um zukünftige Angriffe zu vereinfachen. Unter den potenziellen Cyberkriminellen finden sich Experten, die über umfangreiche Kenntnisse der IT-Systeme, ICS-Architekturen und die von ihnen unterstützten Prozesse verfügen. Einige wissen auch, wie Steuerungen für das PLM (Produktlebenszyklus-management) und für Subsysteme programmiert werden.

Die Bedrohungsforscher bei TrapX führten kürzlich Untersuchungen verschiedener Cyberangriffe durch, die gegen die ICS von Kunden gerichtet waren. Dadurch sollten unerwartete Probleme bei der Verteidigung hervorgehoben werden. Die zwei nachstehend beschriebenen Vorfälle ereigneten sich 2017 und werden immer noch untersucht.

Ziel: ein großes internationales Unternehmen für Wasseraufbereitung und Abfallverwertung

Angreifer nutzten den DMZ-Server des Unternehmens als Ausgangspunkt, um das interne Netzwerk zu kompromittieren. Das Sicherheitsteam erhielt Warnungen von Deception-Sicherheitstechnologie, die in den Netzwerk-DMZ integriert ist. Dieses physische oder logische Subnetz trennt interne Netzwerke von nicht vertrauenswürdigen Netzwerken wie dem Internet und schützt so andere interne Infrastrukturen. Die Untersuchung ergab Folgendes:

- Der DMZ-Server wurde aufgrund einer Fehlkonfiguration kompromittiert, die RDP-Verbindungen erlaubt.
- Nach der Kompromittierung wurde der Server über mehrere IPs von politischen „Hacktivisten“ gesteuert, die gegen diese Einrichtung sind.
- Die Angreifer konnten vom kompromittierten internen Netzwerk aus mehrere große Angriffe gegen diverse andere Anlagen des Unternehmens starten.

Ziel: ein Kraftwerk

Zu den kritischen Ressourcen dieses Kraftwerks zählen eine sehr große ICS-Infrastruktur und die erforderlichen SCADA-Komponenten (Supervisory Control And Data Acquisition), mit denen Prozesse verwaltet und ausgeführt werden. Die Anlage gilt als kritische nationale Infrastruktur und unterliegt der Kontrolle und Aufsicht der zuständigen nationalen Sicherheitsbehörde. Aus diesem Grund wird sie als Hochsicherheitsanlage betrachtet.

Der beteiligte CISO beschloss die Implementierung einer Deception-Technologie, um die Standard-IT-Ressourcen der Anlage vor Ransomware-Angriffen zu schützen. Die Technologie wurde zudem in der ICS-Infrastruktur angewandt. Bald danach erhielt das Sicherheitsteam mehrere Warnungen, die auf eine Verletzung der Systeme innerhalb der kritischen Infrastruktur für den Anlagenbetrieb hinwiesen. Die sofortige Untersuchung kam zu folgendem Ergebnis:

- Ein Gerät im Netzwerk für die Prozesssteuerung versuchte, mit den Deception-Traps zu interagieren, die als PLM-Controller getarnt waren. Hier wurde also in der Tat aktiv versucht, die genauen Funktionen und Prozesse des PLM-Controllers im Netzwerk abzurufen.
- Normalerweise würde das Gerät in diesem Fall deaktiviert werden, aber der für die Wartung verantwortliche Hersteller vergaß, die Verbindung wieder zu deaktivieren. Dieses Versehen führte dazu, dass das Netzwerk für die Prozesssteuerung nun anfälliger für Angreifer war.
- Die von den Gegnern gesammelten Informationen waren genau das, was sie brauchten, um den Anlagenbetrieb zu stören und dem weiteren Betrieb möglicherweise noch größeren Schaden zuzufügen.

Empfehlungen

Viele ICS-Verletzungen beginnen mit der Kompromittierung von anfälligen Servern und Rechenressourcen innerhalb des unternehmenseigenen IT-Netzwerks. Die Bedrohungsforscher bei TrapX empfehlen Organisationen, die folgenden Maßnahmen zu ergreifen, um Risiken zu reduzieren und die Integrität von Betriebsabläufen in ihren Anlagen sicherzustellen:

- Überprüfen Sie Hersteller und Systeme und sorgen Sie dafür, dass alle Patches und Updates umgehend angewendet werden. (Sind keine Patches verfügbar, sollten Sie die Migration zu einer neuen Technologie in Erwägung ziehen.)
- Reduzieren Sie die Verwendung von USB-Speichersticks und DVD-Laufwerken.
- Isolieren Sie ICS-Systeme von IT-Netzwerken. Lassen Sie keine direkten Verbindungen zwischen den beiden zu, beispielsweise Netzwerkverbindungen, Laptops und USB-Speichersticks.
- Implementieren Sie Maßnahmen, welche die Verwendung der ICS-Netzwerke für andere Zwecke als notwendige Betriebsabläufe deutlich einschränken. Schränken Sie den Zugriff auf ICS-Workstations und -Monitore über externe Internetbrowser ein. Rechnen Sie damit, dass diese Richtlinien fehlschlagen, und halten Sie einen Plan B bereit.
- Ermitteln und ersetzen Sie alle eingebetteten Kennwörter oder Standardkennwörter in Ihrem Produktionsnetzwerk. Implementieren Sie, wo möglich, eine Zwei-Faktor-Authentifizierung.
- Prüfen Sie Pläne für die Disaster Recovery nach einem großen Cyberangriff.

Weitere Anwendungsfälle finden Sie im TrapX Security-Forschungsbericht *Anatomy of an Attack: Industrial Control Systems Under Siege.*

Cisco Security Capabilities Benchmark Study 2018: Mehr OT- und IoT-Angriffe zu erwarten

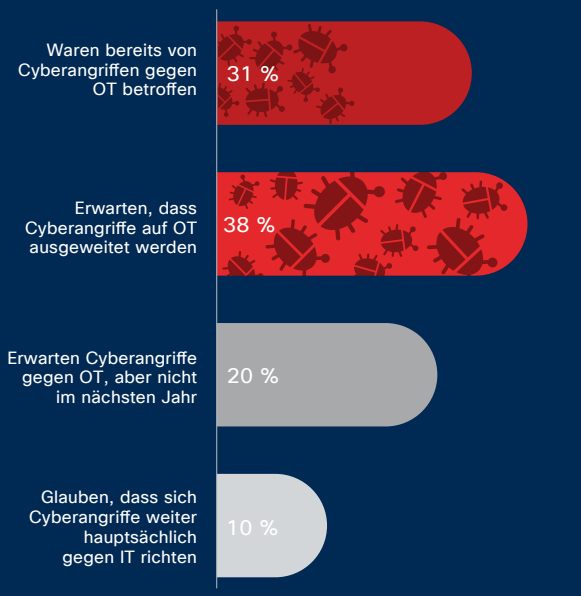
Angriffe auf die Betriebstechnik (OT; Operational Technology) wie ICS- und IoT-Geräte kamen noch nicht so häufig vor, weshalb viele Sicherheitsexperten sie noch gar nicht direkt miterlebt haben. Laut Untersuchungen für die **Cisco Security Capabilities Benchmark Study 2018** rechnen Sicherheitsexperten aber fest mit derlei Angriffen und versuchen herauszufinden, wie sie diesen begegnen können.

Häufig sind diese Systeme mit wenigen Schutzfunktionen und nicht gepatchter, veralteter Software ausgestattet, was sie für Angriffe anfällig macht.

„Wir verfügen noch über OT-Geräte, die schon 25 Jahre alt sind. Unsere Kompressoren und Maschinen sind stellenweise sogar schon 40 Jahre alt“, so ein Befragter. „IT-Fachleute kennen das Prozedere. Sie geben wichtige Informationen weiter, z. B. wenn Windows X nicht mehr unterstützt wird oder eine Oracle-Version ihren EOL-Status (End of Life) erreicht. Für die OT-Umgebung gibt es so etwas nicht.“

Nur wenige Sicherheitsexperten haben etwas Handfestes zur Absicherung der OT in ihren Organisationen zu sagen. Das liegt entweder daran, dass es keine bzw. nur eine recht eingeschränkte OT gibt oder weil es noch nicht viele IoT-Implementierungen gibt. Von diesen Fachleuten gaben 31 Prozent an, dass ihre Organisationen bereits von Cyberangriffen auf die OT-Infrastruktur betroffen waren, und 38 Prozent rechneten damit, dass sich Angriffe im nächsten Jahr von der IT auf die OT ausweiten würden (Abbildung 33).

Abbildung 33 31 Prozent der Unternehmen waren von Cyberangriffen auf die OT-Infrastruktur betroffen



Quelle: Cisco Security Capabilities Benchmark Study 2018

Grafiken für 2018 hier herunterladen: cisco.com/go/acr2018graphics

SCHWACHSTELLEN UND PATCHING

Diese vielen verschiedenen Sicherheitsrisiken können dazu führen, dass die Unternehmen Schwachstellen in ihrer Technologie übersehen. Wer sie nicht übersehen wird, sind die Gegner, die daraufhin berechnen, wie sie die potenzielle Schwachstelle durch einen Angriff bestmöglich ausnutzen.

Vor nicht allzu langer Zeit lautete die Best-Practice noch, dass bekannte Schwachstellen innerhalb von 30 Tagen gepatcht werden sollen. Wer heutzutage damit so lange wartet, könnte sein Angriffsrisiko erhöhen, denn die Angreifer erstellen und nutzen Exploits heute viel schneller. Unternehmen dürfen kleine Sicherheitslücken nicht vergessen, denn auch sie können, einmal von den Gegnern entdeckt, schwere Auswirkungen haben. Das gilt insbesondere für die Ausspähungsphase, wo potenzielle Angreifer nach Wegen in das System suchen.

Verbreitete Schwachstellen in 2017 – Buffer Overflow-Fehler, Apache Struts

Buffer Overflow-Fehler führten die Liste der CWE-Schwachstellen (Common Weakness Enumeration) an, die Cisco 2017 nachverfolgte. Allerdings gab es auch bei anderen Kategorien Bewegungen. Die Schwachstellen bei der Eingabevalidierung nahmen zu, während Pufferfehler zurückgingen (Abbildung 34).

Abbildung 34 Aktivitäten der CWE-Bedrohungskategorien

Bedrohungskategorien	Jan. – Sep. 2016	Jan. – Sep. 2017	Änderung
CWE-119: Buffer Errors	493	403	(-22 %)
CWE-20: Input Validation	227	268	+15 %
CWE-264: Permissions, Privileges and Access	137	163	+18 %
CWE-200: Information Leak/Disclosure	125	250	+100 %
CWE-310: Cryptographic Issues	27	17	(-37 %)
CWE-78: OS Command Injections	7	15	+114 %
CWE-59: Link following	5	0	

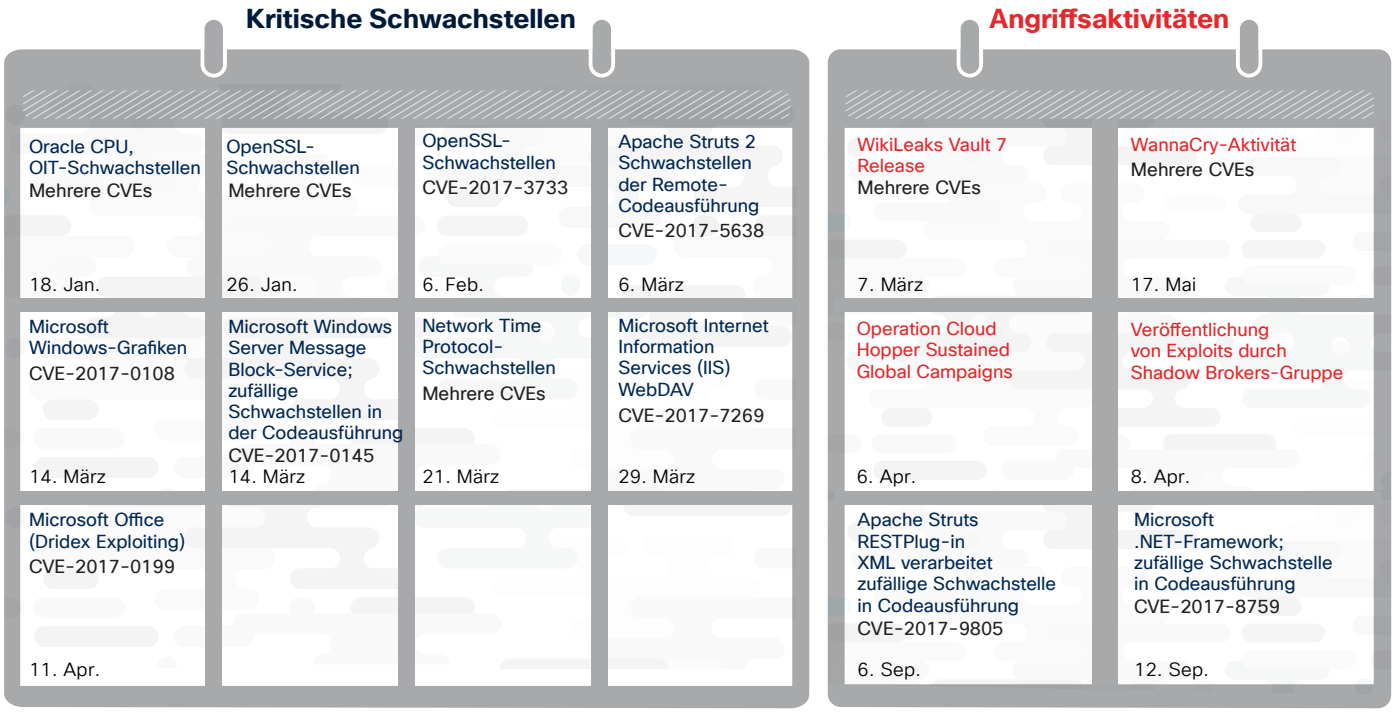
Quelle: Cisco Security Research

Die Untersuchung der kritischen Schwachstellen in (Abbildung 35) zeigt, dass Apache Struts-Schwachstellen im Jahr 2017 immer noch eine Rolle spielten. Apache Struts ist ein Open-Source-Framework für die Erstellung von Java-Anwendungen, das weit verbreitet ist. Apache Struts-Schwachstellen waren 2017 in mehrere Sicherheitsverletzungen bei großen Daten-Brokern involviert.

Zwar spürt Apache Schwachstellen auf und stellt schnell Patches bereit, doch kann sich das Patching von Infrastrukturlösungen wie Apache Struts ohne Verringerung der Netzwerkleistung als schwierig erweisen. Wie in einigen vorherigen Cisco Security Reports[19] bereits erwähnt wurde, können Schwachstellen in Open-Source-Software oder Software von Drittanbietern manuelle Patches erfordern, die dann womöglich nicht so häufig durchgeführt werden wie automatische Patches von Standardsoftware-Herstellern. Das verschafft den Angreifern deutlich mehr Zeit, um ihre Angriffe zu starten.

Tiefgreifende Scans von Betriebssystemen bis zur Bibliothek- oder Einzeldateiebene können Organisationen einen Überblick über die Komponenten von Open-Source-Lösungen geben.

Abbildung 35 Kritische Schwachstellen und Angriffsaktivitäten



Quelle: Cisco Security Research

Grafiken für 2018 hier herunterladen: cisco.com/go/acr2018graphics

19 *Cisco Midyear Cybersecurity Report 2017*: cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

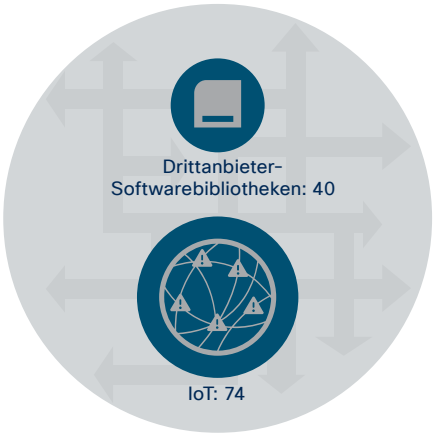
IoT- und Bibliotheksschwachstellen spielten 2017 eine große Rolle

Zwischen dem 1. Oktober 2016 und 30. September 2017 entdeckten Cisco Bedrohungsforscher 224 neue Schwachstellen in Produkten, die nicht von Cisco stammten. Davon betrafen 40 Schwachstellen die Softwarebibliotheken von Drittanbietern und 74 IoT-Geräte (Abbildung 36).

Die relativ große Anzahl an Schwachstellen in Bibliotheken deutet darauf hin, dass Lösungen von Drittanbietern, die das Framework für viele Unternehmensnetzwerke bereitstellen, näher untersucht werden müssen. Verteidiger sollten davon ausgehen, dass Softwarebibliotheken von Drittanbietern ein Angriffsziel darstellen könnten. Es reicht also nicht aus sicherzustellen, dass die aktuelle Softwareversion läuft oder dass keine offenen CVEs gemeldet wurden. Sicherheitsteams sollten Patches häufig kontrollieren und die Sicherheitsmaßnahmen von Drittanbietern überprüfen. Die Teams könnten zum Beispiel verlangen, dass die Hersteller Erklärungen zum Security Development Lifecycle vorlegen.

Eine weitere Best-Practice zur Prüfung von Drittanbietersoftware ist sicherzustellen, dass automatische Updates oder Update-Suchen sicher durchgeführt werden. Wenn beispielsweise ein Update initiiert wird, sollten Sicherheitsexperten sicher sein, dass die Kommunikation für diese Software über einen sicheren Kanal (wie SSL) erfolgt und die Software über eine digitale Signatur verfügt. Beide Maßnahmen sind erforderlich. Wenn nur digitale Signaturen verwendet werden, aber kein sicherer Kanal, könnte ein Angreifer den Datenverkehr abfangen und ein Update möglicherweise mit einer älteren Softwareversion ersetzen. Diese ist dann zwar digital signiert, könnte aber Schwachstellen enthalten. Wenn nur ein sicherer Kanal verwendet wird, könnte ein Angreifer womöglich den Updateserver des Herstellers kompromittieren und das Update durch Malware ersetzen.

Abbildung 36 Schwachstellen in Bibliotheken von Drittanbietern und im IoT



Gesamtzahl Schwachstellen: 224

Quelle: Cisco Security Research

Spectre und Meltdown: proaktive Vorbereitung kann die Behebung dieser Schwachstellen beschleunigen

Im Januar 2018 wurden die Schwachstellen Spectre und Meltdown bekannt. Diese ermöglichten den Angreifern eine Kompromittierung von Daten auf Plattformen, die über die neueste Generation von Computerprozessoren verfügen. Daraufhin gab es große Sorge, dass die Sicherheitsexperten keinen angemessenen Schutz vor diesen Angriffen bieten können. Mithilfe der Schwachstellen können Angreifer Anwendungsdaten im Arbeitsspeicher auf dem Chipsatz einsehen und großen Schaden anrichten, weil die betroffenen Mikroprozessoren in allem zu finden sind – vom Mobiltelefon bis zur Serverhardware.

Die Bedrohungen, die von Schwachstellen wie Spectre oder Meltdown ausgehen, machen deutlich, wie wichtig die Kommunikation mit Sicherheitsexperten über mögliche Lösungen, wie z. B. Patches, ist. Darüber hinaus muss sichergestellt werden, dass auch Drittanbieter, wie Cloud-Anbieter oder andere Anbieter der Lieferkette, Best-Practices einhalten, um durch Schwachstellen verursachte Sicherheitslücken zu schließen. Product Security Incident Response Teams, oder PSIRTs (wie das Cisco PSIRT), reagieren umgehend auf Ankündigungen von Schwachstellen, stellen Patches bereit und beraten Kunden, wie sie Risiken vermeiden können.

Anstatt zu hoffen, dass der Kelch an ihnen vorübergeht, müssen die Organisationen damit rechnen, dass Schwachstellen wie Spectre und Meltdown auch bei ihnen auftreten. Vorbereitung ist alles. Sie benötigen die entsprechenden Systeme, mit denen potenzielle Schäden gemindert werden können. Beispielsweise sollten Sicherheitsteams die von ihnen gesteuerten Geräte erfassen und Konfigurationen von verwendeten Funktionen dokumentieren. Denn einige Schwachstellen sind von der Konfiguration abhängig und beeinträchtigen die Sicherheit nur, wenn bestimmte Funktionen aktiviert sind.

Sicherheitsteams sollten auch Drittanbieter (z. B. Cloud-Anbieter) nach ihren Update- und Patching-Prozessen fragen. Organisationen müssen von ihren Cloud-Anbietern mehr Transparenz einfordern, was die Behebung derartiger Schwachstellen und die Reaktionsgeschwindigkeit auf Warnungen angeht. Letzten Endes sind die Organisationen selbst dafür verantwortlich, wie gut sie auf diese Fälle vorbereitet sind. Sie müssen mit PSIRT-Organisationen kommunizieren und Prozesse entwickeln, um schnell auf Schwachstellen reagieren zu können.

Weitere Informationen finden Sie im Talos Blog-Beitrag zu Spectre und Meltdown.

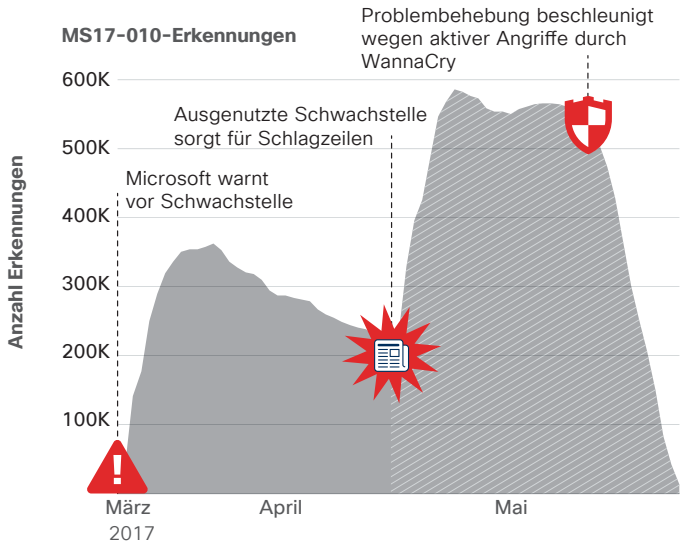
Aktive Exploits spornen Bemühungen zur Problembehebung an – IoT-Geräte sind aber ausgenommen

Qualys, Inc., ein Cisco Partner und Anbieter von Cloud-basierten Sicherheits- und Compliance-Lösungen, untersuchte rückblickend das Patch Management in Unternehmen vor und nach der WannaCry-Kampagne, von der im Mai 2017 viele Organisationen betroffen waren.

Der Ransomware-Kryptowurm WannaCry, von dem viele Sicherheitsexperten annehmen, dass er für die Löschung von Daten konzipiert wurde, nutzte eine Sicherheitslücke von Microsoft Windows namens EternalBlue, die von der Hackergruppe Shadow Brokers Mitte April 2017 veröffentlicht wurde. (Weitere Informationen zu diesem Thema finden Sie im Abschnitt „Die Bedrohung ist real: 2018 lauern neue, sich eigenständig verbreitende, netzwerkbasierte Bedrohungen“ auf Seite 6.)

Am 14. März 2017 veröffentlichte Microsoft ein Sicherheits-Update (MS17-010), das Benutzer auf eine kritische Schwachstelle im Microsoft Windows SMB Server hinwies. Abbildung 37 zeigt, wie die Anzahl der erkannten Geräte mit Schwachstellen Höchstwerte erreicht und dann zwischen Mitte März und April wieder langsam zurückgeht, weil Organisationen ihre Systeme überprüft und Patches angewendet haben.

Abbildung 37 Patching-Verhalten vor und nach der WannaCry-Kampagne



Quelle: Qualys

Grafiken für 2018 hier herunterladen: cisco.com/go/acr2018graphics

Allerdings musste eine beträchtliche Anzahl an Geräten ab Mitte April weiter ohne Patches auskommen. Am 14. April veröffentlichten die Shadow Brokers ein funktionierendes Exploit, das gegen die bekannte Schwachstelle in verschiedenen Microsoft Windows-Versionen gerichtet werden konnte. Abbildung 37 zeigt, dass sich die Anzahl der erkannten Geräte mit dieser Schwachstelle kurz darauf fast verdoppelte. Das passierte, als die Organisationen von dem Exploit sowie der Tatsache erfahren hatten, dass es unterstützte und nicht unterstützte Windows-Versionen beeinträchtigen konnte. Dies kam bei einer Remote-Prüfung von Qualys heraus, das einen Teil des Exploit-Codes verwendete.

Doch selbst nach der Veröffentlichung des Exploits wurden vor Mitte Mai, als die WannaCry-Kampagne weltweit für Schlagzeilen sorgte, keine flächendeckenden Patches angewendet. Abbildung 37 zeigt die steile Kurve für Problembehebungen nach dieser Kampagne. Ende Mai waren nur noch wenige nicht gepatchte Geräte übrig.

Die von Qualys durchgeführte Untersuchung des Patching-Verhaltens von Kunden zeigt, dass erst ein entscheidendes Ereignis eintreten muss, um viele Organisationen zum Patching kritischer Schwachstellen zu bewegen. Nicht einmal die Kenntnis eines aktiven Exploits reicht aus, um die Problembehebung zu beschleunigen. Im Fall der WannaCry-Kampagne hatten Unternehmen zwei Monate lang Zugriff auf das Patch für die Microsoft-Sicherheitslücke, bevor die Ransomware-Angriffe erfolgten.

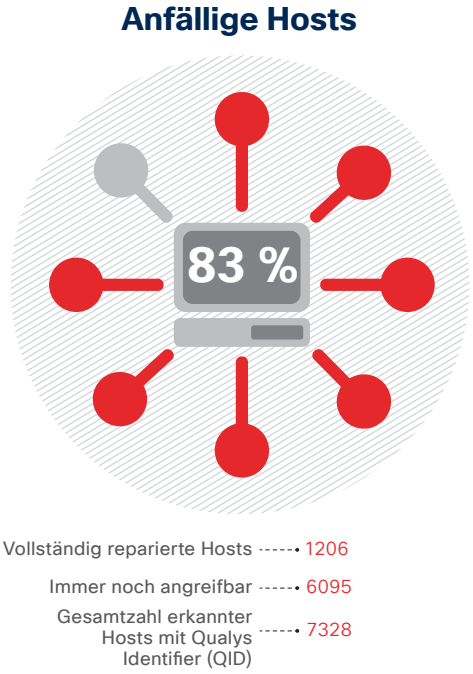
Ein weiterer Faktor war laut Forschern von Cisco und Qualys-Partner Lumeta, dass unbekannte, nicht verwaltete, nicht genehmigte und Schatten-IT-Endpunkte nicht gepatcht wurden. Diese blinden Flecken konnten Angreifer ausnutzen. Da Schwachstellenscanner diese Systeme nicht kannten, konnten sie keine Patches bewerten und empfehlen, was sie anfällig für WannaCry machte.

Patching für IoT-Geräte ist noch langsamer oder findet überhaupt nicht statt

Qualys untersuchte auch Patching-Trends für IoT-Geräte. Die Geräte in der Stichprobe enthielten IP-fähige HVAC Systeme, Türschlösser, Brandmeldeanlagen und Kartenleser.

Die Forscher untersuchten insbesondere IoT-Geräte, die für diverse bekannte Bedrohungen anfällig sind. Dazu gehört die Malware Devil's Ivy, die eine Schwachstelle in einem Stück Code namens gSOAP nutzt, welcher weithin für physische Sicherheitsprodukte verwendet wird; und Mirai, ein IoT-Botnet, das sich mittels Brute-Force-Angriffen gegen Telnet-Server mit Zielsystemen verbindet.

Abbildung 38 Trends beim Patching von IoT-Geräten



Quelle: Qualys

Qualys fand insgesamt 7328 Geräte, aber nur bei 1206 wurde der Fehler behoben (siehe Abbildung 38). Das bedeutet, dass 83 Prozent der IoT-Geräte in der Stichprobe noch kritische Schwachstellen aufweisen. Qualys fand zwar keinen Beweis dafür, dass Angreifer aktiv auf diese Schwachstellen abzielten, die Gefahr bestand aber. Die von dieser Gefahr betroffenen Unternehmen scheinen allerdings nicht motiviert, die Problembehebung zu beschleunigen.

Laut Qualys gibt es mehrere mögliche Erklärungen für diese Patching-Trägheit. Beispielsweise könnten einige Geräte nicht aktualisierbar sein. Andere wiederum könnten direkten Support durch den Hersteller erfordern. Darüber hinaus ist es nicht immer klar, wer in der Organisation für die Wartung von IoT-Geräten verantwortlich ist. Technikerteams, die sich beispielsweise um das HVAC-System eines Unternehmens kümmern, sind sich eventuell nicht bewusst, dass dieses System durch IT-Risiken beeinträchtigt werden kann, bzw. dass es IP-fähig ist.

Noch bedenklicher ist jedoch die geringe Anzahl an IoT-Geräten, die Qualys gefunden hat. Die tatsächliche Zahl dürfte wesentlich höher sein, weil Organisationen schlicht nicht wissen, wie viele IoT-Geräte mit ihrem Netzwerk verbunden sind. Dieser Mangel an Transparenz setzt sie einem hohen Kompromittierungsrisiko aus (siehe Seite 34 für weitere Informationen zu diesem Thema).

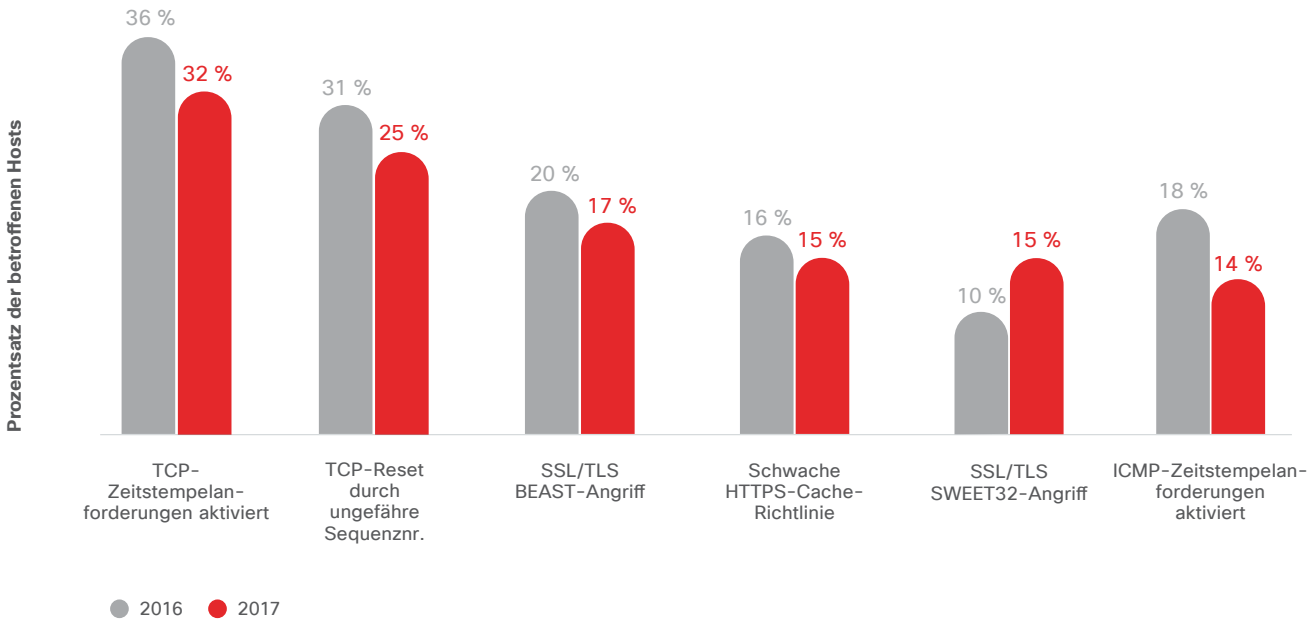
Ein erster Schritt zur Lösung dieses Problems ist eine Bestandsaufnahme aller IoT-Geräte im Netzwerk. Erst dann können Organisationen entscheiden, ob die Geräte scanbar sind und von Herstellern noch unterstützt werden. Außerdem lässt sich erkennen, welche Mitarbeiter im Unternehmen diese Geräte besitzen und verwenden. Die IoT-Sicherheit lässt sich außerdem verstärken, indem alle IoT-Geräte wie andere Rechengeräte behandelt werden. Dadurch wird sichergestellt, dass sie Firmware-Updates erhalten und regelmäßig gepatcht werden.

Die häufigsten Schwachstellen weisen einen niedrigen Schweregrad aber ein hohes Risiko auf

Laut Sicherheitsexperten der SAINT Corporation, einem Hersteller von Sicherheitslösungen und Cisco Partner, bleiben Schwachstellen mit niedrigem Schweregrad oft jahrelang unbeachtet, weil Unternehmen entweder nichts von ihnen wissen oder sie nicht als besondere Risiken betrachten. Diese kleinen, aber entscheidenden Sicherheitslücken könnten für Gegner jedoch das Einfallstor in Systeme sein.

SAINT untersuchte Daten zu Schwachstellen, die in den Jahren 2016 und 2017 von über 10.000 Hosts erfasst wurden. Das Unternehmen erstellte eine Liste mit Schwachstellen, die in allen untersuchten Organisationen am häufigsten gefunden wurden. Dabei kam heraus, dass Schwachstellen mit niedrigem Schwergrad am meisten auftraten (siehe Abbildung 39). (Hinweis: Einige der untersuchten Organisationen hatten mehr als einen Host.)

Abbildung 39 Am häufigsten erkannte Schwachstellen mit niedrigem Schweregrad, 2016-2017



Quelle: SAINT Corporation

Es folgt ein Überblick über die drei häufigsten Schwachstellen mit niedrigem Schweregrad aus Abbildung 39 und die Gründe, weshalb sie für Angreifer nützlich sein könnten:

TCP-Zeitstempelanfragen aktiviert
TCP-Zeitstempel liefern Informationen darüber, wie lange ein System ausgeführt wurde oder wann es zuletzt neu gestartet wurde. Dadurch könnten Gegner erfahren, über welche patchbare Schwachstellen das System möglicherweise verfügt. Außerdem könnten Softwareprogramme den Systemzeitstempel verwenden, um einen beliebigen Zufallszahlengenerator zu starten und Verschlüsselungsschlüssel zu erzeugen.

TCP-Reset nach ungefährer Sequenznummer
Remote-Angreifer können die Sequenznummern erraten und einen Denial-of-Service-Angriff für persistente TCP-Verbindungen verursachen. Dies geschieht durch die wiederholte Einspeisung von TCP RST-Paketen insbesondere in Protokolle, die auf langlebige Verbindungen wie das Border Gateway Protocol setzen.

„BEAST"-Angriff
Ein Angreifer kann die Schwachstelle BEAST (Browser Exploit Against SSL/TLS) nutzen, um einen MiTM-Angriff (Man-in-the-Middle) zu starten und damit geschützte Inhalte zu lesen, die zwischen Parteien ausgetauscht werden. (Hinweis: Die Durchführung dieses Angriffs ist kompliziert, da der Angreifer die Kontrolle über den Client-seitigen Browser haben muss, um Datenpakete schnell zu lesen und einzuspeisen.)

Die Sicherheitsexperten bei SAINT erkannten während der Untersuchung keine Gegner, die diese Schwachstellen mit niedrigem Schweregrad aktiv ausnutzten.

Die in Abbildung 39 gezeigten Schwachstellen sind der Security-Community bekannt. Einige von ihnen werden jedoch nicht unbedingt geflagged oder führen zu einer automatischen Warnung bei routinemäßigen Compliance-Prüfungen wie dem PCI DSS-Audit (Payment Card Industry Data Security Standard). Gemäß den für diese Branche relevanten Standards gelten sie nicht als kritische Schwachstellen. Jede Branche bewertet die Kritikalität von Schwachstellen anders.

Außerdem können die meisten der in Abbildung 39 gezeigten typischen Schwachstellen mit niedrigem Schweregrad nur schwer oder gar nicht durch das Patch-Management behoben werden. Das liegt daran, dass sie aus Problemen bei der Konfiguration oder mit Sicherheitszertifikaten entstanden sind (z. B. schwache SSL-Chiffren oder selbst signierte SSL-Zertifikate).

Organisationen sollten Schwachstellen mit niedrigem Schweregrad, die ein Risiko darstellen könnten, umgehend beheben. Sie sollten Prioritäten für die Problembehebung eher auf der Basis bewerten und identifizieren, wie sie Risiken empfinden, und sich nicht auf Bewertungen von Drittanbietern oder die teilweise Nutzung eines Bewertungssystems, wie CVSS, oder ein bestimmtes Compliance-Rating stützen. Nur die Organisationen selbst kennen ihre einzigartigen Umgebungen und ihre Strategien für das Risikomanagement.

ITeil II:
Die Verteidigungsstrategien

Teil II: Die Verteidigungsstrategien

Die Techniken der Angreifer entwickeln sich schneller weiter, als die der Verteidiger. Sie verwenden ihre Exploits, Umgehungsstrategien und Fertigkeiten zudem als Waffen und testen diese aus, um immer umfangreichere Angriffe zu starten. Die Frage lautet heute nicht, ob, sondern wann eine Organisation einem Cyberangriff ausgesetzt sein wird. Daher ist es für die Unternehmen wichtig, vorbereitet zu sein und sich von dem Angriff schnell wieder zu erholen. Das hängt weitgehend davon ab, welche Schritte sie heute unternehmen, um ihren Sicherheitsstatus zu stärken.

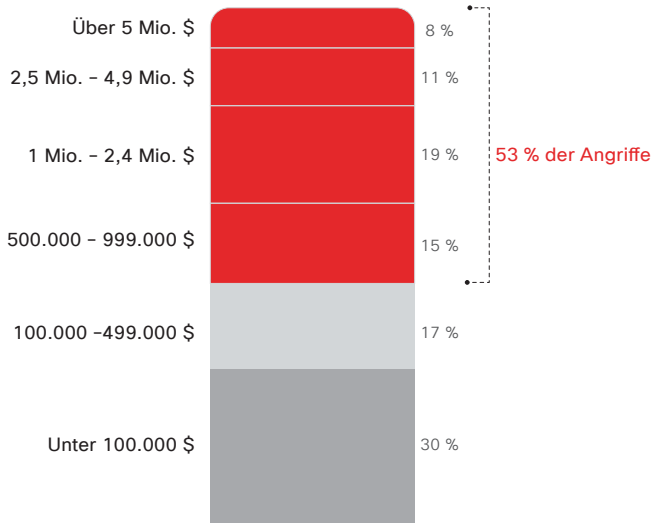
Die Ergebnisse unserer Cisco Security Capabilities Benchmark Study 2018 *ergaben, dass Verteidiger viel Arbeit vor sich haben und einige Herausforderungen meistern werden müssen. Wir haben CISOs (Chief Information Security Officers) und SecOp-Manager (Security Operations) von Unternehmen unterschiedlicher Größe und aus mehreren Ländern zu ihren Sicherheitsressourcen und -verfahren befragt, um zu ermitteln, wie diese den aktuellen Sicherheitsstatus ihrer Organisation einschätzen.*

Die Cisco Security Capabilities Benchmark Study 2018 beleuchtet die aktuell in Unternehmen eingesetzten Sicherheitsverfahren und vergleicht die Ergebnisse mit den 2017, 2016 und 2015 durchgeführten Erhebungen. An der Untersuchung waren mehr als 3.600 Befragte in 26 Ländern beteiligt.

Die Kosten eines Angriffs

Die Angst vor Sicherheitsverletzungen gründet auf den finanziellen Kosten der Angriffe, die längst nicht mehr hypothetisch sind. Sicherheitsverletzungen ziehen einen echten wirtschaftlichen Schaden nach sich, von dem sich die Unternehmen oft erst Monate oder sogar Jahre später wieder erholen. Laut den Untersuchungsteilnehmern führten mehr als die Hälfte aller Angriffe (53 Prozent) zu finanziellen Schäden von über 500.000 US-Dollar, unter anderem durch Verlust von Umsätzen, Kunden und Geschäftschancen sowie Out-of-Pocket-Zahlungen (Abbildung 40).

Abbildung 40 53 Prozent aller Angriffe führen zu Schäden von 500.000 US-Dollar oder mehr



Quelle: Cisco Security Capabilities Benchmark Study 2018

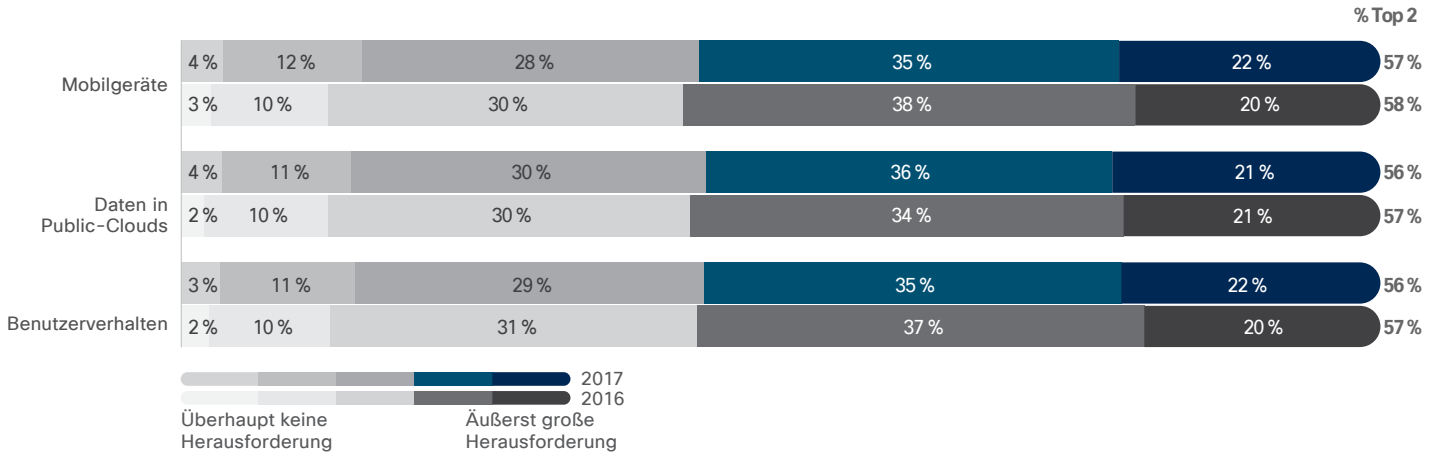
Grafiken für 2018 hier herunterladen: cisco.com/go/acr2018graphics

Herausforderungen und Hindernisse

Die Sicherheitsteams treffen bei ihren Bemühungen zum Schutz des Unternehmens auf zahlreiche Hindernisse. Es müssen gleich mehrere Bereiche und Funktionen verteidigt werden, was die Herausforderung nur noch größer macht.

Zu den am schwierigsten zu verteidigenden Bereichen und Funktionen zählen Mobilgeräte, Daten in der Public Cloud und das Benutzerverhalten (Abbildung 41).

Abbildung 41 Die am schwierigsten zu verteidigenden Bereiche: Mobilgeräte und Cloud-Daten

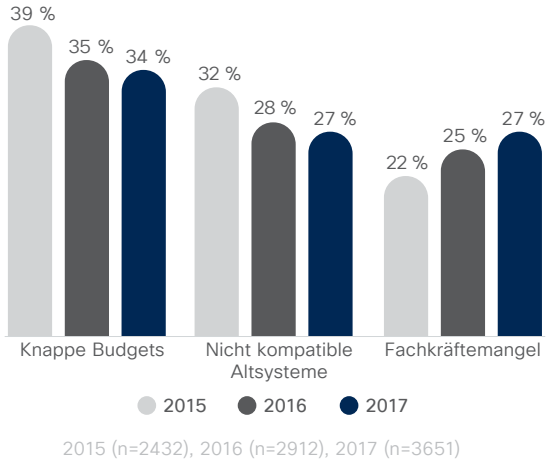


Quelle: Cisco Security Capabilities Benchmark Study 2018

Grafiken für 2018 hier herunterladen: cisco.com/go/acr2018graphics

Sicherheitsexperten geben die Faktoren Budget, Interoperabilität und Personal als die größten Herausforderungen beim Sicherheitsmanagement an (Abbildung 42). Der Mangel an Fachkräften wird ebenfalls als Herausforderung genannt, wenn es um die Einführung erweiterter Sicherheitsprozesse und -technologien geht. Im Jahr 2017 gaben 27 Prozent der Befragten den Fachkräftemangel als Problem an; 2016 waren es noch 25 Prozent und 2015 22 Prozent.

Abbildung 42 Das größte für die Sicherheit: budgetäre Einschränkungen

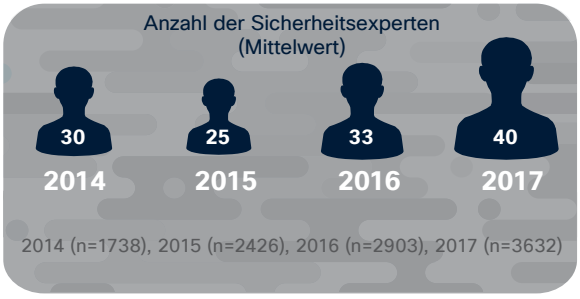


Quelle: Cisco Security Capabilities Benchmark Study 2018

In allen Branchen und Regionen steht der Fachkräftemangel ganz oben auf der Liste der Probleme. „Es wäre wirklich zu schön, wenn ich mit dem Zauberstab schwenken und 10 Prozent mehr Mitarbeiter einstellen könnte. Diese könnten dann Leute unterstützen, auf denen der größte Druck lastet, weil ihre speziellen Servicebereiche stark nachgefragt werden“, erklärt ein CISO eines großen Unternehmens für Professional Services.

Der Mangel an Fachkräften ist ja eine ständige Herausforderung, trotzdem berichten Organisationen, dass sie nach weiteren Ressourcen für ihre Sicherheitsteams suchen und diese einstellen. Im Jahr 2017 betrug die durchschnittliche Anzahl an Sicherheitsexperten in Organisationen 40 Mitarbeiter, das ist eine deutliche Zunahme im Vergleich zu 33 im Jahr 2016 (Abbildung 43).

Abbildung 43 Organisationen stellen mehr Sicherheitsexperten ein



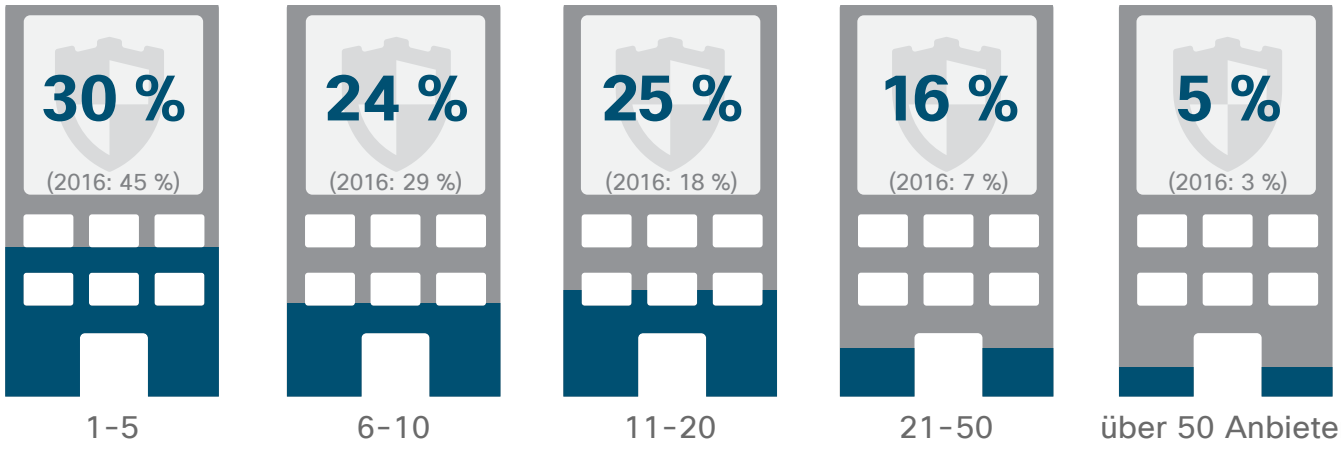
Quelle: Cisco Security Capabilities Benchmark Study 2018

Durch Hersteller verursachte Komplexität bei der Orchestrierung

Viele Verteidiger nutzen einen komplexen Mix aus Produkten von verschiedenen Herstellern; diese Fülle an Tools führt dazu, dass die Sicherheitslandschaft eher unübersichtlich als klarer wird. Diese Komplexität beeinflusst die Fähigkeit einer Organisation, Angriffe abzuwehren. Zum Beispiel steigt das Risiko von Verlusten.

Im Jahr 2017 gaben 25 Prozent der Sicherheitsexperten an, dass sie Produkte von 11 bis 20 Herstellern verwenden; im Jahr 2016 waren es noch 18 Prozent. Auch 2017 erklärten 16 Prozent, dass sie Produkte von 21 bis 50 Herstellern beziehen; 2016 waren es 7 Prozent (Abbildung 44).

Abbildung 44 Organisationen verwendeten 2017 mehr Anbieter von Sicherheitslösungen

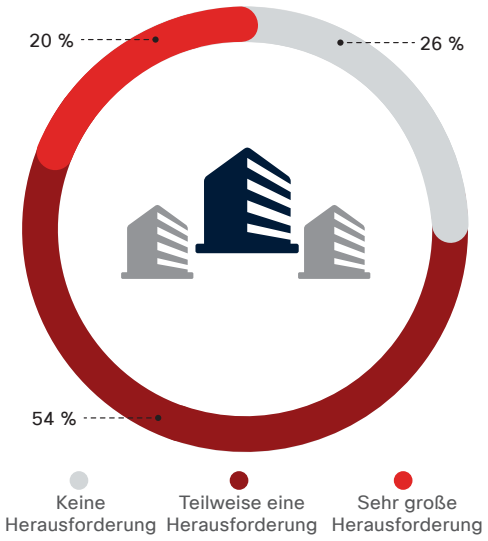


Quelle: Cisco Security Capabilities Benchmark Study 2018

Grafiken für 2018 hier herunterladen: cisco.com/go/acr2018graphics

Steigt die Anzahl der Hersteller, wird auch die Orchestrierung von Warnungen von diesen vielen Herstellerlösungen eine immer größere Herausforderung. Wie in Abbildung 45 dargestellt, gaben 54 Prozent der Sicherheitsexperten an, dass die Verwaltung mehrerer Warnungen unter diesen Umständen recht anspruchsvoll ist; für 20 Prozent sogar sehr schwierig.

Abbildung 45 Herausforderung bei der Orchestrierung von Warnmeldungen



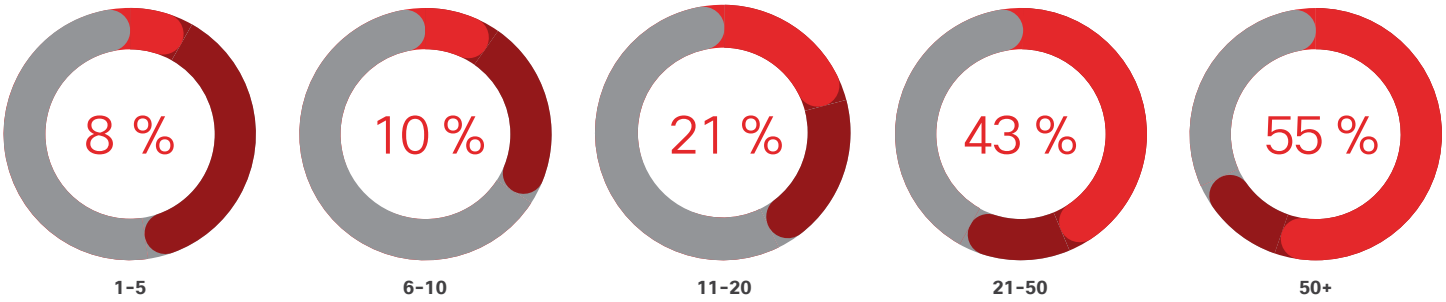
Quelle: Cisco Security Capabilities Benchmark Study 2018

Probleme der Security-Teams bei der Orchestrierung von Warnmeldungen unterschiedlicher Hersteller

Wie in Abbildung 46 zu sehen, gaben 8 Prozent der Organisationen mit Lösungen von nur 1 bis 5 Herstellern an, dass die Orchestrierung von Warnungen sehr anspruchsvoll ist. Bei Organisationen, die Lösungen von mehr als 50 Herstellern nutzen, sagten 55 Prozent, dass die Orchestrierung ein großes Problem darstellt.

Werden die erhaltenen Warnungen nicht orchestriert und nicht verstanden, könnten echte Bedrohungen unbemerkt ins System eindringen.

Abbildung 46 Zunehmende Anbieteranzahl erschwert die Orchestrierung von Sicherheitswarnungen



	Bildungswesen	Finanzsektor	Behörden/ Verwaltung	Gesundheit	Fertigung	Pharmaindustrie	Einzelhandel	Telekommunikation	Transport- und Verkehrswesen	Versorgung/ Energie
Sehr große Herausforderung	17 %	24 %	16 %	42 %	14 %	25 %	19 %	14 %	12 %	27 %

Quelle: Cisco Security Capabilities Benchmark Study 2018

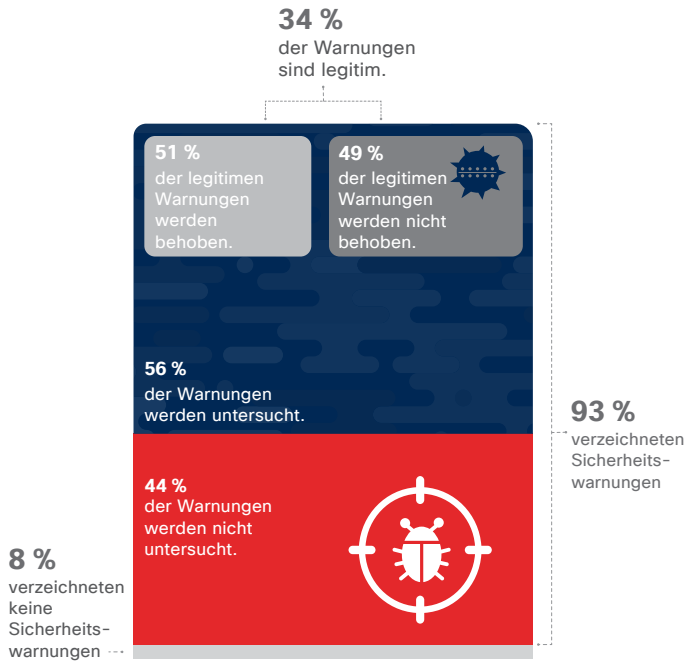
Grafiken für 2018 hier herunterladen: cisco.com/go/acr2018graphics

Die Informationen der Befragten zeigen, dass die Lücken zwischen Warnungen, die erzeugt, untersucht und schließlich behoben wurden, weiter bestehen bleiben. Siehe Abbildung 47:

- In Organisationen, die täglich Sicherheitswarnungen erhalten, werden durchschnittlich 44 Prozent dieser Warnungen nicht untersucht.
- Von den untersuchten Warnungen werden 34 Prozent als legitim erachtet.
- Von diesem Anteil werden wiederum 51 Prozent behoben.
- Fast die Hälfte (49 Prozent) der legitimen Warnungen werden nicht behoben.

Bei dieser Vorgehensweise bleiben zahlreiche legitime Warnungen unbearbeitet. Ein Grund dafür scheint der Mangel an Personal und Fachkräften zu sein, welche die Untersuchung aller Warnungen vereinfachen könnten.

Abbildung 47 Viele Warnungen werden nicht untersucht oder behoben

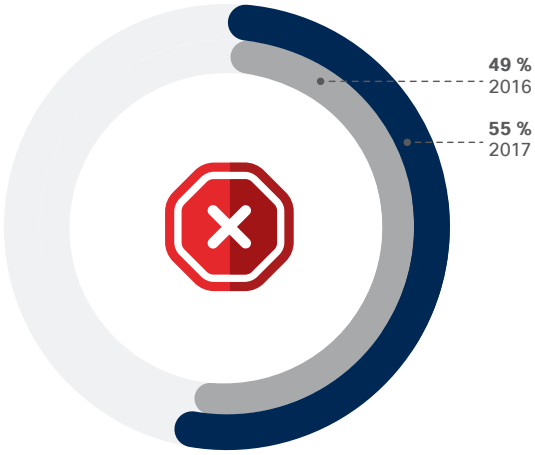


Quelle: Cisco Security Capabilities Benchmark Study 2018

Auswirkungen: Öffentliches Aufsehen bei Sicherheitsverletzungen, höheres Risiko von Verlusten

„Es gibt zwei Arten von Unternehmen: diejenigen, bei denen Sicherheitsverletzungen aufgetreten sind, und solche, die nicht wissen, dass ihre Verteidigungslinien durchbrochen wurden“, erklärt ein Teilnehmer der Benchmark-Studie. (Frei nach dem bekannten Zitat des früheren Cisco CEO John Chambers: „Es gibt zwei Arten von Unternehmen: diejenigen, die gehackt wurden, und solche, die nicht wissen, dass sie gehackt wurden.“) Zwar versuchen die Organisationen, auch auf zukünftige Sicherheitsprobleme vorbereitet zu sein, Schätzungen von Sicherheitsexperten zufolge, werden sie jedoch Opfer einer Sicherheitsverletzung, die die Aufmerksamkeit der Öffentlichkeit erregt. 55 Prozent der Teilnehmer gaben an, dass ihre Organisationen im letzten Jahr in den Fokus der Öffentlichkeit geraten ist (Abbildung 48).

Abbildung 48 55 Prozent der Organisationen waren in den Fokus der Öffentlichkeit geraten



2016 (n=2824), 2017 (n=3548)

Quelle: Cisco Security Capabilities Benchmark Study 2018

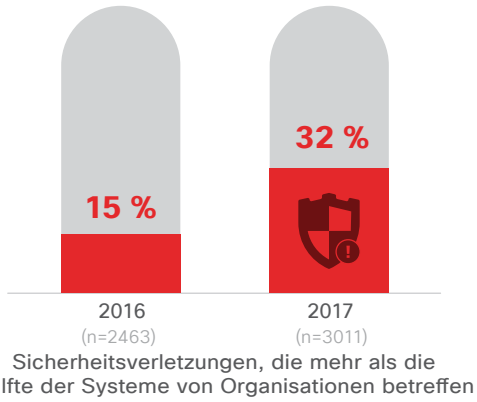
Grafiken für 2018 hier herunterladen: cisco.com/go/acr2018graphics

> *„Es ist davon auszugehen, dass beinahe jedes Fortune 500-Unternehmen in den vergangenen 24 Monaten von Sicherheitsverletzungen betroffen war. Darauf müssen Sie, und insbesondere Ihre Marketing- und PR-Abteilung, vorbereitet sein.“*
>
> *– Teilnehmer an der Benchmark-Studie*

Organisationen meldeten deutlich mehr Sicherheitsverletzungen, die 50 Prozent der Systeme betrafen, (Abbildung 49), als die befragten Organisationen im vergangenen Jahr. Im Jahr 2017 sagten 32 Prozent der Sicherheitsexperten, dass die Sicherheitsverletzungen mehr als die Hälfte ihrer Systeme betrafen; im Jahr 2016 waren es 15 Prozent. Am häufigsten betroffen von Sicherheitsverletzungen sind die Bereiche Betrieb, Finanzen, geistiges Eigentum und Markenreputation (Abbildung 50).

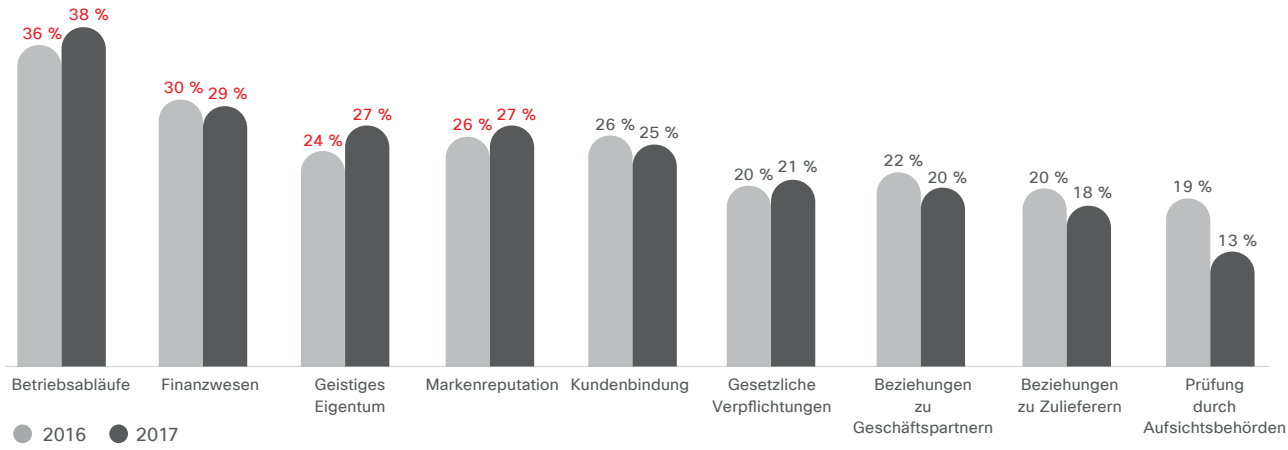
In komplexen Sicherheitsumgebungen ist die Wahrscheinlichkeit höher, dass Sicherheitsverletzungen auftreten. Von den Organisationen, die Produkte von 1 bis 5 Herstellern nutzen, gaben 28 Prozent an, dass sie nach einer Sicherheitsverletzung dem Fokus der Öffentlichkeit ausgesetzt waren; diese Zahl stieg bei Organisationen mit Produkten von über 50 Herstellern auf 80 Prozent (Abbildung 51). Dies könnte womöglich an den besseren Einblicken in die Bedrohungen liegen, die einige Produkte gewähren.

Abbildung 49 Deutlicher Anstieg der Sicherheitsverletzungen, die mehr als 50 Prozent der Systeme betreffen



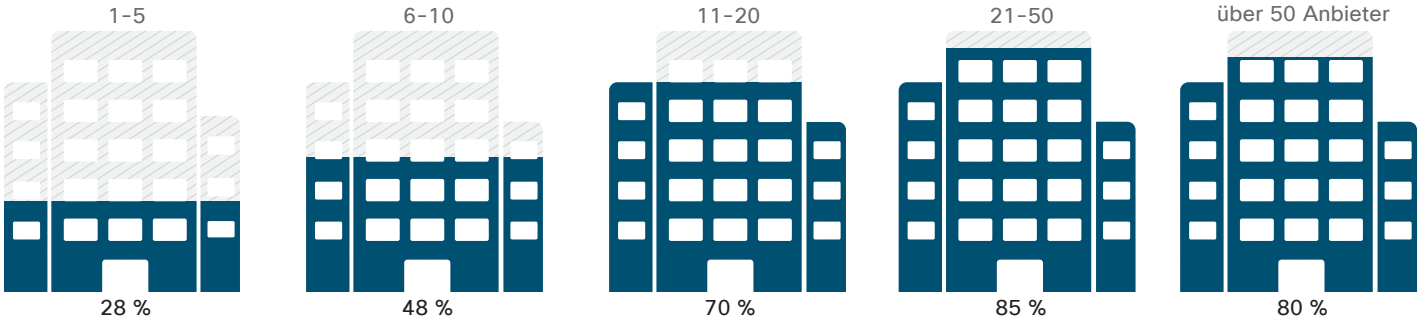
Quelle: Cisco Security Capabilities Benchmark Study 2018

Abbildung 50 Betrieb und Finanzabteilung am wahrscheinlichsten von Sicherheitsverletzungen betroffen



Quelle: Cisco Security Capabilities Benchmark Study 2018

Abbildung 51 80 Prozent der Organisationen, die Produkte von mehr als 50 Herstellern verwenden, waren in den Fokus der Öffentlichkeit geraten



Quelle: Cisco Security Capabilities Benchmark Study 2018

Grafiken für 2018 hier herunterladen: cisco.com/go/acr2018graphics

Der Nutzen eines integrierten Frameworks

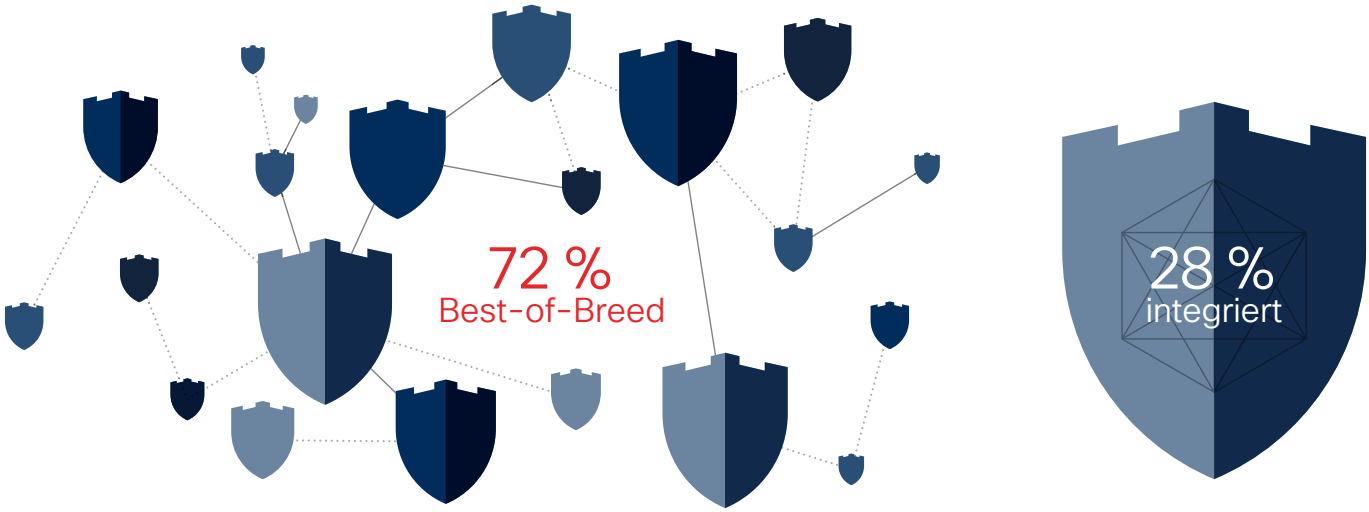
Warum sollte man eine Vielzahl an Produkten von zahlreichen Herstellern nutzen, wenn die daraus resultierende Umgebung schwer zu verwalten ist? Ein Hauptgrund dafür ist der Best-of-Breed-Ansatz, bei dem Sicherheitsteams die für jede Sicherheitsanforderung am besten geeignete Lösung auswählen. Laut Benchmark-Studie sind Sicherheitsexperten, die diesem Ansatz folgen, auch davon überzeugt, dass er kosteneffizienter ist.

Beim Vergleich von Best-of-Breed- mit integrierten Lösungen sagten 72 Prozent der Sicherheitsexperten, dass sie punktuelle Best-of-Breed-Lösungen kaufen, um bestimmte Anforderungen zu erfüllen. Ihnen gegenüber stehen 28 Prozent, die Produkte kaufen, welche als integrierte Lösung zusammenarbeiten sollen (siehe Abbildung 52). Von den Organisationen mit Best-of-Breed-Ansatz führen 57 Prozent die Kosteneffizienz an, während 39 Prozent meinen, dass der Best-of-Breed-Ansatz sich einfacher implementieren lässt.

Interessanterweise bringen Organisationen, die einen integrierten Sicherheitsansatz verfolgen, ähnliche Argumente für ihre Wahl vor. 56 Prozent sagen, dass ein integrierter Ansatz kosteneffizienter ist. 47 Prozent geben an, dass er einfacher zu implementieren ist.

Eine einfache Implementierung wird zunehmend als Argument für die Verwendung eines integrierten Architekturansatzes angeführt: 2016 erklärten nur 33 Prozent der Organisationen, dass eine einfache Implementierung der Grund für den integrierten Ansatz war; 2017 waren es 47 Prozent. Lösungen von einem einzelnen Anbieter mögen zwar nicht für alle Organisationen praktikabel sein, aber wer verschiedene Sicherheitslösungen kauft, sollte sicherstellen, dass diese auch zusammenarbeiten, um Risiken zu reduzieren und die Effektivität zu steigern.

Abbildung 52 72 Prozent kaufen Best-of-Breed-Lösungen, weil sie spezifische Anforderungen erfüllen



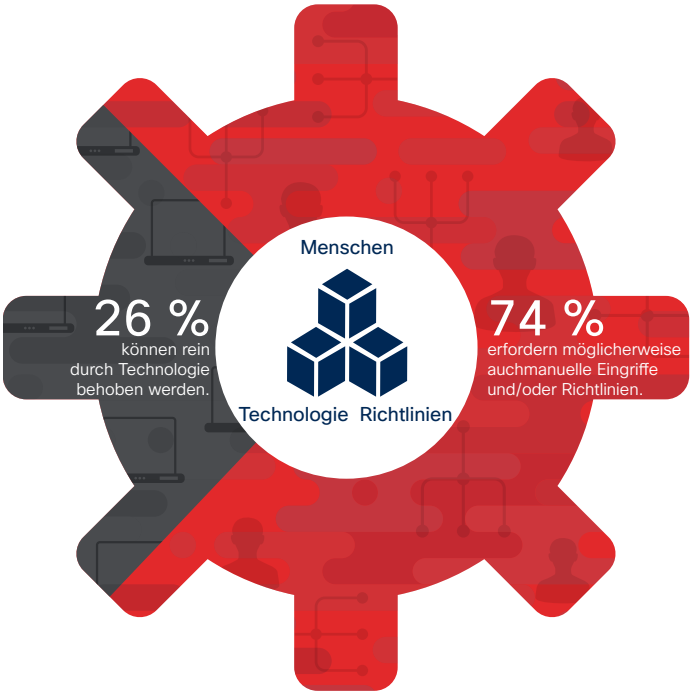
Quelle: Cisco Security Capabilities Benchmark Study 2018

Services: Ausgerichtet auf Menschen, Richtlinien und Technologien

Angesichts der potenziellen Verluste und der Beeinträchtigung von Systemen dürfen sich Organisationen nicht ausschließlich auf Technologien als Verteidigungsmaßnahme verlassen. Das bedeutet, dass andere Möglichkeiten zur Verbesserung der Sicherheit untersucht werden müssen, etwa die Anwendung von Richtlinien oder Benutzerschulungen. Diesen ganzheitlichen Sicherheitsansatz erkennen wir bei den Problemen, die im Rahmen einer Intelligence Lead Security Assurance (bekannt als „Red Team"-Bewertung) ermittelt wurden. Diese wurde vom Cisco Advanced Services Security Advisory-Team zur Verfügung gestellt.

Bei der Untersuchung von Daten aus verschiedenen Red Team-Bewertungen, die 2017 durchgeführt wurden, identifizierten Serviceteammitglieder drei wichtige Verteidigungsfaktoren: Menschen, Richtlinien und Technologien. Sollte sich eine Organisation für die Behebung von Sicherheitslücken ausschließlich auf Technologien stützen, würde sie nur 26 Prozent der Probleme lösen, die in Angriffsimulationen des Red Team ermittelt wurden. Damit würden 74 Prozent der Probleme ungelöst bleiben (siehe Abbildung 53). Organisationen, die nur Richtlinien zur Lösung von Sicherheitsproblemen verwenden, könnten nur 10 Prozent der Probleme lösen; und mit Benutzerschulungen für Mitarbeiter wären es lediglich 4 Prozent. Es müssen also alle drei Bereiche gemeinsam angegangen werden.

Abbildung 53 Nur 26 Prozent der Sicherheitsprobleme können allein mit Produkten behoben werden



Quelle: Cisco Security Research

Abbildung 54 zeigt Beispiele für Probleme, die während der Simulationen ermittelt wurden (nach Kategorie unterteilt). Einige Probleme, wie schwache Kennwörter, finden sich in allen drei Kategorien. Die Erstellung stärkerer Kennwörter kann Verbesserungen im Personalverhalten (Benutzerschulungen), bei Produkten (Konfiguration von Servern für die Erstellung komplexerer Kennwörter) und bei Richtlinien (Vorgaben für die Erstellung starker Kennwörter) erfordern.

Abbildung 54 Arten von Problemen, die während Angriffssimulationen erkannt werden, kategorisiert nach Behebungsanforderungen

Quelle: Cisco Security Research

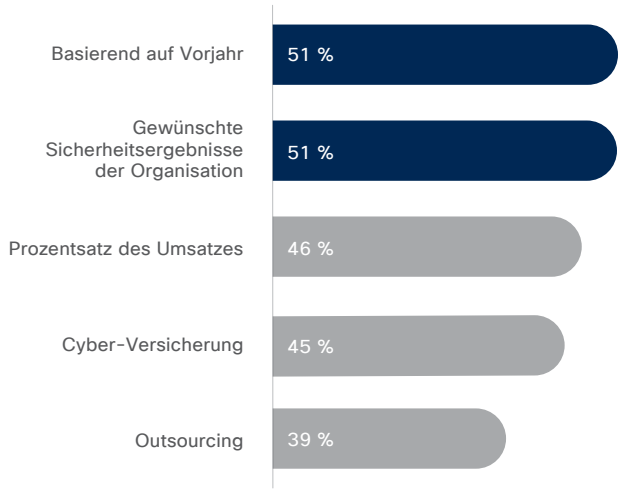
Organisationen können ihre Chancen auf eine erfolgreiche Verwaltung aller drei Faktoren verbessern, wenn sie sicherstellen, dass auf jeder Organisationsebene – nicht nur hier und da – Sicherheitsmaßnahmen integriert werden. Sie sollten auch vermeiden, sich ausschließlich auf Produkte oder technische Verbesserungen zu verlassen, um Sicherheitsprobleme zu beheben. Damit Produkte erfolgreich eingesetzt werden können, müssen Unternehmen sinnvolle Richtlinien und Prozesse für diese Technologie verstehen und umsetzen können.

Erwartungen: Investition in Technologie und Schulungen

Sicherheitsexperten rechnen damit, dass Bedrohungen gegen ihre Organisation komplex und anspruchsvoll bleiben. Sie erwarten, dass Gegner anspruchsvollere und schädlichere Methoden entwickeln, um in Netzwerke einzudringen. Sie wissen außerdem, dass der moderne Arbeitsplatz günstige Bedingungen für Angreifer schafft: Die Mobilität der Mitarbeiter und die wachsende Anzahl von IoT-Geräten bieten Angreifern neue Ansatzpunkte für Kampagnen. Neben zunehmenden Bedrohungen rechnen Sicherheitsexperten damit, dass sie stärker beobachtet werden: von Regulierungsbehörden, Führungskräften, Stakeholdern, Partnern und Kunden.

Um die Wahrscheinlichkeit von Risiken und Verlusten zu mindern, müssen Verteidiger festlegen, wie und wo begrenzte Ressourcen eingesetzt werden. Sicherheitsexperten geben größtenteils an, dass die Sicherheitsbudgets relativ stabil bleiben. Nur große öffentliche Sicherheitsverletzungen können zu einem Umdenken führen und neue Ausgaben für Technologien und Verfahren nach sich ziehen. 51 Prozent gaben an, dass Sicherheitsausgaben auf den Budgets der Vorjahre basieren, während ein ähnlicher Prozentsatz erklärte, dass gewünschte Ergebnisse das Budget beeinflussen würden (Abbildung 55). Die meisten Sicherheitsverantwortlichen glauben, dass ihr Unternehmen angemessen in Sicherheitslösungen investiert.

Abbildung 55 51 Prozent gaben an, dass Sicherheitsausgaben auf den Budgets der Vorjahre basieren

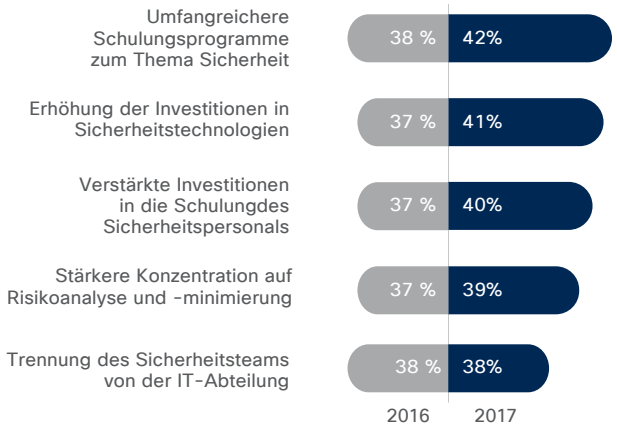


Quelle: Cisco Security Capabilities Benchmark Study 2018

Bei der Planung von Budgets arbeiten viele Unternehmen systematisch Wunschlisten durch, die als Teil umfassender Sicherheitspläne erstellt wurden und Investitionen priorisieren, sobald Ressourcen verfügbar werden. Investitionen können zurückgestellt werden, wenn neue Schwachstellen entweder durch einen internen Vorfall, eine weithin publik gemachte Sicherheitsverletzung oder bei einer routinemäßigen Risikobewertung durch eine dritte Partei aufgedeckt werden.

Die wichtigsten treibenden Faktoren für zukünftige Investitionen und damit verbundene Technologie- und Prozessverbesserungen scheinen Sicherheitsverletzungen zu sein. Im Jahr 2017 gaben 41 Prozent der befragten Sicherheitsexperten an, dass Sicherheitsverletzungen die Ursache für höhere Investitionen in Sicherheitstechnologien und -lösungen sind; 2016 waren es noch 37 Prozent (Abbildung 56). Vierzig Prozent sagten, dass Sicherheitsverletzungen zu höheren Investitionen in Schulungen für Sicherheitspersonal führten; im Jahr 2016 waren 37 Prozent dieser Ansicht.

Abbildung 56 Sicherheitsverletzungen fördern Investitionen in Technologien und Schulungen



2016 (n=1375), 2017 (n=1933)

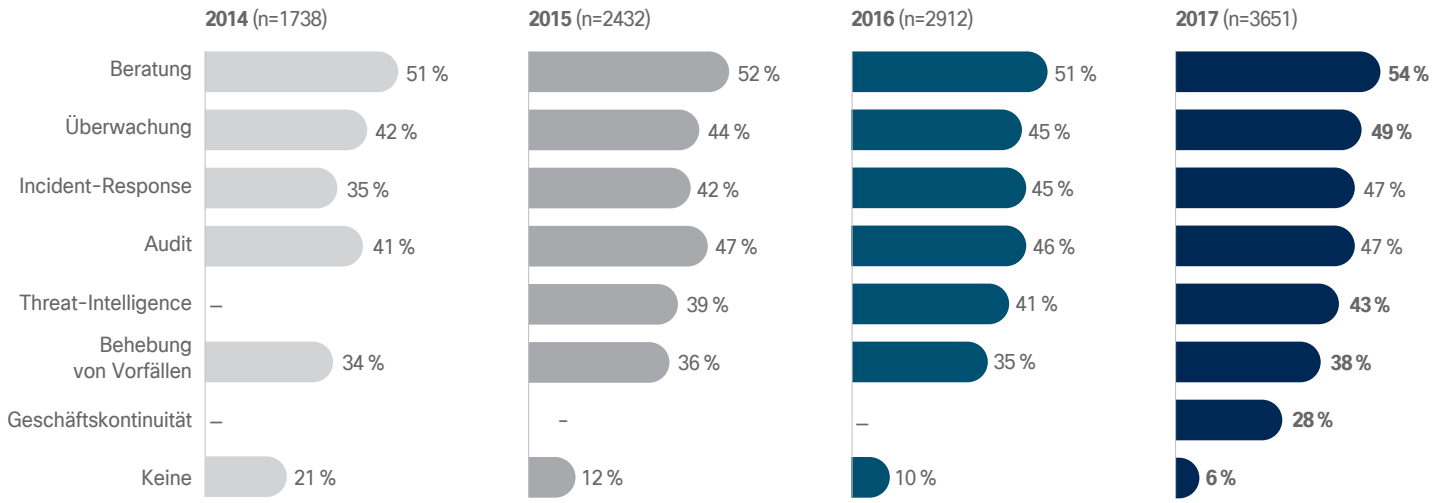
Quelle: Cisco Security Capabilities Benchmark Study 2018

Grafiken für 2018 hier herunterladen: cisco.com/go/acr2018graphics

Sicherheitsexperten rechnen mit mehr Ausgaben für Tools, die künstliche Intelligenz und maschinelles Lernen nutzen, um die Verteidigungsmaßnahmen zu verbessern und das Arbeitsaufkommen besser managen zu können. Darüber hinaus planen sie in Tools zu investieren, die Schutz für kritische Systeme bieten, wie kritische Infrastrukturservices.

Um vorhandene Ressourcen besser nutzen und Verteidigungsmaßnahmen optimieren zu können, verlassen sich Organisationen zunehmend auf Hilfe von außerhalb. Von den befragten Sicherheitsexperten sagten 49 Prozent, dass sie 2017 Monitoring-Services ausgelagert haben; 2015 waren es 44 Prozent. Im Jahr 2017 lagerten 47 Prozent die Incident Response aus; im Jahr 2015 waren es 42 Prozent (Abbildung 57).

Abbildung 57 Auslagerung von Monitoring und Incident Response nimmt Jahr für Jahr zu



Quelle: Cisco Security Capabilities Benchmark Study 2018

Grafiken für 2018 hier herunterladen: cisco.com/go/acr2018graphics

Weitere Ergebnisse der Cisco Security Capabilities Benchmark Study 2018 finden Sie im Anhang auf **Seite 64**.

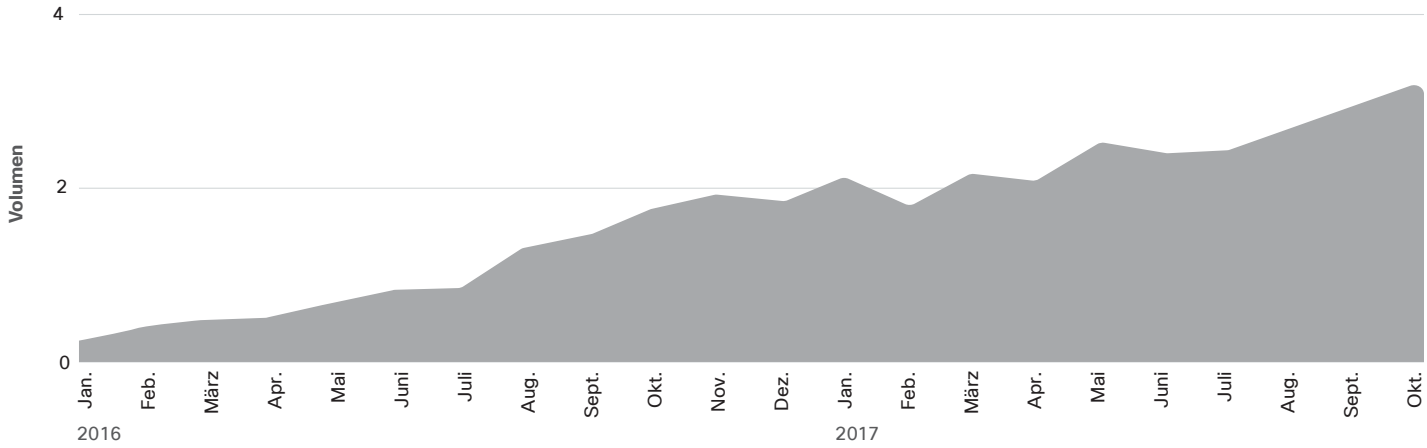
Fazit

Fazit

In der modernen Bedrohungslandschaft gibt es Gegner, die einer Erkennung geschickt entgehen können. Sie verfügen über effektivere Tools, wie Verschlüsselung und raffinierte Taktiken, wie den Missbrauch legitimer Internet-Services, um ihre Aktivitäten zu verschleiern und herkömmliche Sicherheitstechnologien zu unterwandern. Außerdem entwickeln sie ihre Taktiken laufend weiter, damit ihre Malware auf dem neuesten Stand und effektiv bleibt. Es kann lange dauern, bis selbst bekannte Bedrohungen identifiziert werden.

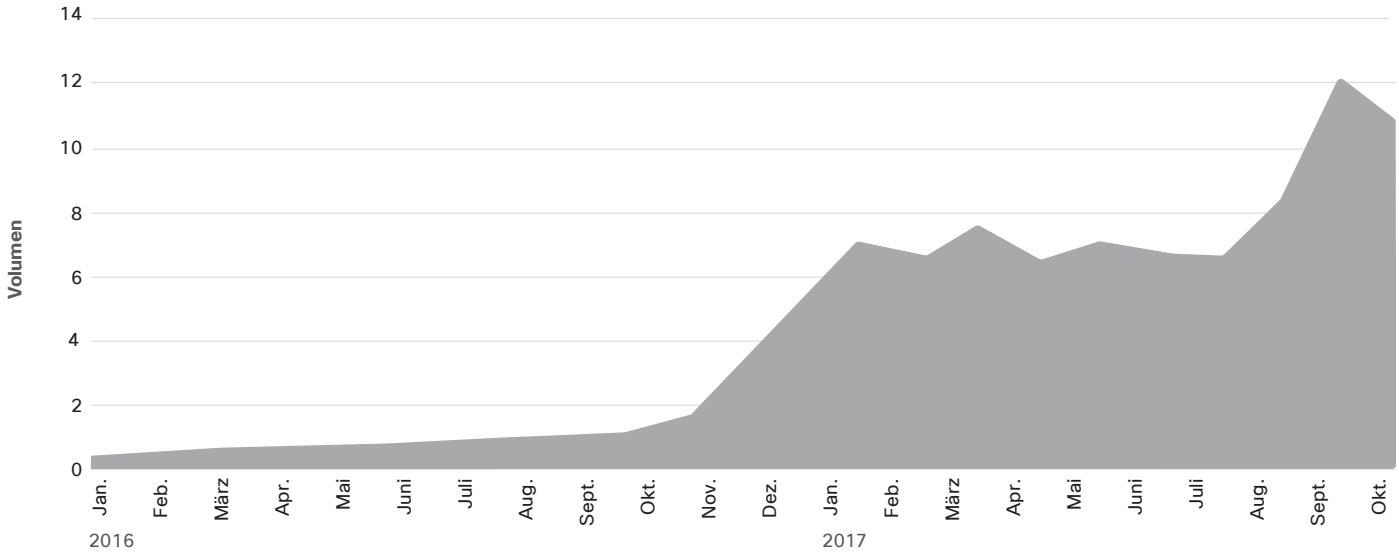
Ein Grund dafür, dass sich Verteidiger laufend Gefechte mit Angreifern liefern müssen und nicht das große Ganze der Bedrohungslandschaft überblicken können, ist die reine Menge des potenziell schädlichen Datenverkehrs. Unsere Untersuchung zeigt, dass sich die Gesamtzahl der von Cloud-basierten Cisco Sicherheitsprodukten beobachteten Vorfälle zwischen Januar 2016 und Oktober 2017 vervierfacht hat (siehe Abbildung 58). Die Gesamtzahl entspricht der Anzahl aller Ereignisse, gutartige oder schädliche, die von unseren Cloud-basierten Sicherheitsprodukten in diesem Zeitraum beobachtet wurden.

Abbildung 58 Gesamtzahl der Ereignisse



Quelle: Cisco Security Research

Abbildung 59 Gesamtvolumen an Malware



Quelle: Cisco Security Research

Unsere Sicherheitsprodukte verzeichneten zudem einen Anstieg des Malware-Aufkommens um das Elffache im selben Zeitraum, wie in Abbildung 59 zu sehen.

Entwicklungen beim Malware-Volumen wirken sich auf die TTD (Time to detection; Bedrohungserkennungszeit) der Verteidiger aus. Sie ist eine wichtige Kennzahl für Organisationen, mit der nachvollzogen werden kann, wie gut die Sicherheitsmaßnahmen bei der von den Gegnern losgetretenen Malware-Flut wirken.

Der TTD-Mittelwert von Cisco beträgt im Zeitraum von November 2016 bis Oktober 2017 etwa 4,6 Stunden und hilft zu veranschaulichen, wie schwierig die Identifizierung von Bedrohungen in dieser chaotischen Bedrohungslandschaft ist. Immerhin liegt die Zahl deutlich unter der durchschnittlichen TTD von 39 Stunden, die wir im November 2015 nach Aufzeichnung der ersten TTD gemeldet hatten, sowie unter dem 14-Stunden-Durchschnitt, der im *Cisco Annual Cybersecurity Report 2017* für den Zeitraum von November 2015 bis Oktober 2016 angeführt ist.[20]

Für Cisco war die Verwendung von Cloud-basierter Sicherheitstechnologie ein entscheidendes Mittel, um die durchschnittliche TTD niedrig zu halten. Da die Anzahl der Gesamtereignisse sowie die Anzahl der von Malware attackierten Endpunkte weiterhin steigt, kann die Cloud hinsichtlich Skalierung und Aufrechterhaltung der Performance helfen. Diese Flexibilität ist von On-premise-Sicherheitslösungen einfach nicht zu erwarten. Eine maßgerechte Lösung zu erstellen, die über einen Zeitraum von zwei Jahren mehr als das 10-fache Volumen an Malware-Ereignissen bewältigen und gleichzeitig Reaktionszeiten aufrechterhalten oder steigern kann, ist für jede Organisation ein schwieriges und kostspieliges Unterfangen.

Cisco definiert die Bedrohungs-Erkennungszeit (auch „Time-to-Detection", TTD) als die Zeitspanne vom Auftreten einer Kompromittierung bis zu deren Erkennung als Bedrohung. Für die Ermittlung der TTD ziehen wir Sicherheitstelemetrie heran, die von Cisco Security-Produkten weltweit erfasst wird. Durch kontinuierliche Analysen dieser Daten können wir dann feststellen, zu welchem Zeitpunkt ein bislang unbekannter Schadcode auf ein Endgerät heruntergeladen wurde, und zu welchem Zeitpunkt dieser Code als Bedrohung klassifiziert wurde.

Der TTD-Mittelwert entspricht dem Durchschnitt der pro Zeitraum beobachteten monatlichen Mittelwerte.

20 *Cisco Annual Cybersecurity Report 2017:* cisco.com/c/m/en_au/products/security/offers/annual-cybersecurity-report-2017.html.

Über Cisco

Informationen zu Cisco

Cisco bietet intelligente Lösungen für die IT-Sicherheit und verfügt über das branchenweit umfangreichste Portfolio an Systemen für eine fortschrittliche Bedrohungsabwehr, die unterschiedlichste Angriffsvektoren abdecken. Unser bedrohungsorientierter und operationalisierter Sicherheitsansatz verringert die Komplexität und Fragmentierung von Sicherheitslösungen und stellt gleichzeitig ein hohes Maß an Transparenz, konsistente Kontrollen und intelligenten Schutz vor Bedrohungen vor, während und nach einem Angriff bereit.

Die Forschungsgruppe des Collective Security Intelligence (CSI) Ecosystem ermittelt Entwicklungen in der Bedrohungslandschaft anhand von Telemetriedaten aus zahllosen Geräten und Sensoren, öffentlichen Feeds sowie der Open-Source-Community. Dazu werden jeden Tag mehrere Milliarden Internetanfragen sowie Millionen von E-Mails, Malware-Stichproben und Netzwerk-Zugriffsversuche analysiert.

Eine hochmoderne Infrastruktur, unterstützt durch branchenführende Systeme, wertet die Telemetriedaten aus. Dies ermöglicht maschinelles Lernen, es können Bedrohungen für Netzwerke, Rechenzentren, Endpunkte, Mobilgeräte, virtuelle Systeme, das Internet, den E-Mail-Verkehr und die Cloud nachverfolgt sowie Ursachen ermittelt und Outbreaks analysiert werden. Die so gewonnenen Informationen fließen direkt in den Echtzeitschutz der Produkte und Services ein, die bei Cisco Kunden weltweit im Einsatz sind.

Weitere Informationen zu unserem bedrohungsorientierten Sicherheitsansatz finden Sie unter: cisco.com/go/security.

CISCO ANNUAL CYBERSECURITY REPORT 2018 – MITWIRKENDE

Wir möchten unseren Bedrohungsforschern und anderen Fachexperten bei Cisco sowie unseren Technologiepartnern danken, die zum **Cisco Annual Cybersecurity Report 2018** *beigetragen haben. Ihre Forschung und Erkenntnisse sind für Cisco extrem wichtig, denn so können wir die Security-Community, andere Unternehmen und Benutzer dabei unterstützen, einen genauen Einblick in die Komplexität und das Ausmaß moderner, globaler Cyberbedrohungen zu erhalten und ihnen Best-Practices und weitere Tipps zur Verbesserung der Bedrohungsabwehr mitzuteilen.*

Unsere Technologiepartner spielen ebenfalls eine entscheidende Rolle. Sie unterstützen unser Unternehmen bei der Entwicklung einer unkomplizierten, offenen und automatisierten Sicherheitsstrategie, die den Organisationen die Integration der Lösungen ermöglicht, die für den Schutz ihrer Umgebungen unerlässlich sind.

Cisco Advanced Malware Protection (AMP) für Endpunkte

Cisco AMP für Endpunkte bietet automatisierte Präventions-, Erkennungs- und Reaktionsfunktionen in einer einzigen Lösung. Die Lösung überwacht und analysiert Anzeichen für schädliche Aktivitäten, um Bedrohungen zu identifizieren, welche die erste Verteidigungslinie umgehen und für Organisationen das größte Risiko darstellen. Dabei kommen diverse Erkennungsmethoden zum Einsatz, wie z. B. erweitertes Sandboxing, Exploit-Prävention und maschinelles Lernen, um Bedrohungen schnell zu erkennen und zu beheben. Cisco AMP für Endgeräte ist die einzige Lösung, die Retrospective Security bietet. Damit kann schnell auf Bedrohungen reagiert und Ausmaß, Ursprung und Quarantänemöglichkeiten für Bedrohungen identifiziert werden.

Cisco CloudLock

Cisco CloudLock bietet Cloud Access Security Broker (CASB)-Lösungen, die Unternehmen bei der sicheren Nutzung der Cloud unterstützen. CloudLock bietet Transparenz und Kontrolle für alle Benutzer, Daten und Anwendungen in Software-as-a-Service (SaaS)-, Platform-as-a-Service (PaaS)- und Infrastructure-as-a-Service (IaaS)-Umgebungen mithilfe von aussagekräftigen Daten zur Cybersicherheit, die von Datenanalysten seines CyberLabs erfasst und durch Sicherheitsanalytik von Crowdsourcing-Quellen ergänzt werden.

Cisco Cognitive Threat Analytics

Cisco Cognitive Threat Analytics ist ein Cloud-basierter Dienst, der Sicherheitsverletzungen, Aktivitäten von Malware in geschützten Netzwerken und andere Sicherheitsbedrohungen mittels statistischer Analysen des Netzwerkverkehrs erkennt. Der Dienst identifiziert die Symptome von Malware-Infektionen oder Datenschutzverletzungen anhand von Verhaltensanalysen und Anomalie-Erkennung und schließt so die Lücken von Abwehrsystemen am Perimeter. Neben fortschrittlichen statistischen Modellen bringt Cognitive Threat Analytics maschinelles Lernen zum Einsatz. So können neue Bedrohungen selbständig erkannt und der Schutz laufend optimiert werden.

Cisco Product Security Incident Response Team (PSIRT)

Das Cisco PSIRT ist ein dediziertes globales Team, das den Eingang, die Untersuchung und die Veröffentlichung von Informationen zu Sicherheitslücken bei Cisco Produkten und Netzwerken verwaltet. Das PSIRT erhält Berichte von unabhängigen Forschern, Branchenunternehmen, Herstellern, Kunden und anderen Quellen, die sich mit der Produkt- oder Netzwerksicherheit beschäftigen.

Cisco Security Incident Response Services (CSIRS)

Das Cisco CSIRS-Team setzt sich aus geschulten Incident-Responders zusammen, die Cisco Kunden vor, während und nach einem Sicherheitsvorfall unterstützen. CSIRS setzt hoch qualifizierte Mitarbeiter, Security-Lösungen der Enterprise-Klasse, hochmoderne Response-Techniken und seit langem bewährte Best-Practices zur Abwehr von Angreifern ein, um sicherzustellen, dass Kunden proaktiv gegen Angriffe vorgehen, im Ernstfall schnell reagieren und den Geschäftsbetrieb nach einem Angriff rasch wieder aufnehmen können.

Cisco Talos Intelligence Group

Die Cisco Talos Intelligence Group gehört zu den größten kommerziellen Threat-Intelligence-Teams weltweit und setzt sich aus renommierten Forschern, Analysten und Technikern zusammen. Unterstützt werden diese Teams durch beispiellose Telemetriedaten und ausgeklügelte Systeme, mit denen eine genaue, schnelle und aussagekräftige Threat-Intelligence für Cisco Kunden, Produkte und Dienstleistungen erstellt werden kann. Die Talos Group schützt Cisco Kunden vor bekannten und neuen Bedrohungen, deckt gängige Software-Schwachstellen auf und fängt Bedrohungen ab, bevor sie sich ausbreiten und größeren Schaden anrichten können. Die durch Talos gesammelt Threat-Intelligence ist in die Cisco Produkte integriert, wodurch bekannte und neue Bedrohungen erkannt, analysiert und bekämpft werden können. Talos befolgt die offiziellen Regelsätze von Snort.org, ClamAV und SpamCop und veröffentlicht viele Open-Source-Tools zur Untersuchung und Analyse.

Cisco Threat Grid

Cisco Threat Grid ist eine Plattform für Malware-Analysen und Threat-Intelligence. Threat Grid führt statische und dynamische Analysen von verdächtigen Malware-Stichproben durch, die von Kunden und Produktintegrationen auf der ganzen Welt eingeholt werden. Hunderttausende dieser Stichproben, darunter verschiedenste Dateitypen, werden täglich über die Benutzeroberfläche des Threat Grid Cloud-Portals (oder über die Threat Grid-API) an die Threat Grid-Cloud gesendet. Threat Grid lässt sich zudem als Vor-Ort-Appliance bereitstellen.

Cisco Umbrella

Cisco Umbrella ist ein sicheres Internet-Gateway, das die erste Verteidigungslinie gegen Bedrohungen im Internet bildet, egal welche Seiten Benutzer aufrufen. Da Umbrella in das Fundament des Internets integriert ist, bietet es umfassende und transparente Einblicke in Aktivitäten an allen Standorten, auf allen Geräten und von allen Benutzern. Umbrella analysiert und lernt aus diesen Aktivitäten und deckt automatisch Infrastrukturen von Angreifern auf, die für aktuelle und neue Bedrohungen vorbereitet wurden. Die Lösung blockiert Abfragen proaktiv, bevor eine Verbindung hergestellt wird.

Security Research and Operations (SR&O)

SR&O ist zuständig für das Bedrohungs- und Schwachstellenmanagement aller Produkte und Services von Cisco, wie das branchenführende Cisco PSIRT. Auf Veranstaltungen wie der Cisco Live und Black Hat bieten die SR&O in Zusammenarbeit mit Cisco Partnern und anderen Branchenvertretern eine Anlaufstelle bei Fragen bezüglich aktueller Entwicklungen in der Bedrohungslandschaft. Daneben ist SR&O an der Bereitstellung von neuen Services wie Cisco Custom Threat Intelligence (CTI) beteiligt, mit dem Anzeichen für Kompromittierungen identifiziert werden können, die vorhandene Sicherheitsinfrastrukturen nicht erkennen oder beheben konnten.

Security and Trust Organization

Die Security and Trust Organization ist für den Schutz der Kunden von Cisco aus dem öffentlichen und privaten Sektor verantwortlich. Der Fokus liegt dabei nicht nur auf der konsistenten Anwendung der Grundsätze der Cisco Secure Development Lifecycle and Trustworthy Systems über das gesamte Produkt- und Serviceportfolio von Cisco hinweg, sondern auch auf dem Schutz von Cisco vor den komplexen Bedrohungen von heute. Sicherheit und Vertrauen schließen bei Cisco Menschen und Richtlinien ebenso wie Prozesse und Technologien ein. Denn erst auf dieser Basis können Informationssicherheit, vertrauenswürdige Technik, Datenschutz und Privatsphäre, Cloud-Sicherheit, Transparenz und Nachvollziehbarkeit sowie Zuverlässigkeit gegenüber Kunden umfassend sichergestellt werden. Weitere Informationen finden Sie unter trust.cisco.com.

Cisco Annual Cybersecurity Report 2018 – mitwirkende Technologiepartner

ANOMALI®

Die Threat-Intelligence-Lösungen der Anomali-Suite unterstützen Organisationen bei der aktiven Erkennung und Untersuchung von sowie der Reaktion auf Cyberbedrohungen. Die preisgekrönte Threat Intelligence-Plattform ThreatStream bündelt und optimiert Millionen von Bedrohungsindikatoren. So hat sich mittlerweile eine „Cyber-No-Fly-Liste“ gebildet. „Anomali“ wird in die interne Infrastruktur integriert, um neue Angriffe zu identifizieren. Die Lösung führt seit Jahren forensische Analysen bestehender Sicherheitslücken durch und ermöglicht Sicherheitsteams, Bedrohungen schnell zu verstehen und einzudämmen. „Anomali“ bietet zudem STAXX an, ein kostenloses Tool, mit dem Threat-Intelligence gesammelt und geteilt wird, sowie Anomali Limo, ein kostenloser, sofort einsetzbarer Intelligence-Feed. Um mehr zu erfahren, besuchen Sie anomali.com und folgen Sie uns auf Twitter: @anomali.

LUMETA
DETECT WITH A HIGHER SENSE

Lumeta unterstützt Sicherheits- und Netzwerkteams bei der Verhinderung von Sicherheitsverletzungen, indem es wertvolle Einblicke in die Cyberwelt bietet. Lumeta bietet im Vergleich zu anderen Lösungen auf dem Markt eine unübertroffene Erkennung von bekannten, unbekannten, Schatten- und nicht genehmigten Netzwerkinfrastrukturen. Seine Produkte ermöglichen außerdem die Überwachung von Netzwerken und Endgeräten in Echtzeit, um nicht autorisierte Änderungen zu erkennen, Leak-Pfade zu verhindern, eine ordnungsgemäße Netzwerksegmentierung sicherzustellen und verdächtiges Netzwerkverhalten in dynamischen Netzwerkelementen, Endgeräten, virtuellen Systemen und Cloud-basierten Infrastrukturen zu identifizieren. Weitere Informationen finden Sie unter lumeta.com.

Qualys, Inc. (NASDAQ: QLYS) ist ein Pionier und führender Anbieter von Cloud-basierten Sicherheits- und Compliance-Lösungen mit mehr als 9.300 Kunden in über 100 Ländern, darunter einen Großteil der Forbes Global 100- und Fortune 100-Unternehmen. Die Cloud-Plattform von Qualys und dessen integrierte Lösungs-Suite unterstützen Organisationen bei der Vereinfachung der Sicherheitsprozesse und Senkung der Compliance-Kosten, z. B. durch die Bereitstellung kritischer Security-Intelligence nach Bedarf und die Automatisierung von umfangreichen Audit-, Compliance- und Schutzfunktionen für IT-Systeme und Web-Anwendungen. Qualys wurde 1999 gegründet und hat strategische Partnerschaften mit führenden Anbietern von Managed-Services und Consulting-Services weltweit aufgebaut. Weitere Informationen finden Sie unter qualys.com.

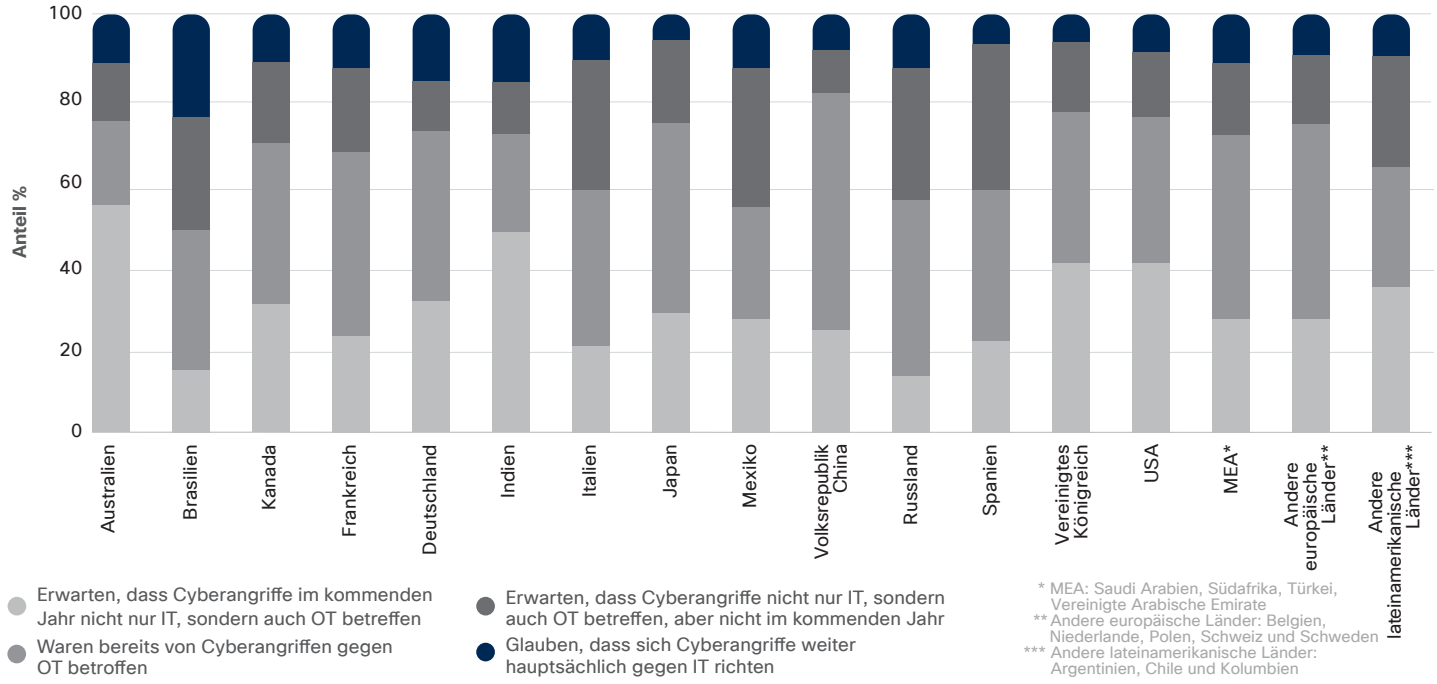
Radware (NASDAQ: RDWR) ist ein weltweit führender Anbieter von Anwendungsbereitstellungs- und Cybersicherheitslösungen für virtuelle, Cloud-basierte und softwaredefinierte Rechenzentren. Das preisgekrönte Portfolio des Unternehmens sorgt für zuverlässige Servicelevel unternehmenskritischer Anwendungen, wovon mehr als 10.000 Enterprise- und Carrier-Kunden weltweit profitieren. Weitere Expertenressourcen und -informationen zum Thema Sicherheit erhalten Sie im Online Security Center von Radware, das eine umfassende Analyse von DDoS-Angriffstools, Trends und Bedrohungen enthält: security.radware.com.

SAINT Corporation, ein führender Anbieter integrierter Schwachstellen-Managementlösungen der nächsten Generation, hilft Unternehmen und Institutionen des öffentlichen Sektors, Risiken auf allen Ebenen der Organisation zu identifizieren. SAINT ermöglicht, dass ein effektiver Zugriff sowie ein hohes Maß an Sicherheit und Datenschutz gewährleistet werden. Der Anbieter stärkt die InfoSec-Abwehr und senkt gleichzeitig die Gesamtbetriebskosten. Weitere Informationen finden Sie unter saintcorporation.com.

TrapX Security bietet ein automatisiertes Sicherheitsnetz, das Echtzeit-Bedrohungen abfängt und gleichzeitig verwertbare Informationen anbietet, um Angreifern abzuwehren. Mit TrapX DeceptionGrid™ können Unternehmen Zero-Day-Malware erkennen, eindämmen und analysieren, die von den weltweit effektivsten APT-Organisationen eingesetzt werden. Ganze Branchen verlassen sich auf TrapX zum Ausbau ihres IT-Ecosystems und der Reduzierung von kostspieligen Kompromittierungen, Sicherheitslücken und Verstößen gegen die Compliance-Anforderungen. Die TrapX-Abwehrfunktionen sind in die Netzwerk- und unternehmenskritische Infrastruktur eingebettet. Es werden keine Agents oder Konfigurationen benötigt. Durch modernste Malware-Erkennung, Threat-Intelligence, forensische Analysen und Funktionen zur Behebung in einer einzigen Plattform werden Komplexität und Kosten reduziert. Weitere Informationen finden Sie unter trapx.com.

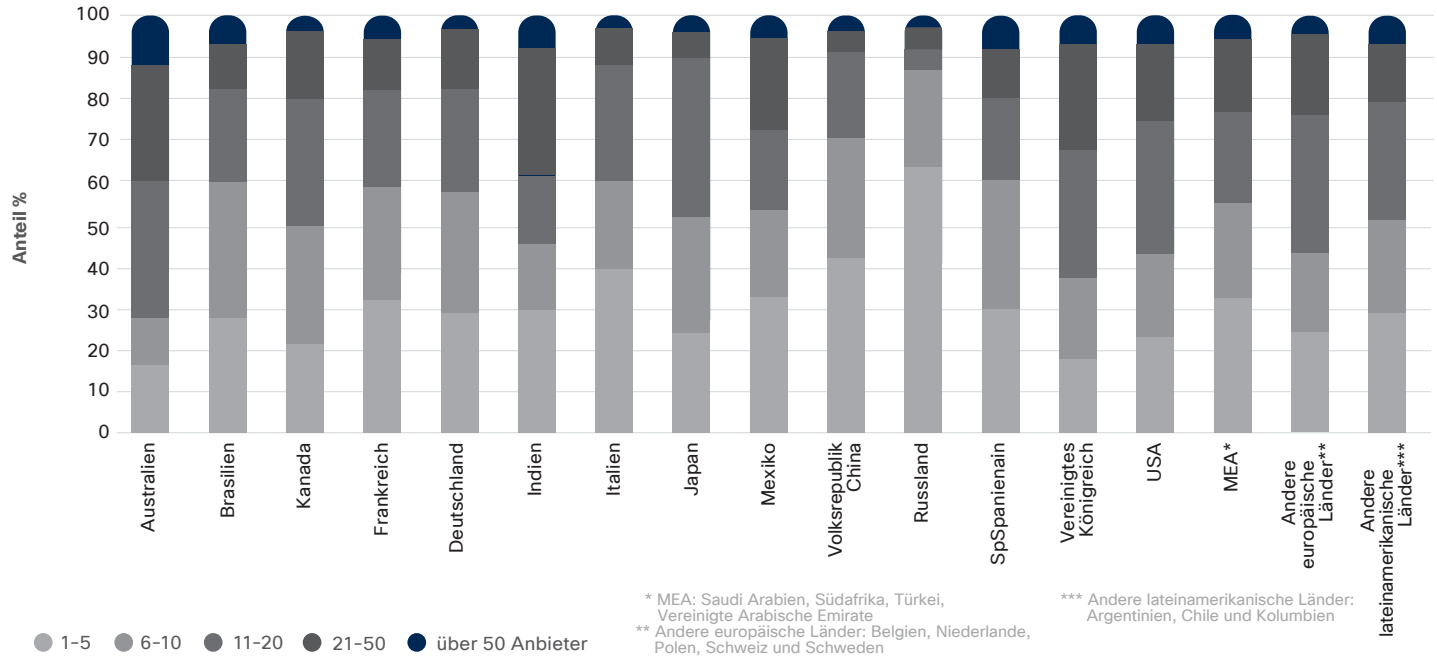
Anhang

Abbildung 60 Erwartungen bezüglich Cyberangriffen auf die OT und IT, nach Land oder Region



Quelle: Cisco Security Capabilities Benchmark Study 2018

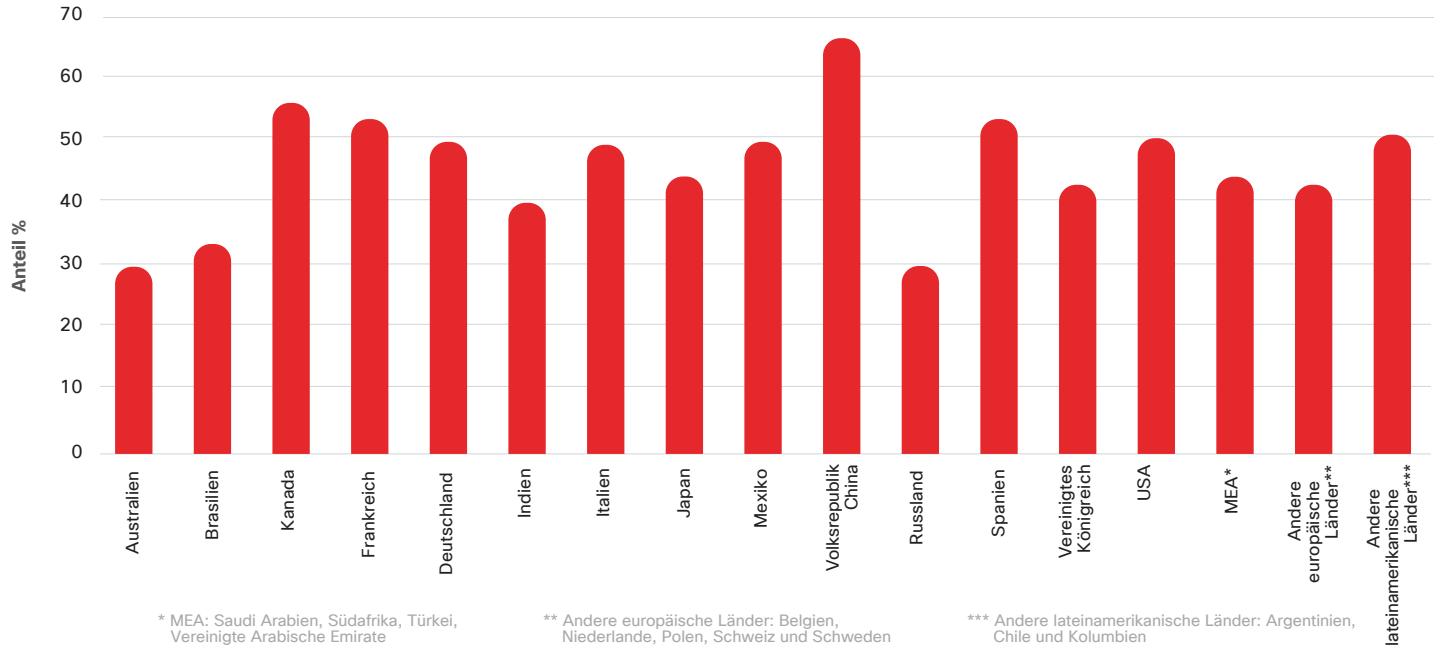
Abbildung 61 Anzahl der Hersteller von Sicherheitslösungen in einer Umgebung, nach Land oder Region



Quelle: Cisco Security Capabilities Benchmark Study 2018

Grafiken für 2018 hier herunterladen: cisco.com/go/acr2018graphics

Abbildung 62 Prozentsatz der nicht untersuchten Warnmeldungen, nach Land oder Region



* MEA: Saudi Arabien, Südafrika, Türkei, Vereinigte Arabische Emirate

** Andere europäische Länder: Belgien, Niederlande, Polen, Schweiz und Schweden

*** Andere lateinamerikanische Länder: Argentinien, Chile und Kolumbien

Quelle: Cisco Security Capabilities Benchmark Study 2018

Abbildung 63 Hindernisse bei der Einführung erweiterter Sicherheitsprozesse und -technologien, nach Land oder Region

Welches sind Ihrer Meinung nach die größten Hindernisse bei der Einführung erweiterter Sicherheitsprozesse und -technologien?

	Australien	Brasilien	Kanada	Frankreich	Deutschland	Indien	Italien	Japan	Mexiko	Volksrepublik China	Russland	Spanien	Vereinigtes Königreich	US	MEA*	Andere europäische Länder**	Andere lateinamerikanische Länder***
Budgetbeschränkungen	23 %	35 %	29 %	33 %	25 %	36 %	38 %	31 %	31 %	38 %	60 %	33 %	27 %	34 %	36 %	37 %	35 %
Konkurrierende Prioritäten	28 %	11 %	29 %	27 %	28 %	26 %	24 %	27 %	16 %	27 %	20 %	18 %	32 %	32 %	25 %	18 %	24 %
Fachkräftemangel	25%	28 %	19 %	22 %	24 %	31 %	24%	28 %	30 %	25 %	35 %	33 %	31 %	26 %	25 %	23 %	26 %
Mangelndes Wissen über erweiterte Sicherheitsprozesse und -technologien	26 %	26 %	24 %	21 %	22 %	24 %	21 %	26 %	23 %	29 %	18 %	21 %	27 %	22 %	22 %	17 %	21 %
Probleme hinsichtlich Kompatibilität mit Rechtssystemen	27 %	19 %	30 %	27 %	30 %	30 %	22 %	23 %	32 %	40 %	25 %	25 %	24 %	28 %	30 %	25 %	28 %
Zertifizierungsanforderungen	33 %	27 %	29 %	29 %	24 %	27 %	27 %	22 %	27 %	23 %	22 %	27 %	27 %	30 %	24 %	33 %	21 %
Unternehmenskultur bezüglich Sicherheit	30 %	23 %	25 %	20 %	16 %	26 %	17 %	21 %	26 %	17 %	19 %	24 %	28 %	25 %	20 %	20 %	27 %
Kaufzurückhaltung wegen fehlender Bewährung am Markt	19 %	20 %	23 %	26 %	25 %	29 %	20 %	28 %	15 %	16 %	17 %	20 %	21 %	22 %	22 %	21 %	25 %
Zu hohe Arbeitsbelastung lässt derzeit keine neuen Aufgaben zu	22 %	16 %	28 %	18 %	28 %	28 %	26 %	27 %	23 %	21 %	15 %	28 %	22 %	22 %	20 %	17 %	19 %
Organisation betrachtet sich nicht als besonders gefährdet	25 %	18 %	21 %	22 %	24 %	17 %	14 %	20 %	12 %	16 %	11 %	13 %	21 %	21 %	21 %	20 %	16 %
Security is not an executive-level priority	22 %	10 %	17 %	17 %	20 %	13 %	13 %	23 %	15 %	18 %	11 %	11 %	19 %	19 %	17 %	19 %	21 %

* MEA: Saudi Arabien, Südafrika, Türkei, Vereinigte Arabische Emirate

** Andere europäische Länder: Belgien, Niederlande, Polen, Schweiz und Schweden

*** Andere lateinamerikanische Länder: Argentinien, Chile und Kolumbien

Quelle: Cisco Security Capabilities Benchmark Study 2018

Grafiken für 2018 hier herunterladen: cisco.com/go/acr2018graphics

Abbildung 64 Kauf von Lösungen zum Schutz vor Sicherheitsbedrohungen, nach Land oder Region

Welches Beispiel beschreibt am besten, wie Ihre Organisation Sicherheitslösungen zur Bedrohungsabwehr kauft?

Land	N=	Kaufen typischerweise punktuelle Best-of-Breed-Lösungen für spezifische Anforderungen	Kaufen typischerweise Lösungen, die mit anderen Produkten zusammenarbeiten
Australien	203	86	14
Brasilien	197	72	28
Kanada	185	67	33
Frankreich	191	59	41
Deutschland	195	69	31
Indien	199	78	22
Italien	201	71	29
Japan	223	72	28
Mexiko	198	77	23
Volksrepublik China	205	63	37
Russland	196	58	42
Spanien	148	70	30
Vereinigtes Königreich	194	76	24
USA	393	81	19
MEA*	249	69	31
Andere europäische Länder**	199	73	27
Andere lateinamerikanische Länder***	196	71	29

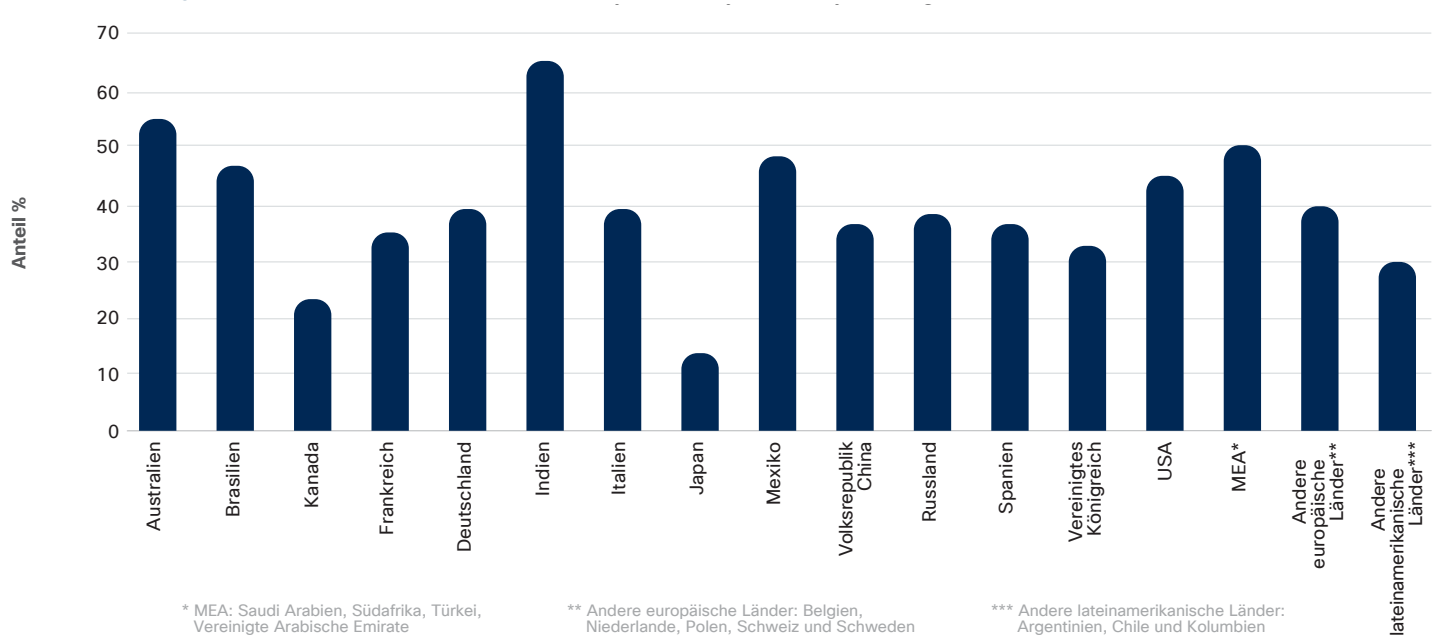
* MEA: Saudi Arabien, Südafrika, Türkei, Vereinigte Arabische Emirate

** Andere europäische Länder: Belgien, Niederlande, Polen, Schweiz und Schweden

*** Andere lateinamerikanische Länder: Argentinien, Chile und Kolumbien

Quelle: Cisco Security Capabilities Benchmark Study 2018

Abbildung 65 Prozentsatz der Unternehmen, die ihrer Meinung nach das standardisierte Infosec-Framework einhalten, nach Land oder Region



* MEA: Saudi Arabien, Südafrika, Türkei, Vereinigte Arabische Emirate

** Andere europäische Länder: Belgien, Niederlande, Polen, Schweiz und Schweden

*** Andere lateinamerikanische Länder: Argentinien, Chile und Kolumbien

Quelle: Cisco Security Capabilities Benchmark Study 2018

Grafiken für 2018 hier herunterladen: cisco.com/go/acr2018graphics

Grafiken zum Download

Alle Grafiken aus diesem Bericht können unter folgender Adresse heruntergeladen werden: cisco.com/go/mcr2018graphics.

Aktualisierungen und Korrekturen

Aktualisierungen und Korrekturen zu diesem Projekt finden Sie hier: cisco.com/go/errata.

Hauptgeschäftsstelle Nord- und Südamerika
Cisco Systems, Inc.
San Jose, CA

Hauptgeschäftsstelle Asien-Pazifik-Raum
Cisco Systems (USA) Pte. Ltd.
Singapur

Hauptgeschäftsstelle Europa
Cisco Systems International BV Amsterdam,
Niederlande

Cisco verfügt über mehr als 200 Niederlassungen weltweit. Die Adressen mit Telefon- und Faxnummern finden Sie auf der Cisco Website unter www.cisco.com/go/offices.

Veröffentlicht im Februar 2018