cisco

Annual Security Report 2015

Zusammenfassung

Die Bedroungslandschaft bleibt auch weiterhin hochdynamisch.

Cyberkriminelle verfeinern laufend ihre Angriffsmethoden und entwickeln immer neue Techniken, um unerkannt in Systeme einzudringen und ihre Aktivitäten zu verschleiern. Sicherheitsteams in Unternehmen müssen daher permanent ihre Maßnahmen anpassen, um Firma und Benutzer vor immer raffinierteren Angriffen zu schützen.

Die Benutzer spielen eine zentrale Rolle. Sie sind nicht nur die Ziele der Angreifer, sonder spielen ihnen häufig auch unbewusst in die Hände.

Die Cisco Sicherheitsexperten analysieren im *Cisco Annual Security Report* die aktuellen Entwicklungen im Bereich der IT-Sicherheit. Neben der Rolle von Angreifern und Verteidigern liegt dabei ein besonderes Augenmerk auf den Benutzern, denn diese geraten zunehmend zum schwächsten Glied in der Sicherheitskette eines Unternehmens.

Das Thema Cybersicherheit ist äußerst breit gefasst und komplex und hat auf Privatnutzer ebenso große Auswirkungen wie auf Unternehmen, Regierungen und andere Einrichtungen weltweit. Der *Cisco Annual Security Report 2015* ist in vier Themenkomplexe gegliedert. Auf den ersten Blick kann der Eindruck entstehen, die darin behandelten Probleme stünden nur für sich allein. Bei genauerer Betrachtung wird jedoch deutlich, wie stark sie einander beeinflussen und miteinander in Zusammenhang stehen:

Die vier Themenkomplexe des *Cisco Annual Security Report 2015:*

1. Entwicklungen im Bedrohungsumfeld
2. Ergebnisse der Cisco Security Capabilites Benchmark Study
3. Geopolitische und Branchentrends
4. Cybersicherheit neu überdenken – vom Benutzer bis in die Führungsetage

1. Bedrohungsinformationen

Dieser Abschnitt bietet einen Überblick über aktuelle Forschungsergebnisse von Cisco sowie die neuesten Trends bei Exploit-Kits, Spam, Bedrohungen, Sicherheitslücken und Malvertising (bösartige Online-Werbung). Beleuchtet werden außerdem die zunehmend von Cyberkriminellen eingesetzten Methoden, die Aktivitäten der Benutzer als Ausgangspunkt für ihre Angriffe zu nutzen. Die Grundlage für Ermittlung der Trends im Jahr 2014 bildet ein umfangareicher Satz an globalen Telemetriedaten, die von den Experten von Cisco Security Research analysiert wurden.

2. Ergebnisse der Security Capabilities Benchmark Study

Cisco hat in neun Ländern Chief Information Security Officer (CISO) und Sicherheitsverantwortliche aus Unternehmen unterschiedlicher Größe zu ihren Sicherheitsressourcen und -verfahren befragt, um zu ermitteln, wie diese den aktuellen Sicherheitsstatus ihres Unternehmens einschätzen. Die Ergebnisse der Studie finden Sie exklusiv im *Cisco Annual Security Report 2015*.

3. Geopolitische und Branchentrends

In diesem Abschnitt gehen Experten von Cisco für Sicherheits-, geo- und regionalpolitische Belange auf aktuelle und zukünftige geopolitische Trends ein, die Unternehmen und insbesondere multinationale Konzerne im Auge behalten sollten. Zentrales Thema dabei: Die Zunahme der Cyberkriminalität in Regionen mit schwachen staatlichen Strukturen. Ebenfalls diskutiert werden aktuelle globale Entwicklungen in den Bereichen Datensouveränität, Datenlokalisierung, Verschlüsselung und Datenkompatibilität.

4. Cybersicherheit neu überdenken – vom Benutzer bis in die Führungsetage

Um Sicherheit heute effektiv gewährleisten zu können, müssen Unternehmen das Thema Cybersicherheit neu überdenken. Die Experten von Cisco betonen: Sowohl vor als auch während und nach einem Angriff müssen fortschrittliche Sicherheitskontrollen implementiert werden. Eine wichtiger Appell lautet außerdem: Sicherheit muss Chefsache werden. Wollen Unternehmen ihren Angreifern einen Schritt voraus sein, müssen sie darüber hinaus anpassungsfähiger werden. Möglich wird dies durch einen Sicherheitsansatz, der auf den Prinzipien des „Cisco Sicherheitsmanifest“ basiert.

Die im *Cisco Annual Security Report 2015* behandelten Themen laufen in der Gesamtschau auf Folgendes hinaus: Die Angreifer verstehen es inzwischen noch geschickter, Sicherheitslücken auszunutzen, um ihre schädlichen Aktivitäten zu verbergen. Benutzer und Sicherheitsteams sind gleichermaßen Teil des Problems. Viele Sicherheitsverantwortliche halten ihre Sicherheitsprozesse und -tools zwar für effektiv, tatsächlich besteht jedoch häufig Nachholbedarf. Geopolitische Entwicklungen – von der Gesetzgebung verschiedener Länder bis hin zur Sicherheitslage in bestimmten Regionen – müssen genau beobachtet werden. Denn diese können direkte Auswirkungen auf den Geschäftsbetrieb von Unternehmen sowie darauf haben, wie sie das Thema Sicherheit angehen. Alle diese Faktoren machen deutlich: Unternehmen aller Größenordnungen müssen erkennen, dass es bei der Sicherheit auf die Benutzer ankommt, dass Kompromittierungen unvermeidlich sind und dass es genau jetzt an der Zeit ist, ihren Sicherheitsansatz auf den Prüfstand zu stellen.

Wichtigste Erkenntnisse

Der Cisco Annual Security Report 2015 *fördert wichtige Erkenntnisse zutage.*

Angreifer greifen auf immer raffiniertere Techniken zurück, um über Sicherheitslücken in ihre Zielsysteme zu gelangen und von dort aus unentdeckt zu operieren.

- 2014 wurde ein Prozent der Sicherheitslücken aus dem Common-Vulnerabilities-and-Exposures-Verzeichnis (CVE) aktiv genutzt. Unternehmen müssen daher Prioritäten setzen und sicherstellen, dass sie dieses eine Prozent schnell beheben. Doch selbst führende Sicherheitstechnologie kann Sicherheitslücken nur wirksam schließen, wenn sie durch solide Prozesse unterstütztt wird.
- Seit „Blackhole" im Jahr 2013 hat kein anderes Exploit-Kit einen ähnlichen Erfolg erzielt. Möglich ist aber auch, dass die Entwickler aktueller Exploit-Kits weniger Aufsehen erregen möchten.
- Bei Java-Exploits wurde ein Rückgang von 34 Prozent verzeichnet. Der Grund: Java ist sicherer geworden und daher weniger attraktiv für Angreifer.
- Neuartige Flash-Malware interagiert mit JavaScript. Dies erschwert die Erkennung und Analyse ihrer Aktivitäten erheblich.
- Das Spam-Aufkommen hat von Januar 2014 bis November 2014 um 250 Prozent zugenommen.
- Snowshoe-Spam ist eine zunehmende Bedrohung. Dabei wird jeweils eine geringe Menge Spam von einer großen Anzahl unterschiedlicher IP-Adressen versendet, um die Erkennung zu vermeiden.

Ohne es zu bemerken, werden Benutzer und IT-Teams Teil des Sicherheitsproblems.

- Cyberkriminelle lassen sich bei der Installation von Malware oder beim Aufdecken von Sicherheitslücken von den Benutzer in die Hände spielen.
- Die Heartbleed-Sicherheitslücke macht OpenSSL extrem angreifbar. Dennoch sind 56 Prozent aller OpenSSL-Versionen älter als 50 Monate und damit weiterhin gefährdet.
- Benutzer vernachlässigen die Sicherheit beim Surfen im Internet. Zudem fahren Angreifer stärker zielgerichtete Kampagnen. In zahlreichen Branchen erhöht dies das Risiko für Malware-Infektionen – das höchste Risiko bestand 2014 in der Pharma- und Chemieindustrie.
- Zur Verbreitung von Malware und unerwünschten Anwendungen greifen Cyberkriminelle auf Webbrowser-Add-ons zurück, da viele Benutzer Add-ons grundsätzlich als vertrauenswürdig oder unbedenklich betrachten.

Die Cisco *Security Capabilities Benchmark Study* zeigt: Unternehmen wiegen sich in falscher Sicherheit.

- 59 Prozent der Chief Information Security Officers (CISOs) und 46 Prozent der Sicherheitsverantwortlichen halten ihre Sicherheitsprozesse für optimal.
- Etwa 75 Prozent der CISOs erachten ihre Sicherheitstools als sehr oder äußerst effektiv. Nur ca. 25 Prozent sind der Meinung, dass ihre Sicherheitstools nur in einem gewissen Maß effektiv sind.
- Bei 91 Prozent der Unternehmen mit einem fortschrittlichen Sicherheitsansatz hat das Thema IT-Sicherheit hohe Priorität in der Unternehmensführung.
- Weniger als 50 Prozent der Befragten verwenden Standardtools wie Patching und Konfigurationsmanagement, um Sicherheitslücken zu schließen.
- In mittelständischen Unternehmen ist das Sicherheitsniveau tendeziell höher als in Unternehmen anderer Größen.

Inhalt

Angreifer vs. Verteidiger: ein ständiger Wettlauf

Jeder will dem anderen einen Schritt voraus sein.

Auf Verteidigerseite wurde aufgerüstet – viele nutzen mittlerweile fortschrittlichere Tools, um sich gegen Angriffe abzusichern und die Auswirkungen von Sicherheitsvorfällen gering zu halten. Sie haben erkannt, dass Sicherheit ein geschäftskritischer Faktor ist – und sie sind von ihren Sicherheitsvorkehrungen überzeugt. Auch die Technologieanbieter sind aktiver geworden: Sie suchen gezielter nach Schwachstellen in ihren Produkten und beheben diese, bevor sie von Kriminellen ausgenutzt werden können.

Doch auch die Angreifer schlafen nicht: Nicht nur beim Durchführen ihrer Angriffe, auch beim Verbergen ihrer Aktivitäten werden sie immer raffinierter.

- Sie ändern dynamisch ihre Taktiken und Tools, verschwinden aus einem Netzwerk, bevor sie erkannt werden können oder schalten blitzschnell auf eine andere Methode um.
- Sie fahren Spam-Kampagnen mit Hunderten von IP-Adressen, um reputationsbasierte Anti-Spam-Produkte zu umgehen.
- Sie tarnen Malware als Tools, denen Benutzer vertrauen oder die sie als unbedenklich betrachten, um von deren Systemen aus unbemerkt weitere Infektionen einzuleiten.
- Kaum wurde eine Sicherheitslücke behoben, haben sie bereits eine andere Schwachstelle gefunden, die sie ausnutzen können.
- Sie nisten sich bei ihrem Zielunternehmen ein, teilweise über Wochen oder Monate hinweg, bis sie genügend Ausgangspositionen in der Infrastruktur und den Benutzerdatenbanken eingerichtet haben. Erst dann starten sie ihre eigentlichen Aktivitäten.

Der neuen *Cisco Security Capabilities Benchmark Study* (siehe Seite 24) zufolge befinden Sicherheitsverantwortliche ihre Abwehrmaßnahmen als effektiv. Dennoch ist Datendiebstahl weiterhin an der Tagesordnung, Scamming bleibt nach wie vor lukrativ, und noch immer gelingt es politisch motivierten Kräften, Netzwerke lahmzulegen. Letzlich gesehen ist IT-Sicherheit ein Zahlenspiel: Selbst wenn 99,99 Prozent aller Spam-Nachrichten abgefangen werden können, bedeutet dies noch immer, dass einige durchkommen. Eine vollständige Absicherung gibt es nicht.

Unternehmen setzen vermehrt auf Lösungen, die Netzwerke, Malware und Spam abwehren. Dennoch ist es möglich, dass einige ihren Weg bis zum Benutzer finden. Und dann werden die Benutzer selbst zur Schwachstelle, z. B. wenn sie auf fingierte Anfragen zum Zurücksetzen eines Kennworts hereinfallen.

Die Benutzer werden also zu einem immer schwächeren Glied in der Sicherheitskette. Für Unternehmen wirft dies Fragen auf: Öffnen intuitivere und benutzerfreundlichere Anwendungen und Software neue Schlupflöcher für Cyberkriminelle? Sollen sie annehmen, dass die Benutzer nicht vertrauenswürdig oder lernfähig sind, und deshalb strengere Sicherheitskontrollen einführen, die den Benutzern aber die Arbeit im Tagesgeschäft erschweren? Sollen sie sich die Zeit nehmen, die Benutzer über die Gründe für Sicherheitskontrollen aufzuklären und ihnen zu verdeutlichen, welche entscheidende Rolle sie bei der Gewährleistung von dynamischer Sicherheit spielen?

Die Prinzipien aus dem „Sicherheitsmanifest“ von Cisco auf Seite 45 machen deutlich: Letzteres ist definitiv der beste Ansatz. Technologielösungen allein reichen nicht aus, die Benutzer müssen aktiv in die Sicherheitsstrategie engebunden werden. Denn andernfalls umgehen sie Maßnahmen, die sie in ihrer alltäglichen Arbeit behindern – und schwächen somit eher die Sicherheit. Heute geht es nicht mehr darum, *ob* ein Netzwerk kompromittiert wird, sondern *wann*. Wie reagiert ein Unternehmen dann? Und wenn die Sicherheitsteams wüssten, dass dieser Fall eintreten wird, würden sie das Thema Sicherheit dann anders angehen?

Der *Cisco Annual Security Report 2015* stellt aktuelle Untersuchungsergebnisse der Cisco Security Research Group vor. Im Fokus stehen dabei Neuerungen aus der Sicherheitsbranche, die Unternehmen und Benutzer bei der Abwehr von Angriffen unterstützen sollen, sowie die Techniken und Strategien, die Angreifer nutzen, um die Abwehrmechanismen zu umgehen. Der Report analysiert außerdem die Ergebnisse der *Cisco Security Capabilities Benchmark Study*, in deren Rahmen der Sicherheitsstatus von Unternehmen sowie deren Selbsteinschätzung ihrer Verteidigungsmaßnahmen gegen Cyberangriffe untersucht wird. Ebenfalls diskutiert werden geopolitische Trends, globale Entwicklungen rund um Datenlokalisierung, die Vorteile von fortschrittlichen Zugriffskontrollen und von Segmentierung durch rollenbasierten Zugriff, sowie die Wichtigkeit, Cybersicherheit zu einem Vorstandsthema zu machen.

1. Bedrohungsinformationen

Den Erkenntnissen in diesem Report liegt ein globaler Satz an Telemetriedaten zu Malware-Datenverkehr und anderen bekannt gewordenen Bedrohungen zugrunde, die von Cisco Security Research laufend analysiert und ausgewertet werden. Dies ermöglicht Rückschlüsse auf künftige Aktionen von Cyberkriminellen und kann zur besseren Erkennung beitragen.

Für Autoren von Exploit-Kits gilt: weniger ist oft mehr

Unternehmen streben danach, Branchenführer zu werden. Exploit-Kit-Autoren geben sich mit weniger zufrieden. Eine geringere Popularität ist Cisco Security Research zufolge in vielen Fällen sogar von den Autoren gewünscht.

Wie aus dem *Cisco Midyear Security Report 2014* hervorging, lies sich seit 2013 unter den Exploit-Kits keine eindeutige Spitzenposition mehr ermitteln.[1] Damals verlor das weitverbreitete, zuverlässig gepflegte und äußerst effektive „Blackhole Exploit Kit" an Bedeutung, nachdem „Paunch", sein mutmaßlicher Entwickler und Vertreiber, den Behörden ins Netz ging. Dass derzeit kein Exploit-Kit den Markt dominiert, könnte laut Cisco Security Research darauf hindeuten, dass sich bislang keiner der aktuellen Angriffsbaukästen als technisch überlegen erwiesen hat. Seit Paunch und Blackhole außer Gefecht sind, scheinen zudem mehr Exploit-Kit-Nutzer in Angriffsbaukästen zu investieren, die technisch auf das Verschleiern von Aktivitäten ausgerichtet sind.

Im Jahr 2014 waren den Sicherheitsexperten von Cisco zufolge „Angler", „Sweet Orange" und „Goon" die am häufigsten „in freier Wildbahn" beobachteten Exploit-Kits. Dabei wurde Angler 2014 am häufigsten erkannt, und zwar vor allem Ende August – die Gründe hierfür sind jedoch unklar. Cisco Security Research führt die Popularität von Angler darauf zurück, dass für die Verbreitung von Malware bei diesem Kit keine Windows-Programmdatei heruntergeladen werden muss.

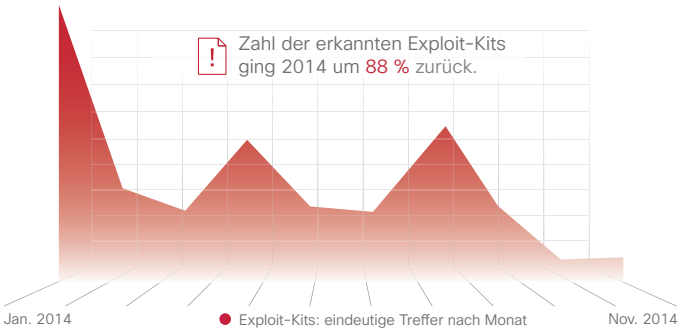
Angler macht sich Sicherheitslücken in Flash, Java, Microsoft Internet Explorer (IE) und auch Silverlight zunutze. Die Forscher von Cisco raten daher, dieses Exploit-Kit ganz besonders im Auge zu behalten. Sobald der Exploit ausgelöst wird, schreibt Angler den Malware-Playload nicht auf eine Festplatte, sondern direkt in den Arbeitsspeicher, z. B. in einen Prozess wie iexplore.exe. Der von Angler verbreitete Playload sieht aus wie ein formloses Objekt aus verschlüsselten Daten, was die Erkennung und Blockierung erschwert.

Näheres zu Angler und darüber, wie Cyberkriminelle das Exploit-Kit über Malvertising bei Benutzern einschleusen, erfahren Sie im Cisco Security Blog-Beitrag „Angling for Silverlight Exploits".

Sweet Orange ist ebenfalls äußerst dynamisch. Seine Komponenten, Ports und Playload-URLs werden laufend verändert, um einer Erkennung zu entgehen. Cisco Security Research schätzt die Effektivität – und damit das Gefahrenpotenzial – von Sweet Orange im Vergleich zu anderen Exploit-Kits am höchsten ein. Sweet Orange schleust Malware unterschiedlicher Art in ungepatchte Endbenutzer-Systeme ein und enthält Exploits für Sicherheitslücken in Adobe Flash Player, IE und Java. Angreifer, die Sweet Orange verwenden, bedienen sich häufig Malvertising-Techniken, um Benutzer (auch an legitime) Websites weiterzuleiten, die das Exploit-Kit hosten. Dabei werden die Benutzer in der Regel mindestens zweimal weitergeleitet. Kompromittierte Websites, auf denen veraltete Versionen von Content-Management-Systemen (z. B. von WordPress oder Joomla) ausgeführt werden, sind ebenfalls dafür bekannt, Sweet Orange zu hosten.[2]

Das Goon-Exploit-Kit ist Cisco Security Research zufolge für seine Zuverlässigkeit bekannt. Dies ist vermutlich auch der Grund für seine zwar eher geringe, aber dafür beständige Popularität im Jahr 2014. Im Vergleich zu anderen Exploit-Kits gilt es bei den Experten von Cisco als das am besten strukturierte. Goon – auch bekannt als Goon/Infinity-Exploit-Kit – wurde erstmals 2013 von Sicherheitsforschern entdeckt. Es handelt sich dabei um ein Framework zur Verbreitung von Malware, das Exploits für Sicherheitslücken in Flash-, Java- oder Silverlight-Komponenten generiert, die auf Windows- oder Mac-Browsern ausgeführt werden.[3]

Abbildung 1: Trends bei Exploit-Kits: Anzahl der eindeutigen Treffer von Januar bis November 2014



Quelle: Cisco Security Research

Im Blog-Beitrag „Fiesta Exploit Pack Is No Party for Drive-By Victims“ geht Cisco Security darauf ein, wie sich Unternehmen gegen das Fiesta-Exploit-Kit absichern können. Dieser Angriffsbaukasten verbreitet Malware über Angriffsvektoren wie Silverlight und verwendet dynamische DNS-Domänen (DDNS) als Landing Pages für den Exploit.

Näheres zum Nuclear-Exploit-Kit, das Benutzersysteme nach Sicherheitslücken absucht und durch diese Lücken geeignete Malwaretypen einschleust,erfahren Sie im Cisco Security Blog-Beitrag „Evolution of the Nuclear Exploit Kit“.

Insgesamt ist zwar festzuhalten, dass die Anzahl erkannter Exploit-Kits in den Monaten nachdem Blackhole ausgeschaltet wurde um 87 Prozent zurückgegangen ist. Im Sommer 2014 verzeichnete Cisco Security Researchallerdings eine Zunahme an erkannten Kits (siehe Abbildung 1). Ein erheblicher Anstieg war in den letzten beiden Augustwochenbei Angler-Exploit-Kits festzuhalten. Im November war die Gesamtzahl an bekannten Exploit-Kits, die erkannt wurden, jedoch wieder rückläufig, wobei Angler und Goon/Infinity auch in diesem Monat am häufigsten zu finden waren. Insgesamt ging die durchschnittliche Anzahl der erkannten Exploit-Kits zwischen Mai und November 2014 um 88 Prozent zurück.

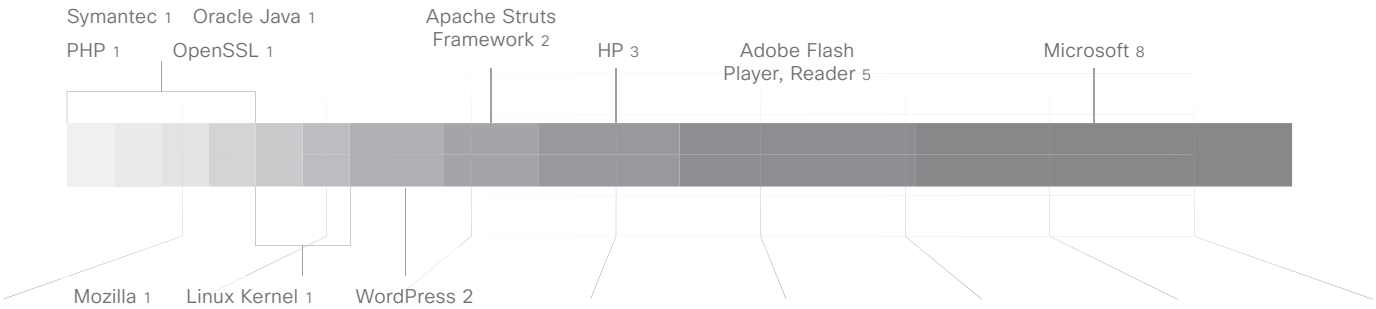
Sicherheitsbedrohungen und -lücken: Java wird als Angriffsvektor zunehmend uninteressant

In den vergangenen Jahren gehörte Java noch zur unglücklichen Riege der Spitzenreiter in Sachen Häufigkeit und Schweregrad der Sicherheitslücken. Cisco Security Research zufolge wird Java aber zunehmend unbeliebt bei Angreifern, da diese schnellere, einfachere und schwerer erkennbare Wege bevorzugen, um Exploits über Sicherheitslücken in Softwareprodukten einzuschleusen.

Unter den 25 wichtigsten anbieter- und produktbezogenen Schwachstellen, die im Zeitraum vom 1. Januar 2014 bis zum 30. November 2014 gemeldet wurden, war Java nur einmal vertreten (siehe „Tabelle 1: Common Vulnerability Scoring System (CVSS)“ auf Seite 10). 2013 zählte Cisco Security Research noch 54 neue Java-Sicherheitslücken mit hoher Dringlichkeit, 2014 dagegen nur 19. Allerdings: Diese älteren Schwachstellen bleiben auch weiterhin ein beliebtes Angriffsziel.

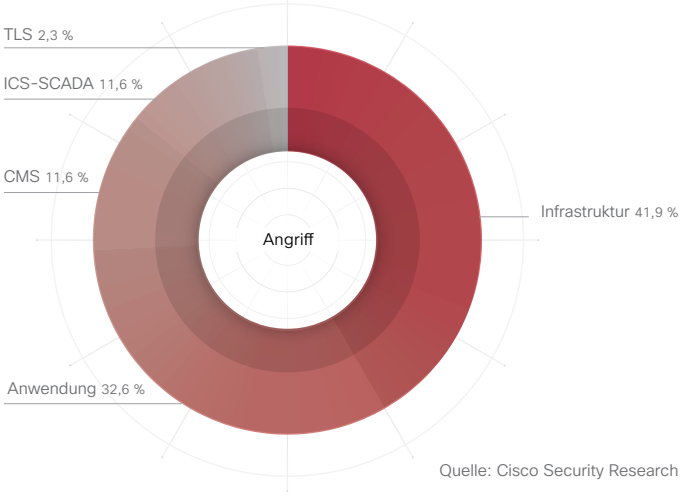
Die Daten der National Vulnerability Database (NVD) zeigen einen ähnlichen Rückgang: Im Jahr 2013 verzeichnete die NVD 309 Java-Sicherheitslücken, 2014 nur noch 253. (Die von Cisco Security Research ermittelte Zahl ist niedriger, da nur schwerwiegende Sicherheitslücken erfasst werden, die einen hohen Wert auf der CVSS-Skala erreichen. Die NVD umfasst dagegen alle gemeldeten Sicherheitslücken.) Abbildung 2 zeigt die für das Jahr 2014 ermittelte Anzahl der ausgenutzten Sicherheitslücken nach Anbieter und Produkt.

Abbildung 2: Anzahl der am häufigsten ausgenutzten Sicherheitslücken nach Anbieter und Produkt



Quelle: Cisco Security Research

Abbildung 3: Populärste Produktkategorien für Exploits



Quelle: Cisco Security Research

Exploits, die client-seitige Sicherheitslücken in Adobe Flash Player und Microsoft IE nutzen, haben Java von der Spitzenposition verdrängt. Ebenfalls weit vorne liegen Exploits, die auf Server abzielen (z. B. Exploits, die Schwachstellen in Apache Struts, dem Open-Source-Framework für Web-Anwendungen, nutzen). Die zunehmende Anzahl an Apache Struts Framework-Exploits ist ein Beispiel dafür, dass Kriminelle immer häufiger auf die Online-Infrastruktur zurückgreifen, um ihre Reichweite und die Wirksamkeit ihrer Angriffe auszubauen.

Aufgrund seiner Beliebtheit ist das Apache Struts Framework ein logischer Ausgangspunkt für Exploits.

Abbildung 3 zeigt die populärsten Produktkategorien für Exploits im Jahr 2014.

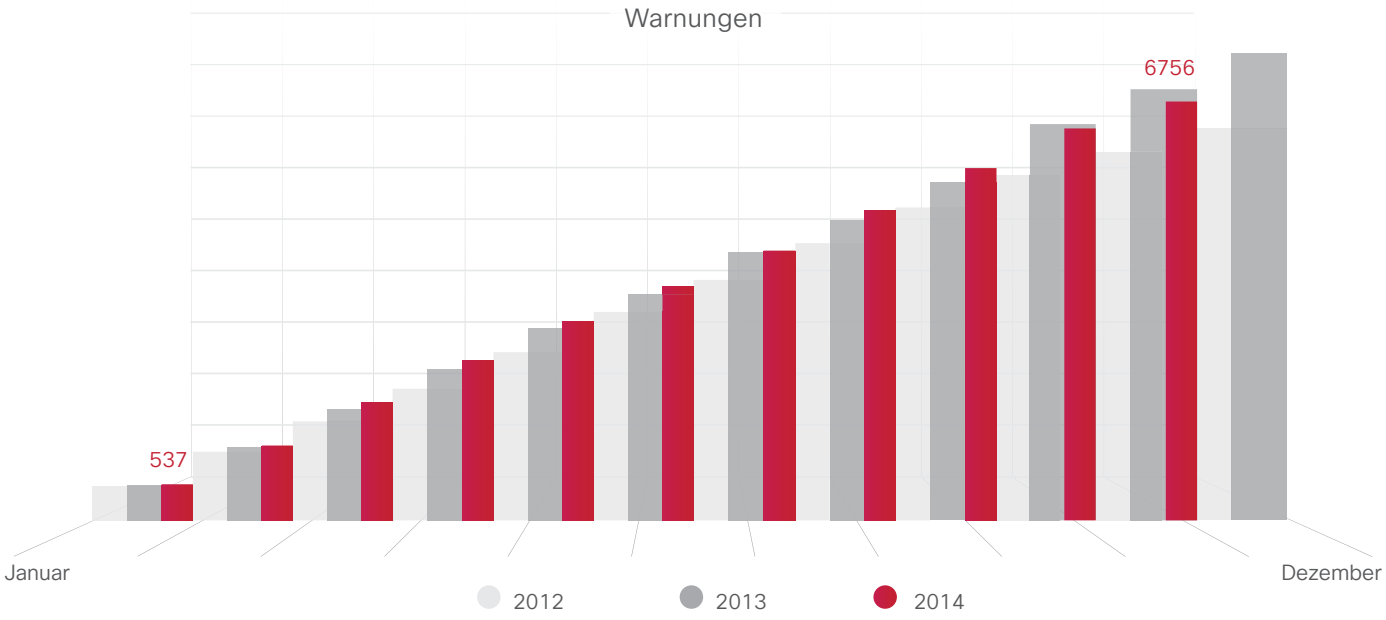
Entsprechend der Daten von Cisco Security Research waren Anwendungen und Infrastruktur im Jahr 2014 am häufigsten Ziel von Angriffen. Content-Management-Systeme (CMS) sind ebenfalls beliebte Ziele. Angreifer nutzen Websites, die veraltete CMS-Versionen ausführen, um Exploits zu verbreiten.

Warnmeldungen pro Jahr insgesamt rückläufig

Die Gesamtanzahl der Warnmeldungen pro Jahr – die Summe der neuen und aktualisierten Produktsicherheitslücken, die 2014 gemeldet und von Cisco Security Research zusammengestellt wurden – ist insgesamt zurückgegangen (Abbildung 4). Im November 2014 wurden insgesamt um 1,8 Prozent weniger Warnmeldungen als im Jahr 2013 verzeichnet. Dieser Wert ist zwar gering, markiert jedoch erstmals seit einigen Jahren einen Rückgang gegenüber dem Vorjahr.

Dies ist mit großer Wahrscheinlichkeit darauf zurückzuführen, dass von Anbieterseite ein stärkerer Fokus auf Softwaretests und -entwicklung gelegt wird. In der Folge werden Entwicklungszyklen verkürzt und so die Zahl der Sicherheitslücken reduziert, die Kriminelle leicht ausnutzen können.

Abbildung 4: Gesamtanzahl der Warnmeldungen pro Jahr



Quelle: Cisco Security Research

Tabelle 1: Am häufigsten ausgenutzte Sicherheitslücken

IntelliShield-ID	Beschreibung	Dringlichkeit	Glaubwürdigkeit	Schweregrad	Basis	Zeitwert
		Common Vulnerability Scoring System (CVSS)				
33695	OpenSSL TLS/DTLS Heartbeat Information Disclosure Vulnerability				5,0	5,0
35880	GNU Bash Environment Variable Content Processing Arbitrary Code Execution Vulnerability				10,0	7,4
35879	GNU Bash Environment Variable Function Definitions Processing Arbitrary Code Execution Vulnerability				10,0	7,4
36121	Drupal Core SQL Injection Vulnerability				7,5	6,2
32718	Adobe Flash Player Remote Code Execution Vulnerability				9,3	7,7
33961	Microsoft Internet Explorer Deleted Memory Object Code Execution Vulnerability				9,3	7,7
28462	Oracle Java SE Security Bypass Arbitrary Code Execution Vulnerabilities				9,3	7,7
30128	Multiple Vendor Products Struts 2 Action: Parameter Processing Command Injection Vulnerability				10,0	8,3

Quelle: Cisco Security Research

Neue und aktualisierte Warnungen im Vergleich

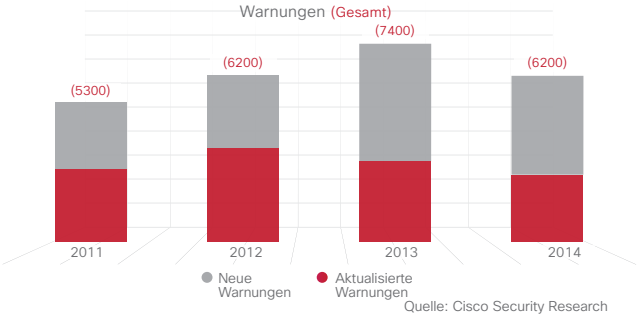
Die Anzahl neuer Warnungen für 2013 und 2014 zeigt: Im Vergleich zu den Vorjahren werden auch weiterhin mehr neue Sicherheitslücken gemeldet. Das bedeutet, dass Anbieter, Entwickler und Sicherheitsexperten eine steigende Zahl neuer Sicherheitslücken in ihren Produkten entdecken, beheben und diese melden. Wie in Abbildung 5 zu sehen ist, sind die Gesamtzahl neuer Warnungen und die jährliche Gesamtzahl in den Jahren 2014 und 2013 unverändert bzw. leicht rückläufig.

In Tabelle 1 sind einige der gemäß des Common Vulnerability Scoring System (CVSS) am häufigsten ausgenutzten Sicherheitslücken aufgeführt. Die National Vulnerability Database (NVD) des US-amerikanischen National Institute of Standards and Technology (NIST) bietet ein Rahmenwerk für die Veröffentlichung der Eigenschaften und Auswirkungen von IT-Sicherheitslücken und unterstützt das CVSS. Der „Dringlichkeitswert" in der CVSS-Tabelle zeigt an, dass diese Sicherheitslücken aktiv ausgenutzt werden. Der entsprechende „Zeitwert" kennzeichnet aktive Exploits. Anhand der Liste der angegriffenen Produkte können Unternehmen zudem erkennen, ob sie Produkte nutzen, die überwacht und gepatcht werden müssen.

In Abbildung 6 sind die Anbieter und Produkte mit den höchsten CVSS-Werten dargestellt. Cisco gibt durch den CVSS-Wert an, dass ein Proof-of-Concept-Exploit-Code existiert, von dessen freier Verfügbarkeit jedoch nichts bekannt ist.

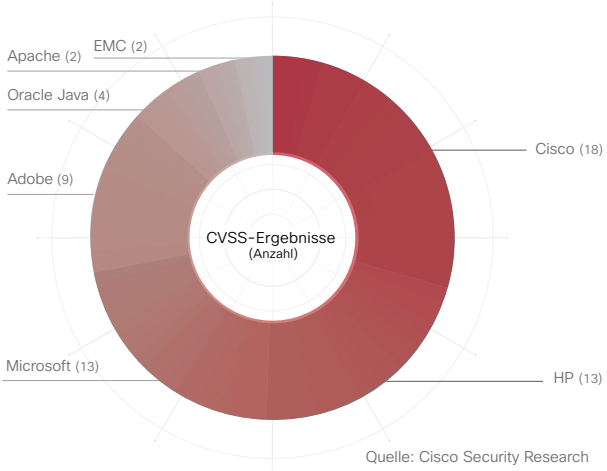
Hinweis: Bei den Sicherheitslücken in Tabelle 1 handelt es sich um diejenigen, die während des Untersuchungszeitraums erste Zeichen einer Exploit-Aktivität gezeigt haben. Der Großteil dieser Sicherheitslücken gehörte noch nicht zum „Mainstream", d. h. sie waren noch nicht Bestandteil kommerzieller Exploit-Kits.

Abbildung 5: Neue und aktualisierte Warnungen im Vergleich



Quelle: Cisco Security Research

Abbildung 6: Anbieter und Produkte mit den höchsten CVSS-Werten



Quelle: Cisco Security Research

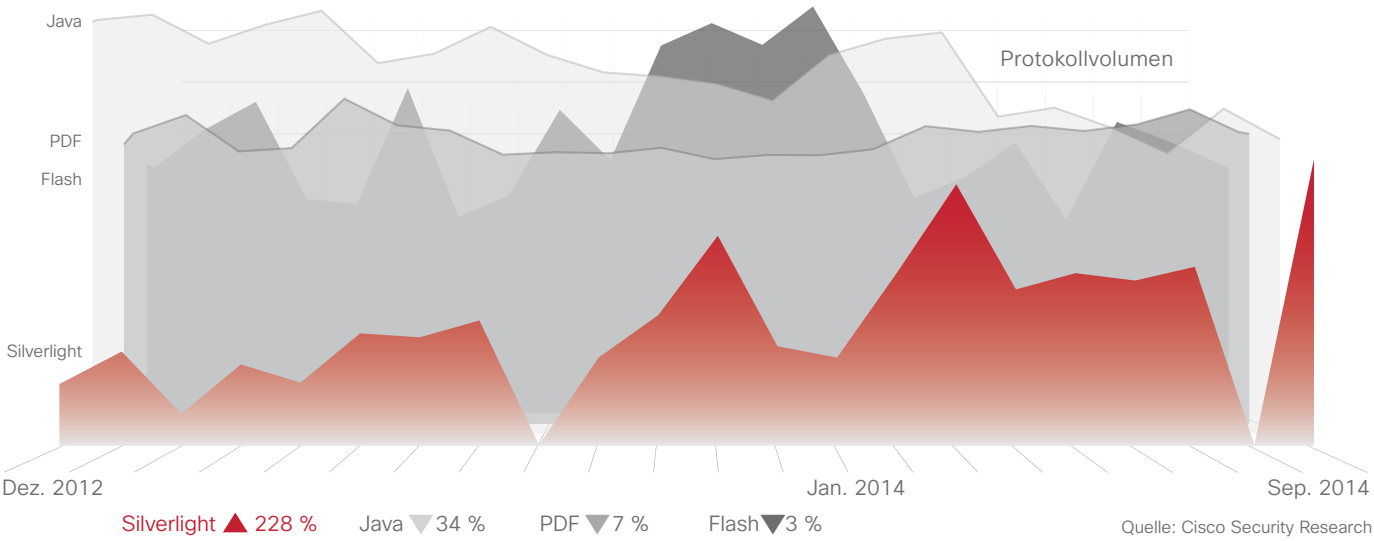
Analyse: Mögliche Faktoren für den Rückgang von Java-Exploits

Cisco Security Research nennt als einen der möglichen Gründe für den Rückgang bei Java-Exploits die Tatsache, dass im Jahr 2014 keine neuen Zero-Day-Exploits für Java bekannt wurden, die einen Angriff ermöglicht hätten. Neuere Versionen von Java führen Patches zudem automatisch aus und ältere, anfälligere, Versionen des Java Runtime Environment werden von den Browser-Anbietern standardmäßig blockiert. Apple geht sogar noch weiter: Ältere und anfällige Java-Versionen werden deaktiviert und Patches über automatische Updates eingespielt. Ein weiterer Faktor: Seit Januar 2013 rät das United States Computer Emergency Readiness Team (US-CERT) dazu, Java abzusichern, zu deaktivieren oder komplett zu deinstallieren.

Die aktuelle Version 8 von Java bietet bessere Kontrollen als frühere Versionen. Zudem lassen sich Sicherheitslücken jetzt schwerer ausnutzen, da nun eine Interaktion mit dem Benutzer via Code-Signing erforderlich ist und der Benutzer über ein Dialogfeld gefragt wird, ob Java aktiviert werden soll. Cyberkriminelke haben mittlerweile leichtere Ziele als Java ausgemacht und nehmen andere Vektoren ins Visier, die eine größere Ausbeute versprechen. So werden z. B. Adobe Flash, PDF-Leseprogramme oder Browser von vielen Benutzern nicht regelmäßig aktualisiert. Hier bietet sich über bekannte und neue Sicherheitslücken eine größere Angriffsfläche. Und, wie bereits aus dem *Cisco Midyear Security Report 2014* hervorging, sind mittlerweile Exploit-Kits im Aufwind, die Microsoft Silverlight-Exploits umfassen.[4]

Abbildung 7 zeigt: Java, bislang der führende Angriffsvektor, verliert seit mehr als einem Jahr stetig an Bedeutung. Bei Flash ist der Verlauf eher unregelmäßig, wobei ein besonders großer Ausschlag im Januar 2014 zu verzeichnen war. Die Nutzung von Sicherheitslücken in PDF-Leseprogrammen blieb konstant – viele Angreifer scheinen also weiterhin auf zielgerichtete E-Mail-Kampagnen mit PDF-Anhängen zu setzen. Silverlight-Angriffe sind weiterhin vergleichsweise selten, insbesondere seit August zeichnet sich jedoch ein Aufwärtstrend ab.

Abbildung 7: Volumen-Trends nach Angriffsvektor



Quelle: Cisco Security Research

Höheres Gefahrenpotenzial durch die Kombination aus Flash und JavaScript?

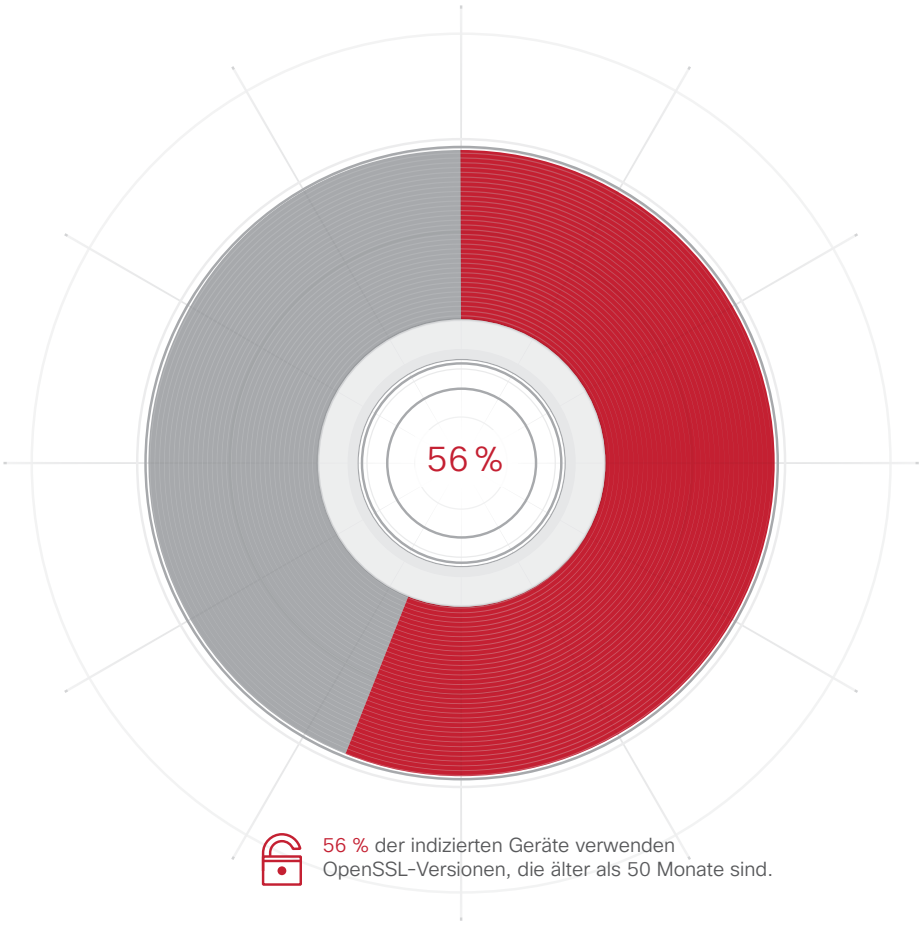
Cisco Security Research registrierte im Jahr 2014 zunehmend Flash-Malware, die mit JavaScript interagiert. Der Exploit erfolgt dabei verteilt über eine Flash- und eine JavaScript-Datei. Ein so Exploit erschwert Sicherheitstools die Identifizierung und Blockierung. Schwieriger wird zudem die Analyse mittels Reverse-Engineering. Für Cyberkriminelle ist dieser Ansatz effizienter und effektiver: Erfolgt die erste Stufe des Angriffs z. B. vollständig über JavaScript, wird die Payload erst in der zweiten Stufe, nach erfolgreicher JavaScript-Ausführung, übertragen. So empfangen nur Benutzer die Payload, die die schädliche Datei ausführen können.

Gefahrenherd veraltete Software: Patches allein sind nicht die Lösung

Wie bereits auf Seite 8 erläutert, bevorzugen Angreifer für ihre Exploits den Weg des geringsten Aufwands. Sie wählen Produkte, die eine größereAngriffsfläche bieten – was im Allgemeinen auf nicht aktualisierte oder veraltete Software zutrifft. So sind z. B. nach wie vor zahlreiche Systeme für die Poodle-Sicherheitslücke im SSL-Protokoll anfällig. Ungepatchte Appliances sind also weiterhin ein Problem.[5] Mit Blick auf die beobachteten Trends weist Cisco Security Research auf eine bedenklich hohe Verbreitung veralteter und angreifbarer Softwareversionen hin und stellt klar: Dieser Zustand wird auch weiterhin zu ernsthaften Sicherheitsvorfällen führen.

Mithilfe von Scan-Engines untersuchte Cisco Security Research mit dem Internet verbundene Geräte, die OpenSSL nutzten. Das Ergebnis: 56 Prozent verwendeten über 50 Monate alte Versionen von OpenSSL. Das bedeutet: Selbst nach Bekanntwerden Heartbleed-Sicherheitslücke[6] in TLS (Transport Layer Security) im Jahr 2014 versäumen es Unternehmen, ihre Systeme durch dieses dringende Upgrade auf die neueste OpenSSL-Version besser abzusichern. Abbildung 8 zeigt den Anteil an veralteten OpenSSL-Versionen im Einsatz.

Abbildung 8: Anteil an veralteten OpenSSL-Versionen im Einsatz



Quelle: Cisco Security Research

Automatische Updates und Patches können helfen

Automatische Updates können vor Gefahren schützen. Cisco Security Research untersuchte die Daten von Geräten, die entweder Chrome oder IE für den Internetzugriff verwendeten. Das Ergebnis: 64 Prozent der Chrome-Anfragen erfolgten über die neueste Version, bei IE dagegen wurde nur bei 10 Prozent der Anfragen die neueste Version verwendet.

Cisco Security Research kommt daher zu dem Schluss: Das automatische Update-System von Chrome kann besser sicherstellen, dass möglichst viele Benutzer die neueste Softwareversion einsetzen. Möglich wäre aber auch, dass Chrome-Nutzer technisch versierter sind als IE-Nutzer und ihre Browser daher eher aktualisieren und Updates installieren.

Die Kombination dieser Daten mit dem Rückgang der Sicherheitslücken und Exploits bei Java macht deutlich: Software, die automatisch aktualisiert wird, kann zu einem insgesamt stärkeren Sicherheit-Framework beitragen. Da manuelle Aktualisierungsprozesse unausweichlich irgendwann zu einer Kompromittierung der Systeme führen, sollten Unternehmen heute auf automatische Updates setzen – auch wenn dadurch von Zeit zu Zeit Ausfälle oder Probleme mit der Kompatibilität auftreten können.

Risiken im Branchenvergleich: zielgerichtete Angriffe und nachlässige Benutzer – eine gefährliche Kombination für Unternehmen in Hochrisiko-Branchen

In der Pharma- und Chemieindustrie wurde 2014 das höchste Auftrittsrisiko von Malware ermittelt. In der ersten Jahreshälfte stand die Medien- und Verlagsbranche an der Spitze, fiel bis November jedoch auf den zweiten Platz zurück. Zu den fünf führenden Branchen zählen außerdem Fertigung, Transport/Spedition und die Luftfahrt. Alle diese Segmente waren in der ersten Hälfte des Jahres 2014 unter den oberen Fünf platziert.

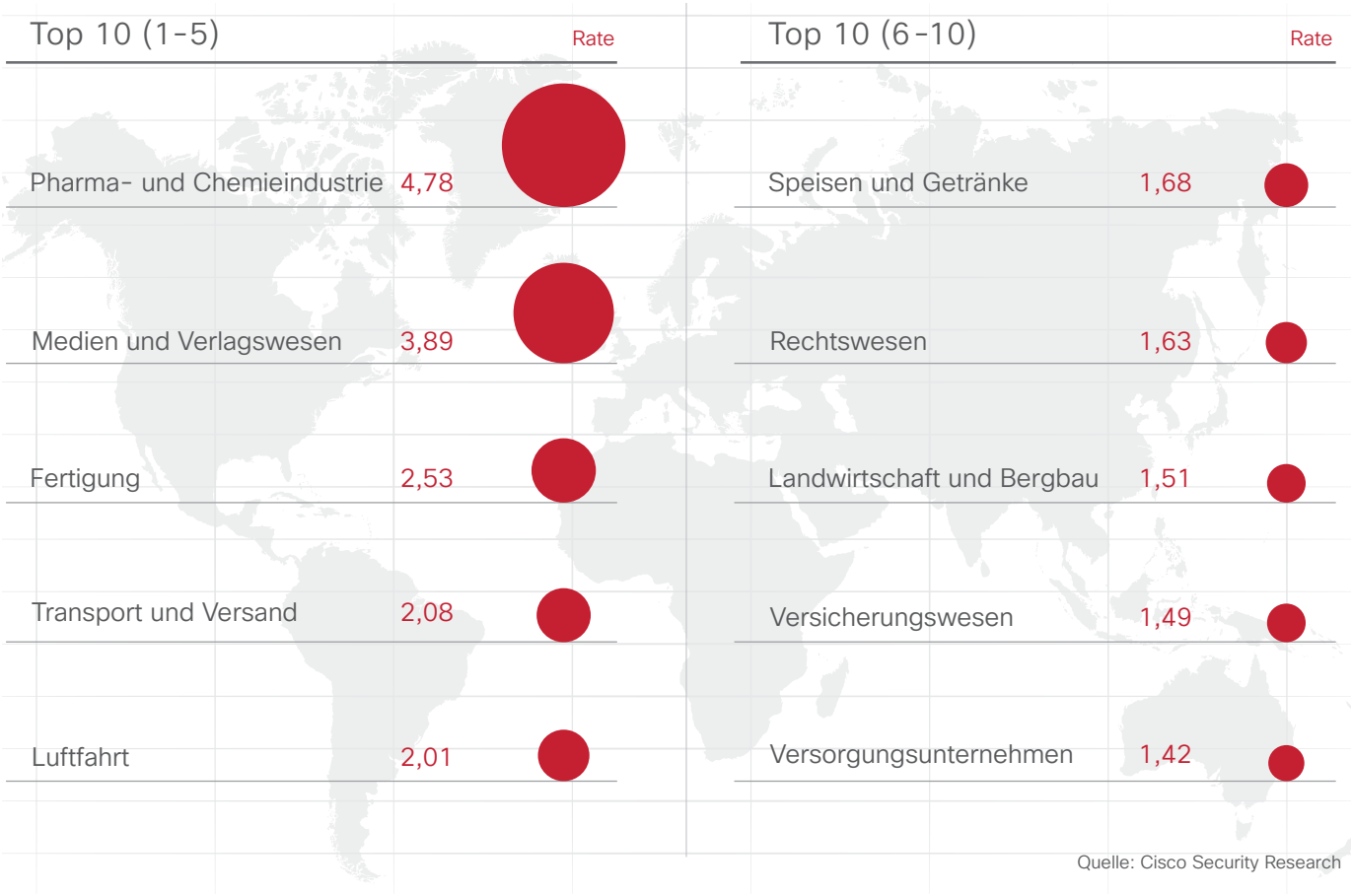
Es mag verblüffen, dass der Einzelhandel in dieser Liste nicht höher platziert ist, nachdem in dieser Branche erst kürzlich einige Angriffe für großes Aufsehen sorgten. Die Rangliste basiert jedoch nicht auf tatsächlichen Verletzungen, sondern auf dem Auftreten von Malware in einer Branche.

Um branchenspezifische Zahlen für das Auftreten von Malware zu bestimmen, vergleicht Cisco Security Research die durchschnittliche Auftrittsrate aller Unternehmen, die Cisco Cloud Web Security verwenden, mit der durchschnittlichen Auftrittsrate aller Unternehmen in einer bestimmten Branche, die den Service nutzen (Abbildung 9). Eine Auftrittsrate von über 1 Prozent in einer Branche weist auf ein höheres Auftrittsrisiko von Web-Malware hin, eine Auftrittsrate unter 1 Prozent steht für ein niedrigeres Risiko. Wird bei einem Unternehmen z. B. eine Auftrittsrate von 1,7 Prozent ermittelt, liegt das Risiko 70 Prozent über dem Mittelwert. Bei einem Unternehmen mit einer Auftrittsrate von 0,7 Prozent liegt das Risiko dagegen 30 Prozent unter dem Mittelwert.

Auftreten und Kompromittierung im Vergleich

Das „Auftreten“ definiert einen Vorfall, bei dem Malware blockiert wird. Im Gegensatz zu einer „Kompromittierung“ wird der Benutzer beim Auftreten von Malware jedoch nicht infiziert, da keine Binärdatei heruntergeladen wird.

Abbildung 9: Auftrittsrisiko von webbasierter Malware nach Branche, alle Regionen, 1. Januar bis 15. November 2014



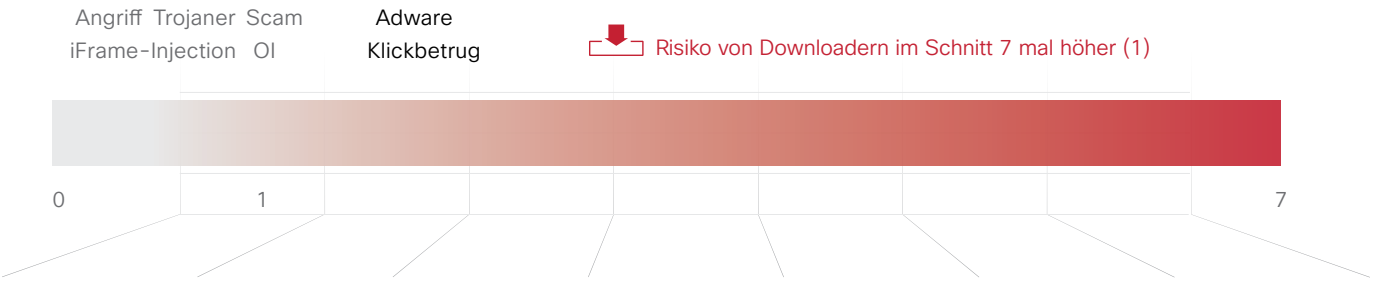
Quelle: Cisco Security Research

Cisco Security Research hat acht Typen von Angriffsmethoden untersucht (Abbildung 10), um die Faktoren für das Auftrittsrisiko von Malware in einer Branche zu ermitteln. Dabei ging es um die Frage, ob Kriminelle bestimmte Branchen stärker anvisieren, oder ob das Benutzerverhalten hinsichtlich der Internetnutzung im jeweiligen Segment hierbei entscheidend ist. Das Team kam zu dem Schluss: Das hohe Risiko in bestimmten Branchen ist einerseits auf zielgerichtete Angriffe und andererseits auf nachlässiges Verhalten der Benutzer zurückzuführen.

Um zu ermitteln, ob sich Benutzer in risikoreichen Branchen tatsächlich anders als in risikoarmen Branchen verhalten, untersuchte Cisco Security Research vier Typen nicht zielgerichteter Angriffsmethoden, mit denen Internetnutzer häufig konfrontiert sind: Adware, Klickbetrug, Scam und iframe-Injections. Ebenfalls untersucht wurden komplexere Angriffsmethoden, die Angreifer häufig bei zielgerichteten Kampagnen einsetzen: Exploit, Trojaner, OI (Erkennungs-Malware) und Downloader.

Hinweis: Die acht Angriffsmethoden wurden von Cisco Security Research in vier heuristische Kategorien eingeteilt.

Abbildung 10: Methoden von Web-Malware-Angriffen: Vergleich der oberen und unteren vier Hochrisiko-Branchen



Quelle: Cisco Security Research

Anhand der oberen und unteren vier Branchen mit dem höchsten Malware-Risiko ermittelte Cisco Security Research anschließend mit Hilfe der Daten von Cisco Cloud Web Security den Prozentsatz der Vorfälle für jede Angriffsmethode und bestimmte dann für die oberen und unteren vier Branchen Durchschnittsraten. Der in Abbildung 10 dargestellte Vergleich wurde durch Dividieren des oberen Durchschnittswertes durch den unteren Durchschnittswert abgeleitet. Ein Verhältnis mit dem Wert 1 weist darauf hin, dass bei den am stärksten und am wenigsten betroffenen Gruppen dieselben Aktivitätsmuster beobachtet wurden.

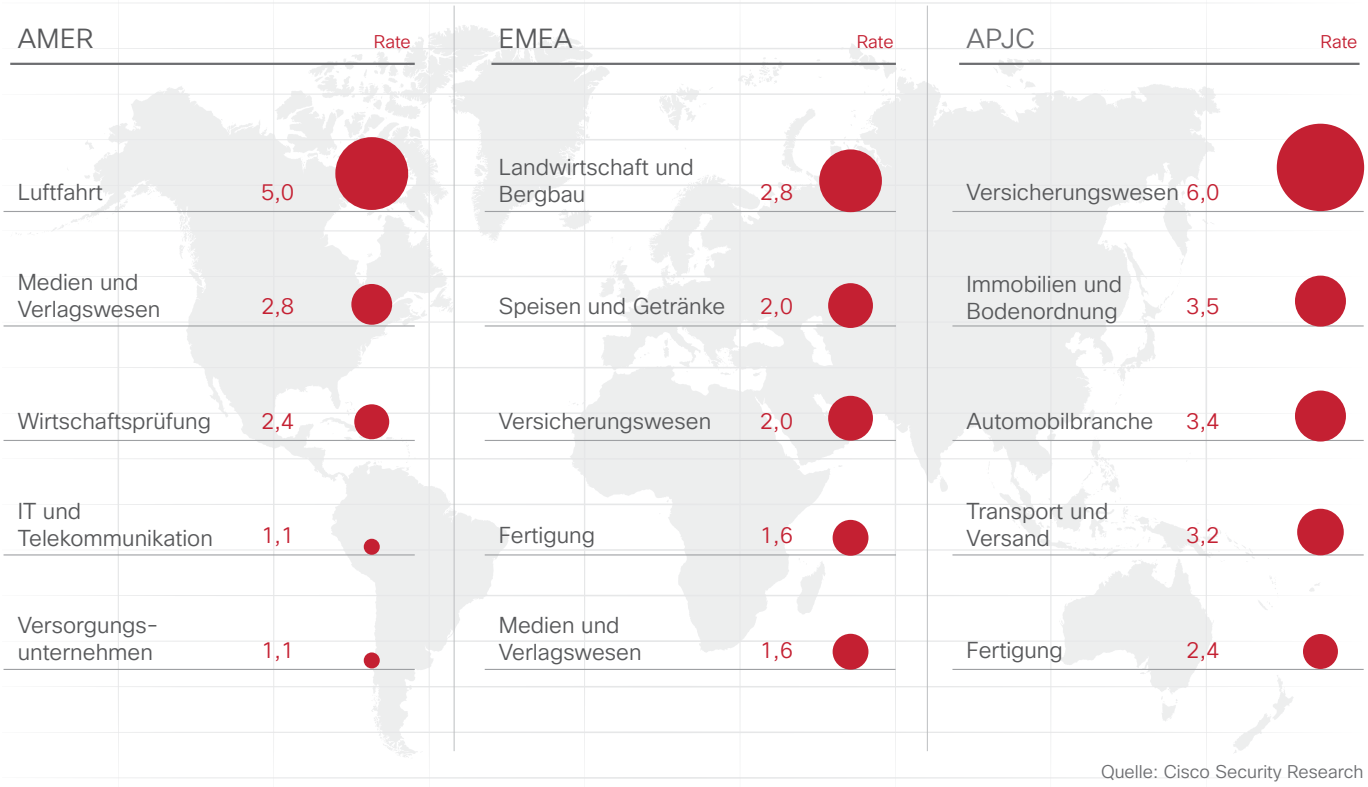
Die Daten zeigen, dass die meisten Branchensegmente mit hohem Risiko von hochentwickelten Downloader-Angriffen betroffen waren, und zwar siebenmal häufiger als die unteren vier Branchensegmente mit hohem Risiko. Ein solcher Wert würde ebenfalls erreicht, wenn zielgerichtete Angriffe auf die Branchen mit dem höchsten Risiko ausgerichtet werden.

Die Auftrittsrate von Klickbetrug und Adware ist in den am häufigsten betroffenen Branchen mit hohem Risiko im Vergleich zu den weniger stark betroffenen Branchen mit geringerem Risiko ebenfalls höher. Dies deutet darauf hin, dass die Differenz komplexere Ursachen hat und nicht nur auf die Ausrichtung von Angreifern auf bestimmte Branchen zurückzuführen ist. Die Gefährdung durch Malware-Angriffe wird außerdem durch das Verhalten der Internetnutzer beeinflusst – in Branchen mit hohem Risiko trägt es zur höheren Auftrittsrate von Web-Malware bei. Auch in Branchen, in denen Wettbewerb und Innovation stark von neuen Medien getrieben werden, sind die Benutzer anfälliger für Web-Malware als in anderen Branchen, in denen die Internetnutzung stark eingeschränkt und/oder streng kontrolliert wird (z. B. in der Regierung).

Cisco Security Research geht davon aus, dass das Risiko von Web-Exploits für Benutzer in der Medien- und Verlagsbranche höher ist als bei Benutzern aus anderen Branchensegmenten, da das Internet in dieser Branche sehr häufig genutzt wird.

Hinweis: Im Jahr 2014 wurde in der Medien- und Verlagsbranche eine überdurchschnittlich hohe Auftrittsrate von Web-Malware-Angriffen verzeichnet. Tatsächlich überstieg sie die von Cisco Security Research seit 2008 ermittelten Zahlen deutlich. Dieser Anstieg kann auch in Zusammenhang mit dem mittlerweile weiter verbreiteten Malvertising auf seriösen Websites stehen.

Abbildung 11: Hochrisiko-Branchen für Malware-Angriffe in den Regionen AMER, APJC und EMEA



Quelle: Cisco Security Research

Auftreten von Malware nach Region

Im Folgenden ist das Auftrittsrisiko von Web-Malware für Hochrisiko-Branchen nach Region angegeben. Die drei Regionen sind wie folgt definiert:

- Nordamerika, Zentralamerika und Lateinamerika (AMER)
- Asien-Pazifik-Raum, China, Japan und Indien (APJC)
- Afrika, Europa und Naher Osten (EMEA)

Cisco Security Research kam bei der Ermittlung aller Hochrisiko-Branchen weltweit (siehe in Abbildung 11 aufgelistete Branchen) zu folgenden Ergebnissen:

- Bei Benutzern aus dem Versicherungswesen in der APJC-Region ist das Auftrittsrisiko von Malware sechsmal höher als bei Benutzern in den 12 Branchen, die in allen drei Regionen untersucht wurden (Basisdurchschnitt: 1,5).
- Bei Benutzern aus der Luftfahrtbranche in der AMER-Region ist das Auftrittsrisiko von Malware fünfmal höher.
- Bei Benutzern aus der Immobilien- und Landverwaltungsbranche in der APJC-Region und bei Benutzern aus der Automobilindustrie in dieser Region ist das Auftrittsrisiko jeweils um den Faktor 3,5 höher.
- Bei Benutzern aus Transport und Versand in der APJC-Region ist das Auftrittsrisiko um den Faktor 3,25 höher.

Cisco Security Research nennt rasant steigende Grundstücks- und Immobilienpreise, die Naturkatastrophen der jüngsten Vergangenheit und die hohe Export- und Produktionsleistung in der APJC-Region als Faktoren dafür, dass Angreifer Benutzer in dieser Region anvisieren, die in der Automobil-, Versicherungs-, Immobilien- und Landverwaltungs- oder Transport- und Speditionsbranche arbeiten oder Geschäfte mit diesen Branchen tätigen. Der Diebstahl von Kundendaten, geistigem Eigentum (einschließlich Angriffe durch Staaten) und Luftfrachtdaten sind wahrscheinlich die wichtigsten Gründe für die Ausrichtung von Angreifern auf Benutzer aus der Luftfahrtbranche in der AMER-Region.

Methoden zur Verbreitung von Malware nach Region

Die Abbildungen 12a bis 12c zeigen die Angriffstechniken, die in der jeweiligen Region am häufigsten zur Verbreitung von Malware genutzt werden. Zur Ermittlung dieser Ergebnisse wurde die Web-Malware, die entsprechend der Daten von Cisco Cloud Web Security in einer Region blockiert wurde (d. h. auftrat), mit allen Bedrohungstypen im Internet ins Verhältnis gesetzt.

Im Verlauf des Jahres 2014 erfolgten die Angriffe in der AMER-Region hauptsächlich mit bösartigen Skripten, iframe-Injections lagen weit abgeschlagen auf dem zweiten Platz. In der APJC-Region wurden im letzten Jahr häufig Scams, bösartige Skripte und webbasierte Exploits verwendet, um Benutzer aller Branchen anzugreifen. In der EMEA-Region wurden besonders viele webbasierte Exploits verzeichnet.

Im Blog-Beitrag „Threat Spotlight: Group 72“, von Cisco Security erfahren Sie, wie Cisco Security Research dazu beitrug, eine Gruppe von Angreifern zu identifizieren und zu verhindern, dass diese wertvolles geistiges Eigentum von bedeutenden Unternehmen aus den Bereichen Fertigung, Industrie, Luft- und Raumfahrt, Verteidigung und Medien erbeuten.

Einzelheiten zum Remote Administration Tool (RAT), das Group 72 für die Internetspionage verwendete, finden Sie in diesem Beitrag: „Threat Spotlight: Group 72, Opening the ZxShell“.

Abbildung 12a. Verteilung der Angriffsmethoden, AMER

Angriffsmethode	Gesamt %
Skript	24,93 %
iFrame-Injection	17,43 %
Exploit	13,63 %
OI (Erkennungs-Malware)	10,35 %
Trojaner	10,06 %

Quelle: Cisco Security Research

Abbildung 12b. Verteilung der Angriffsmethoden, APJC

Angriffsmethode	Gesamt %
Scam	25,26 %
Skript	25,04 %
iFrame-Injection	18,68 %
OI (Erkennungs-Malware)	9,93 %
Exploit	6,72 %

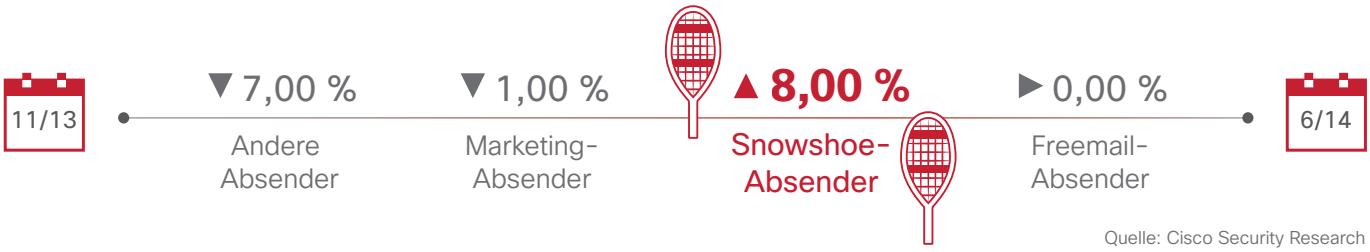
Quelle: Cisco Security Research

Abbildung 12c. Verteilung der Angriffsmethoden, EMEA

Angriffsmethode	Gesamt %
iFrame Angriff	51,48 %
Skript	15,17 %
Angriff	8,64 %
Scam	7,31 %
OI (Erkennungs-Malware)	4,16 %

Quelle: Cisco Security Research

Abbildung 13: Zunahme von Snowshoe-Spam



Quelle: Cisco Security Research

Aktuelle Spam-Trends: Spammer setzen auf „Snowshoe"-Strategie

Phishing bleibt auch weiterhin attraktiv, da Benutzer noch immer auf altbekannte Spam-Taktiken hereinfallen. Cyberkriminelle haben erkannt: Angriffe auf Browser- und E-Mail-Ebene (also auf die Benutzer) führen viel leichter zum Ziel als der Versuch zur Kompromittierung von Servern. Spammer arbeiten daher auch weiterhin an immer raffinierteren Methoden.

Es ist nicht unüblich, dass ein Anti-Spam-System über 99 Prozent der Spam-Nachrichten abfängt, die es durchlaufen. Führende Systeme können sogar mit einer Abfangrate von über 99,9 Prozent aufwarten. Vor diesem Hintergrund ziehen Spammer alle Register, um Spam-Filter zu umgehen. Immer beliebter wird die im Folgenden beschriebene Taktik, mit deren Hilfe Anti-Spam-Technologie umgangen werden soll, die die Reputation einer IP-Adresse prüft.

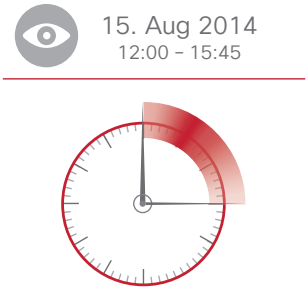
Konkret geht es um „Snowshoe"-Spam: Der Vergleich ist treffend, denn Schneeschuhe ermöglichen das Laufen über Tiefschnee, indem das Gewicht auf eine größere Oberfläche verteilt und so ein Versinken im Schnell verhindert wird. Beim Snowshoe-Spamming werden Massen-E-Mails von einer großen Zahl von IP-Adressen versendet, dabei jedoch eine gringe Zahl von E-Mails pro Adresse. Einige Spam-Filter sind nicht in der Lage, diese Art von Nachrichten zu blockieren. Abbildung 13 zeigt die Zunahme von Snowshoe-Spam zwischen 2013 und 2014.

Kürzlich beobachtete Cisco Security Research eine Snowshoe-Spam-Kampagne, bei der die Angreifer ein Blitzverfahren verwendeten. Die gesamte Spam-Kampagne lief dabei nur drei Stunden, war aber zu einem bestimmten Zeitpunkt tatsächlich für zehn Prozent des weltweiten Spam-Datenverkehrs verantwortlich (Abbildung 14).

Mehr zu Snowshoe-Spam erfahren Sie im Cisco Security Blog-Beitrag „Snowshoe Spam Attack Comes and Goes in a Flurry."

Die Forscher von Cisco konnten bei den untersuchten Snowshoe-Nachrichten einige Standardmerkmale von Spam ausmachen. So enthielten sie Betreffzeilen mit Schreibfehlern wie „Recnhung 2921411.pdf" mit einer zufällig generierten Zahl. Bei den Anhängen handelte es sich in der Regel um PDF-Dateien mit einem Trojaner, der eine Schwachstelle von Adobe Reader ausnutzt.

Abbildung 14: Snowshoe-Spam-Kampagne

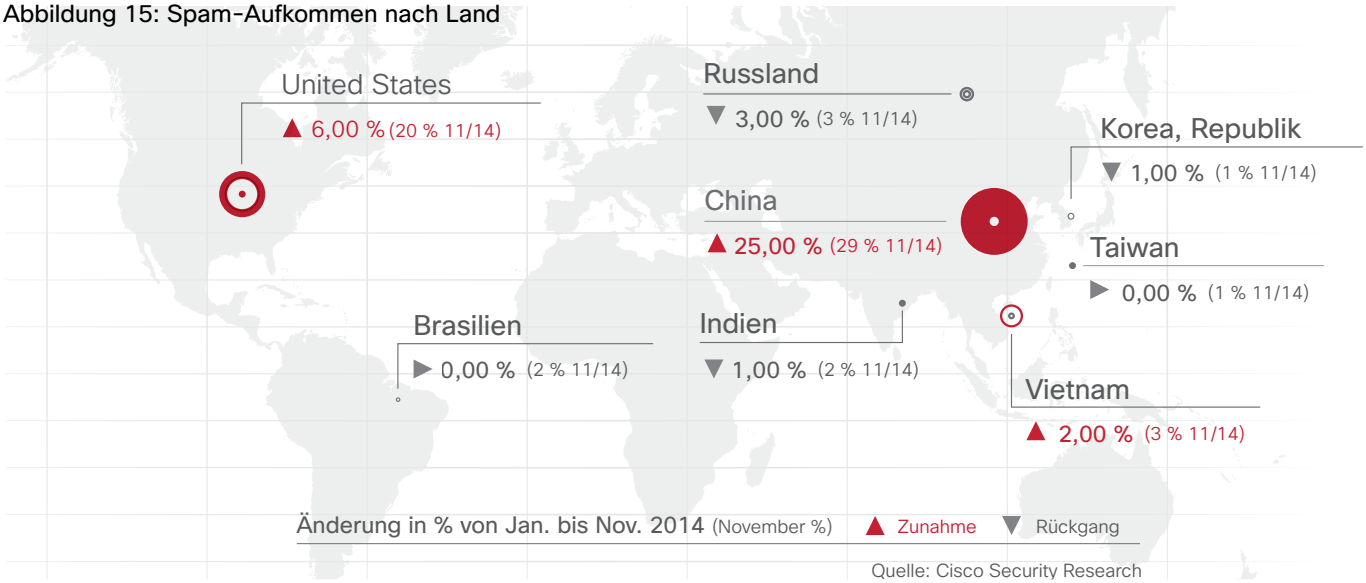


Quelle: Cisco Security Research

Sicherheitsteams sollten jedoch beachten, dass reputationsbasierte Lösungen nicht unbedingt zuverlässigen Schutz vor Snowshoe-Spam bieten, da dieselben Nachrichten im Falle einer Botnet-Kampagne von hunderten oder sogar tausenden Ursprungsorten stammen können. Eine präzisere Erkennung kann durch die Untersuchung auf andere Spam-Merkmale wie die Pflege des E-Mail-Servers erzielt werden. So stimmten bei den von Cisco Security Research beobachteten Kampagnen beispielsweise bei vielen IP-Adressen Forward- und Reverse-DNS nicht überein. Dies gilt im Allgemeinen als ein sicheres Zeichen dafür, dass ein Mail-Server nicht vertrauenswürdig ist.

Bei vielen dieser IP-Adressen gab es auch keine Aufzeichnungen darüber, dass über sie bereits vor dem Beginn der Snowshoe-Kampagne E-Mails versendet wurden. Dies deutet ebenfalls darauf hin, dass Internetkriminelle kompromittierte Systeme zur Erstellung einer Infrastruktur für Snowshoe-Spam verwenden.

Abbildung 15: Spam-Aufkommen nach Land



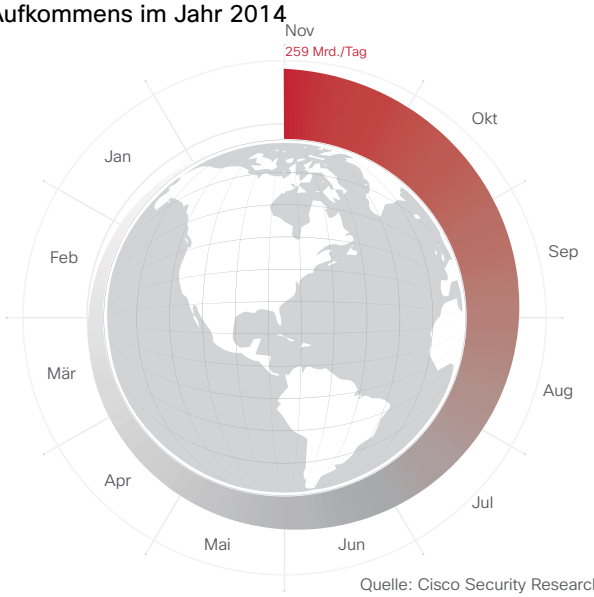
Quelle: Cisco Security Research

Spammer fahren schärfere Geschütze auf, um Benutzer zu überlisten

Das weltweit steigende Aufkommen legt nahe: Spam bleibt für Cyberkriminelle auch weiterhin lukrativ (Abbildung 16). Durch immer geschicktere Formulierungen erhöhen sie ihre Aussichten, dass der Empfänger auf gefährliche Links in der Spam-Nachricht klickt. Ein beliebtes Mittel ist dabei das Social Engineering.

In den USA deutete der Trend 2014 auf ein rückläufiges Spam-Aufkommen hin, in anderen Ländern wurde allerdings im gleichen Zeitraum eine Zunahme verzeichnet (Abbildung 15). Cisco Security Research zufolge ist dies ein Indiz dafür, dass Angreifer zunehmend aus anderen Ländern heraus operieren. Plausibel wäre auch, dass in anderen Regionen mittlerweile ähnlich viel Spam wie in den USA generiert wird. Bislang jedenfalls waren die USA in dieser Hinsicht weltweiter Spitzenreiter. Und auch für 2014 war in den USA eine Zunahme zu verzeichnen.

Abbildung 16: Weltweite Zunahme des Spam-Aufkommens im Jahr 2014



Quelle: Cisco Security Research

Spear-Phishing-Nachrichten gehören seit Jahren zum Standardrepertoire von Cyberkriminellen. Doch mittlerweile sind sie so ausgeklügelt, dass selbst erfahrene Endnutzer Schwierigkeiten haben, fingierte E-Mails von authentischen zu unterscheiden. Gezielt versendet, enthalten diese E-Mails raffiniert gestaltete Nachrichten, die vermeintlich von namhaften Anbietern oder Dienstleistern stammen, von denen die Benutzer auch sonst Nachrichten erhalten. Dies können z. B. Lieferdienste, Online-Shops oder Musik- und Unterhaltungsanbieter sein. Einer fingierten E-Mail mit einem bekannten Namen und Logo werden die den Empfänger mit deutlich größerer Wahrscheinlichkeit täuschen als die altbekannten Spam-Nachrichten mit Werbung für Medikamente oder Uhren. Wird die Nachricht zudem durch eine Handlungsaufforderung ergänzt, die dem Empfänger vertraut ist, z. B. eine Bestellbestätigung oder eine Sendungsverfolgungsnummer, wird er noch stärker geneigt sein, auf die Links in der E-Mail zu klicken.

Cisco Security Research hat kürzlich eine kleine Anzahl von Spear-Phishing-Nachrichten mit Apple Inc. als Absender beobachtet, in denen behauptet wurde, dass die Empfänger ein beliebtes Spiel für iOS-Mobilgeräte heruntergeladen hätten. Die Betreffzeile der E-Mail enthielt eine zufällig generierte Rechnungsnummer, die den vermeintlich seriösen Eindruck verstärkte, da im Regelfall auch legitime E-Mails eine solche Nummer enthalten. Ein Link in der Nachricht legte den Empfängern nahe, sich anzumelden und ihr Kennwort zu ändern, falls sie den Download des Spiels nicht gestartet hätten. Der Link leitete die Benutzer an eine bekannte Phishing-Website weiter.

Spam-Nachrichten werden modifiziert, um Erkennung zu entgehen

Erweist sich ein bestimmtes Schema als erfolgreich für Spammer, d. h. sie konnten Empfänger zum Anklicken von Links in Spam-E-Mails oder zum Kauf gefälschter Produkte verleiten, optimieren sie die Nachrichten unter Beibehaltung ihrer grundlegenden Struktur. Dennoch halten sie die Nachrichten unterschiedlich genug, damit sie – wenigstens für kurze Zeit – nicht von Spam-Filtern erkannt werden. Tabelle 2 zeigt, wie häufig der Nachrichteninhalt während eines Stichprobenzeitraums modifiziert wurde, um die laufenden Gegenmaßnahmen zu umgehen. In der Tabelle sind diejenigen Bedrohungen aufgeführt, bei denen Regeländerungen für die Cisco Email Security Appliance (ESA) erforderlich wurden.

Tabelle 2: Bedrohungswarnungen: Die langlebigsten Spam- und Phishing-Bedrohungen

IntelliShield-ID		Beschreibung	Version	Dringlichkeit	Glaubwürdigkeit	Schweregrad
24986		Warnung zu Bedrohungs-Outbreak: gefälschte FedEx Versandbenachrichtigung	95			
31819		Warnung zu Bedrohungs-Outbreak: gefälschte E-Mail bezüglich Zustellung eines Faxes	88			
30527		Warnung zu Bedrohungs-Outbreak: Anhang mit schädlichen persönlichen Bildern	81			
36121		Warnung zu Bedrohungs-Outbreak: gefälschte Nachricht bezüglich Zahlungs-Stornierung	80			
23517		Warnung zu Bedrohungs-Outbreak: gefälschte E-Mail-Nachricht zu Produktbestellung	79			
23517		Warnung zu Bedrohungs-Outbreak: gefälschter Rechnungsanhang	78			
27077		Warnung zu Bedrohungs-Outbreak: gefälschte Nachricht bezüglich Geldüberweisung	78			
26690		Warnung zu Bedrohungs-Outbreak: gefälschte Nachricht bezüglich Zahlung per Banküberweisung	78			

Quelle: Cisco Security Research

Malvertising über Browser-Add-ons: nicht der Schaden zählt, sondern das Geld

Cisco Security Research hat vor Kurzem eine umfassende Analyse einer webbasierten Bedrohung durchgeführt, bei der Webbrowser-Add-ons durch Malvertising (bösartige Online-Werbung) als Medium zur Verbreitung von Malware und unerwünschten Anwendungen eingesetzt werden. Das Team stellte fest, dass die Bedrohung starke Charakteristika eines Botnet aufwies. Im Rahmen der Untersuchung wurden die Aktivitäten von über 800.000 Benutzern in 70 Unternehmen im Zeitraum vom 1. Januar bis zum 30. November 2014 untersucht, um den Gesamtumfang sowie Zweck und Struktur der Bedrohung zu ermitteln.

Das Ergebnis: Diese Familie von Browser-Add-ons ist nicht nur weitaus umfangreicher als erwartet, die Malware-Autoren verwenden zudem eine Kombination aus äußerst komplexem, professionell geschriebenen Code und einem raffinierten Geschäftsmodell, um ihre Malware möglichst lange profitabel zu halten. Anders ausgedrückt: Auch ohne vollständige Kontrolle über den Ziel-Host lässt sich aus der Malware Gewinn schlagen. Dies führt dazu, dass immer mehr Malware bewusst auf eine geringere Beeinträchtigung des betroffenen Hosts ausgelegt und für eine langfristige Gewinngenerierung in einem großen Kreis von Betroffenen optimiert ist.

Kompromittierte Benutzer werden mit diesen schädlichen Browser-Add-ons infiziert, indem – im Regelfall ohne eindeutige Einwilligung des Benutzers – gebündelte Software (Software, die in Verbindung mit einem anderen Softwarepaket oder -produkt verteilt wird) installiert wird. Dies geschieht, wenn Benutzer Anwendungen wie PDF-Tools oder Videoplayer von unseriösen Quellen herunterladen und diese bewusst installieren, da sie sie für vertrauenswürdig halten.

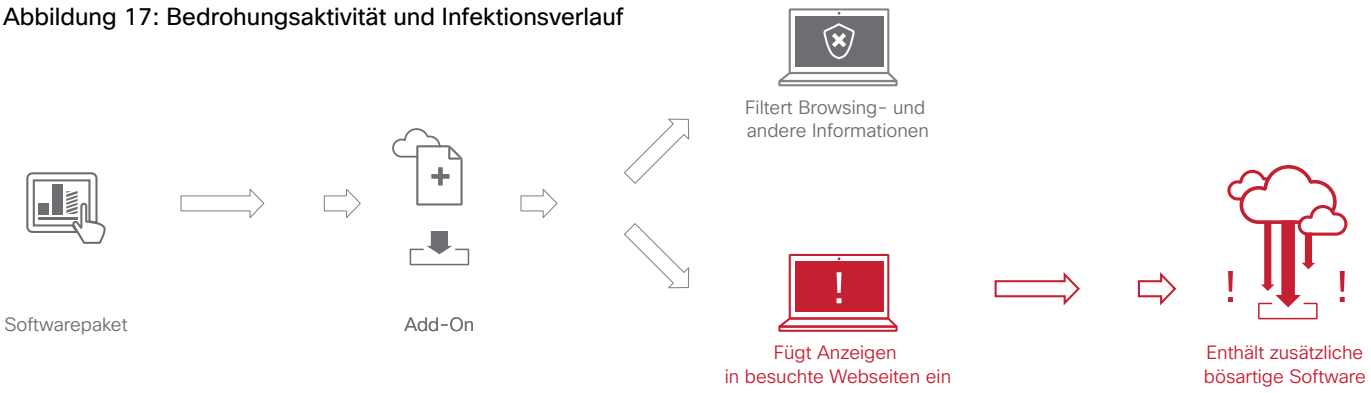
Die Anwendungen können dann mit unerwünschter oder schädlicher Software „gebündelt“ sein. Verbreitet wird die Malware im Rahmen eines PPI-Verfahrens (Pay-per-Install), bei dem der Herausgeber für jede Installation der in der ursprünglichen Anwendung gebündelten Software bezahlt wird.

Viele Benutzer vertrauen Add-ons unbesehen oder halten sie grundsätzlich für unbedenklich. Dieser Ansatz ist für die Verbreitung von Malware daher besonders erfolgversprechend. Für Angreifer ist dieses Verfahren attraktiv, da sie weniger auf andere Techniken wie Exploit-Kits angewiesen sind, die u. U. leichter erkennbar sind. (Siehe „Für Autoren von Exploit-Kits gilt: weniger ist oft mehr“ auf Seite 7.)

Cisco Security Research hat bei dieser Familie von Browser-Add-ons spezielle Charakteristika im Web-Datenverkehr beobachtet, die eine Identifizierung anhand der folgenden zwei Muster ermöglichen: Der Abfrage-String enthält in der Regel verschlüsselte Daten, in denen Informationen wie der Name des Add-ons und die zuvor vom Benutzer besuchte URL (einschließlich Intranet-Links) enthalten sind.

Im Verlauf der Analyse stieß Cisco Security Research auf über 4.000 verschiedene Namen von Add-ons, darunter z. B. PassShow, Bettersurf oder Bettermarkit, sowie zugeordnete SHAs (bee4b83970ffa8346f0e791be92555702154348c14bd8 a1048abaf5b3ca049e35167317272539fa0dece3ac1a60 10c7a936be8cbf70c09e547e0973ef21718e5). Da pro Installation mehr als ein Add-on-Name verwendet werden kann, ist die Malware sehr schwer nachzuverfolgen (Abbildung 17).

Abbildung 17: Bedrohungsaktivität und Infektionsverlauf



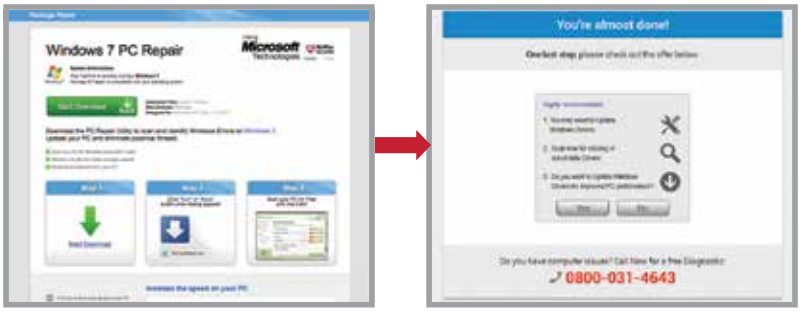
Quelle: Cisco Security Research

Malware verwendet je nach Betriebssystemtyp die geeigneten Exploits

Die von Cisco Security Research analysierten schädlichen Add-ons zeigten je nach Browser-„Fingerabdruck“ des Benutzers eine bestimmte Art von Werbung an. Bei den injizierten Anzeigen für Linux handelte es sich in der Regel um Websites für Online-Glücksspiel. Benutzer von Microsoft IE wurden zu Anzeigen für Downloads von scheinbar legitimer Software umgeleitet, die sich jedoch als schädlich entpuppte.

Linux

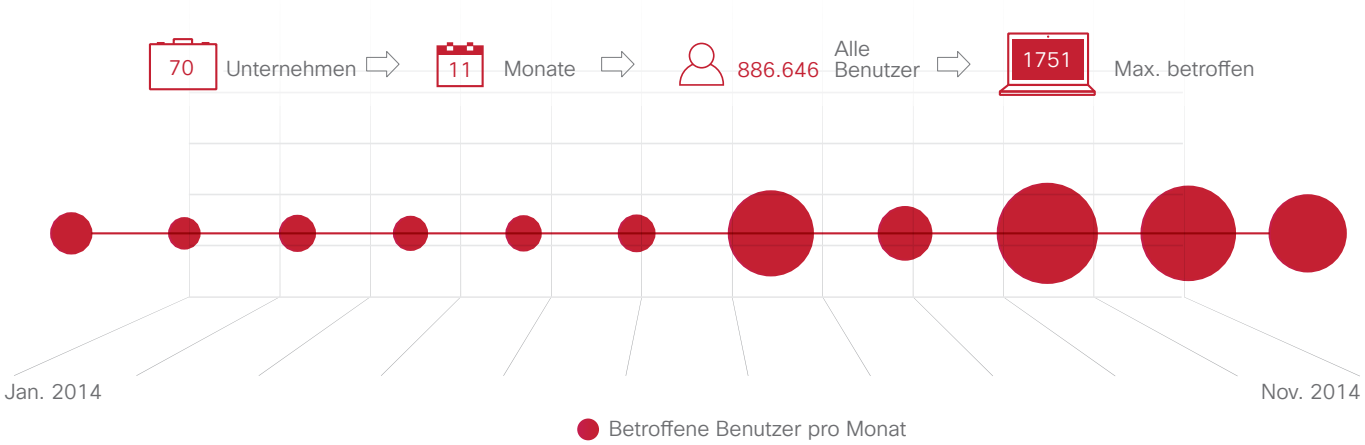
Microsoft IE



Die Analyse der Benutzeraktivität in über 70 Unternehmen über 11 Monate hinweg zeigt, dass die Zahl der von dieser Bedrohung betroffenen Benutzer steigt. Im Januar waren 711 Benutzer betroffen, in der zweiten Jahreshälfte bereits über 1.000, mit einem Spitzenwert von 1.751 im September (Abbildung 18). Der deutliche Anstieg im September und Oktober könnte auf die Online-Aktivität der Menschen zurückzuführen sein, die aus dem Sommerurlaub zurückkehrt sind.

Die Forscher von Cisco haben ermittelt, dass Angreifer ihre Malware-Kampagnen über viele verschiedene Server fahren. Diese Tatsache lässt sich unterschiedlich deuten: Möglich ist, dass die Bedrohung von einer kriminellen Organisation ausgeht, die ihre Aktivitäten geschickt verteilt. Möglich wäre aber auch, dass ein „Technologieanbieter“ sein Produkt an mehrere Gruppen verkauft. Unabhängig davon, wer für die Verbreitung der Malware verantwortlich ist, scheint jedoch das Ziel darin zu bestehen, ein Botnet von beachtlicher Größe zu erstellen.

Abbildung 18: Anzahl der betroffenen Benutzer pro Monat, Jan. bis Nov. 2014



Quelle: Cisco Security Research

Cisco Security Research konnte überdies mehr als 500 verschiedene Domains ermitteln, die mit dieser Bedrohung in Zusammenhang stehen. 24 davon sind im Alexa-Ranking der 1 Millionen meistbesuchten Domains aufgeführt, einige sogar mit einer verhältnismäßig hohen Platzierung (Abbildung 19). Das bedeutet, die Domains werden häufig aufgerufen, das Risiko ist jedoch sehr hoch, bei einem Besuch infiziert zu werden.

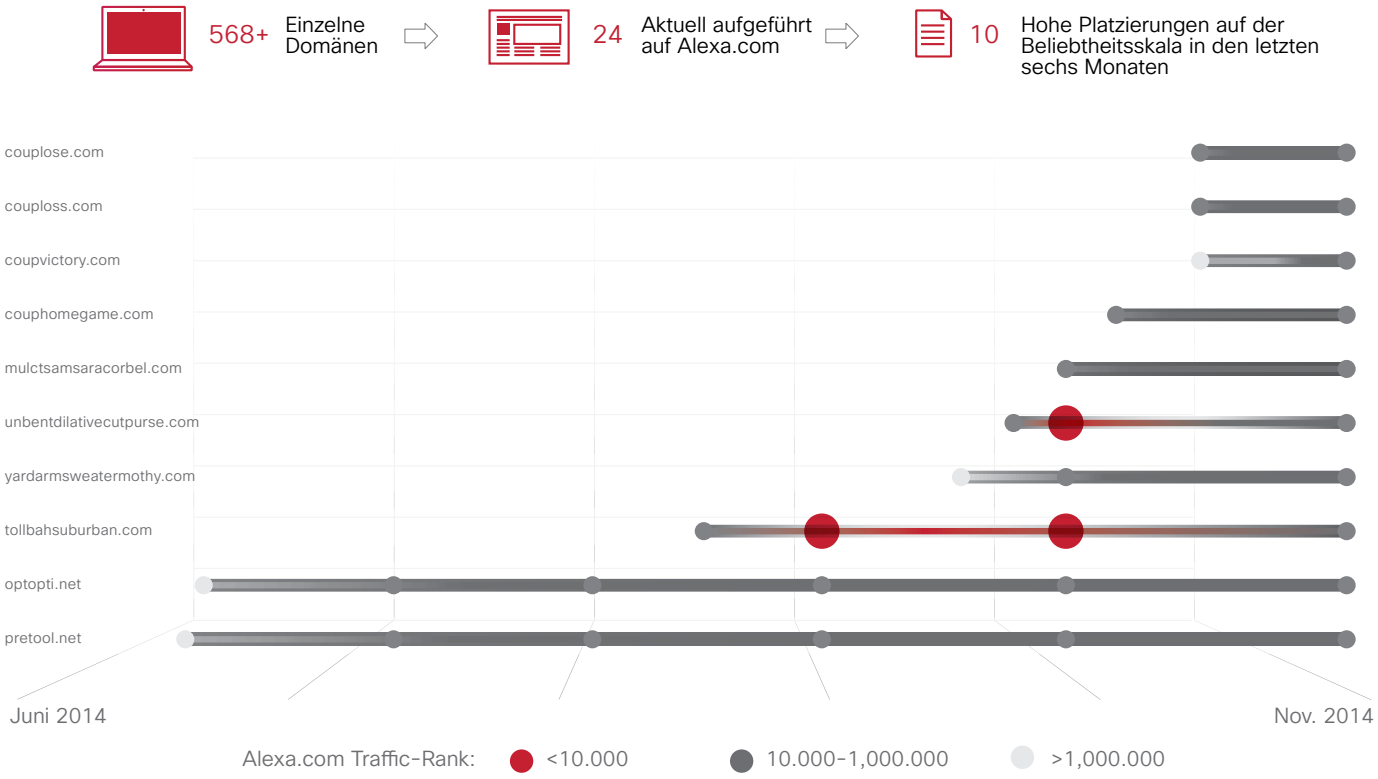
Einige der Domains sind seit mehr als einem Jahr aktiv, die meisten sind jedoch schon nach wenigen Wochen wieder offline (Abbildung 19). Alle haben jedoch gemeinsam, dass die Zahl der Aufrufe sehr schnell ansteigt.

Tipps zur Vorbeugung und Beseitigung

Um eine Kompromittierung durch Browser-Add-ons zu vermeiden oder eine bestehende Infektion zu beseitigen, sollten Benutzer Folgendes beachten:

- Anwendungen nur von vertrauenswürdigen Quellen herunterladen
- Unerwünschte Software aus Paketinstallationen entfernen
- Bedrohungsanalysen, Sandboxing- und Web-Security-Technologien verwenden, um diese Art von Bedrohung zu verhindern oder zu erkennen
- Add-ons nach Möglichkeit manuell entfernen; außerdem Anti-Spyware-Tools verwenden, um unerwünschte Programme zu entfernen

Abbildung 19: Für Browser-Add-ons verwendete Domains mit Alexa-Platzierung



Quelle: Cisco Security Research

2. Cisco Security Capabilities Benchmark Study

Cisco hat in neun Ländern Chief Information Security Officer (CISO) und Sicherheitsverantwortliche aus Unternehmen unterschiedlicher Größe zu ihren Sicherheitsressourcen und -verfahren befragt, um zu ermitteln, wie diese den aktuellen Sicherheitsstatus ihres Unternehmens einschätzen. Abgeschlossen im Oktober 2014, bietet die *Cisco Security Capabilities and Benchmark Study* Einblicke dazu, inwieweit die Sicherheitsstrategien und -prozesse heutiger Unternehmen den aktuellen Anforderungen entsprechen.

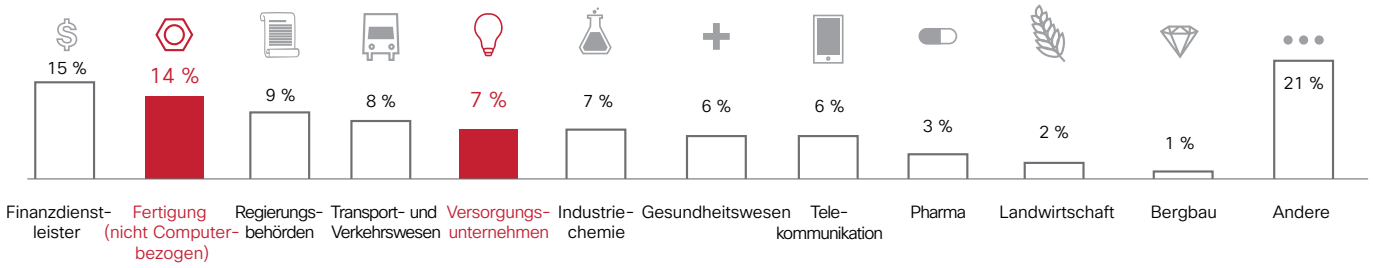
Können Unternehmen Schritt halten?

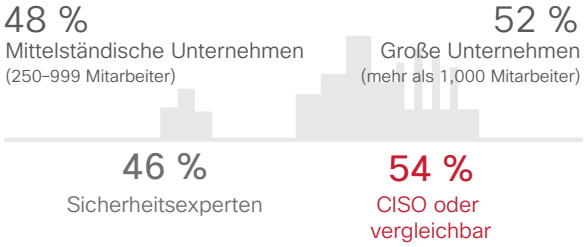
Wie schätzen Sicherheitsverantwortliche die Maßnahmen ihrer Unternehmen gegen Cyberangriffe ein? Aus der neuen Cisco Security Capabilities Benchmark Study geht hervor: Dies hängt davon ab, welche Rolle sie innerhalb des Unternehmens spielen und in welcher Branche sie tätig sind.

Abbildung 20 zeigt eine Auswertung der Antworten nach Branche und Unternehmensgröße. Hersteller aus computerfremden Bereichen sowie Energie- und Versorgungsunternehmen sind demnach in Sachen Sicherheit am besten aufgestellt.

N (Anzahl der Befragten) = 1.738

Abbildung 20: Teilnehmerprofil und Reaktionsfähigkeit





Quelle: *Cisco Security Capabilities Benchmark Study*

Im Rahmen der Studie sollten CISOs und Sicherheitsverantwortliche angeben, welche Ressourcen ihre Unternehmen im Bereich Cybersicherheit einsetzen. welche Sicherheitsverfahren zum Einsatz kommen und welche Sicherheitsrichtlinien bestehen. Auf Basis dieser Daten sollte ermittelt werden, inwieweit ihr Cybersecurity-Ansatz aktuelle Anforderungen erfüllen kann. Positiv ist festzuhalten, dass die Mehrheit der Befragten ihre Sicherheits-Tools und -Prozesse als effektiv bewerten. Allerdings: CISOs schätzen den Sicherheitsstatus ihrer Unternehmen deutlich optimistischer ein als ihre Kollegen in den Sicherheitsteams. So waren 62 Prozent der CISOs vollständig davon überzeugt, dass die Sicherheitsprozesse in ihren Unternehmen klar und hinreichend bekannt sind. Bei den Sicherheitsteams konnten dies nur 48 Prozent behaupten. CISOs sehen auch ihre Sicherheitsprozesse in einem besseren Licht. 59 Prozent der Befragten stimmten vollständig zu, dass diese Prozesse optimiert wurden und dass sie nun an weiteren Verbesserungen arbeiten. Diese Ansicht teilten lediglich 46 Prozent der Sicherheitsteams.

Wie kommt es zu dieser Diskrepanz? Eine plausible Erklärung ist, dass CISOs möglicherweise weniger in die täglichen Sicherheitsaktivitäten involviert sind, während Sicherheitsteams eng zusammenarbeiten, um sowohl ernsthafte als auch kleinere Sicherheitsvorfälle zu beheben. CISOs in sehr großen Unternehmen würden an einem typischen Arbeitstag möglicherweise nicht einmal etwas davon mitbekommen, wenn 1.000 Computer mit Malware infiziert wären. Die Sicherheitsteams dagegen wären eine ganze Zeit mit der Behebung des Problems beschäftigt – was sich in der Folge in einer weniger optimistischen Einschätzung der Unternehmenssicherheit niederschlüge.

CISOs legen zudem möglicherweise Richtlinien fest (z. B. für die Blockierung des Zugriffs auf Social Media), von denen sie glauben, sie schüfen eine starke, unüberwindbare Bedrohungsabwehr. Werden Kanäle wie diese jedoch vollständig geschlossen, fehlen Sicherheitsteams möglicherweise Kenntnisse und Erfahrungen zu den Bedrohungen, die direkt außerhalb ihres Netzwerks lauern.

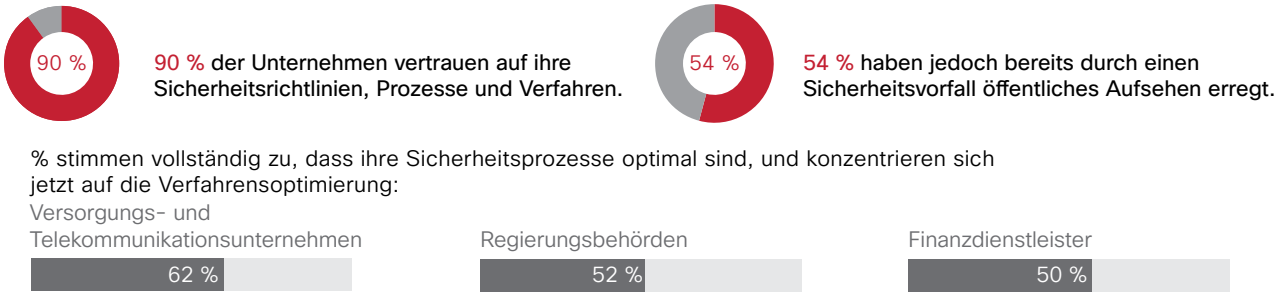
Eine weitere Diskrepanz war bei der Einschätzung der Befragten hinsichtlich der Sicherheitsrichtlinien ihrer Unternehmen festzustellen. So hielten CISOs ebenso wie Sicherheitsteams ihre Richtlinien für sehr effektiv (siehe Abbildung 21), von ihren Fähigkeiten zur Eindämmung von Kompromittierungen waren sie jedoch weniger überzeugt (siehe Abbildung 28).

Eine ähnliche Diskrepanz war hinsichtlich der Sicherheitskontrollen zu beobachten: Nahezu alle Befragten bewerteten ihre Sicherheitskontrollen als angemessen, ein Viertel von ihnen stufte ihre Sicherheitstools jedoch statt „sehr“ oder „äußerst“ lediglich als „einigermaßen“ effektiv ein. (siehe Abbildung 29).

Das Vertrauen in Sicherheitsprozesse und -verfahren scheint außerdem je nach Branche zu variieren. Besonders sicher fühlen sich demnach CISOs und Sicherheitsteams in Energie-, Versorgungs- und Telekommunikationsunternehmen, während Regierungsbehörden, Finanzdienstleister sowie Unternehmen aus Pharmaindustrie und Gesundheitswesen weniger zuversichtlich sind. So sind 62 Prozent der Sicherheitsverantwortlichen aus Telekommunikations- sowie Energie- und Versorgungsunternehmen absolut davon überzeugt, über optimierte Sicherheitsprozesse zu verfügen, bei Finanzdienstleistern sind es hingegen 50, bei Regierungsbehörden 52 Prozent.

Die Daten von Energie-, Versorgungs- und Telekommunikationsunternehmen deuten auf einen besonders fortschrittlichen Sicherheitsansatz hin, bei Regierungsbehörden und Finanzdienstleistern dagegen besteht hier noch Verbesserungspotenzial. Versorgungs- und Energieunternehmen nutzen tendenziell gut dokumentierte Verfahren zur Nachverfolgung von Sicherheitsvorfällen. Dies bedeutet jedoch nicht zwangsläufig, dass sie sicherer sind als Unternehmen anderer Branchen.

Abbildung 21: Wichtigste Erkenntnisse nach Branche und Position



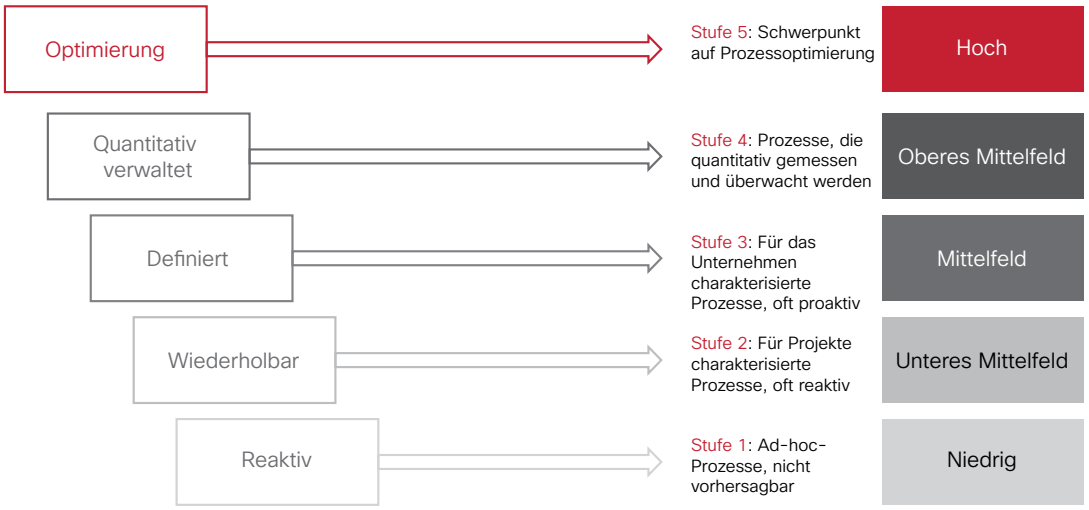
Zwischen großen und mittelständischen Unternehmen sind nur wenige Unterschiede festzustellen. Das deutet darauf hin, dass nur ein geringer Zusammenhang zwischen der Anzahl der Mitarbeiter und dem Sicherheitsniveau eines Unternehmens besteht.

Quelle: *Cisco Security Capabilities Benchmark Study*

Report teilen

Abbildung 22: Bewertungsgrundlage für den Sicherheitsansatz

Cisco untersuchte mehrere Optionen für Beispielsegmentierungen, bevor – basierend auf einer Reihe von Fragen zu den Sicherheitsprozessen – eine Lösung mit fünf Segmenten ausgewählt wurde. Diese Lösung deckt sich weitestgehend mit dem Capability Maturity Model Integration (CMMI).



Quelle: *Cisco Security Capabilities Benchmark Study*

Merkmale eines fortschrittlichen Sicherheitsansatzes

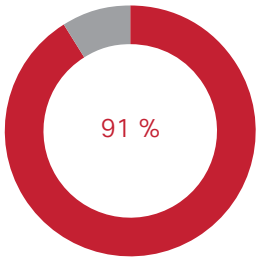
Aus der *Cisco Security Capabilities Benchmark Study* geht außerdem hervor, durch welche Merkmale sich Unternehmen mit einem fortschrittlichen Sicherheitsansatz von anderen unterscheiden. Diese umfassen:

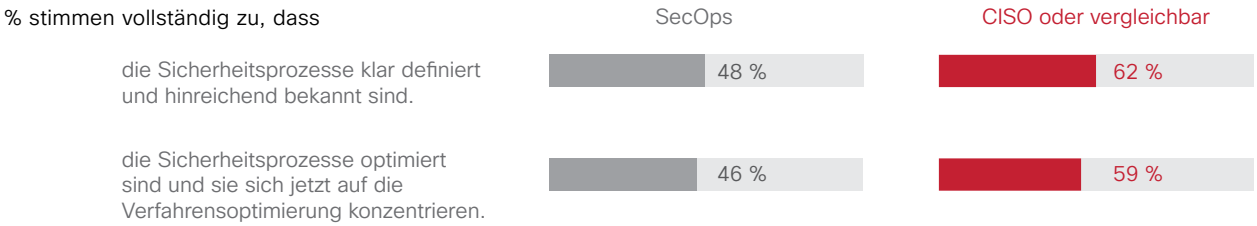
- Cybersicherheit ist ein zentrales Thema in der Unternehmensführung
- Klare, gut dokumentierte Richtlinien und Verfahren
- Integrierte Tools, die in Kombination einsetzbar sind

91 Prozent der Befragten aus Unternehmen mit einem fortschrittlichen Sicherheitsansatz stimmten vollständig zu, dass Cybersicherheit in der Unternehmensführung ein zentrales Thema ist. Dieser Aussage stimmten lediglich 22 Prozent der Befragten aus Unternehmen zu, die hierbei weniger gut abschnitten. Darüber hinaus sind 88 der Befragten aus Unternehmen mit einem fortschrittlichen Sicherheitsansatz davon überzeugt, dass ihre Sicherheitsprozesse klar und hinreichend bekannt sind. In weniger fortschrittlichen Unternehmen dagegen sind es 0 Prozent.

Abbildung 23: Wichtigste Erkenntnisse zum Sicherheitsmanagement in Unternehmen

91 % geben an, dass eine Führungskraft direkt mit der IT-Sicherheit betraut ist.
In der Regel handelt es sich dabei um einen CISO (29 %) oder einen CSO (24 %).





CISOs (und vergleichbar) sind im Hinblick auf den Sicherheitsstatus in ihrem Unternehmen optimistischer als Sicherheitsteams. Eine mögliche Erklärung hierfür ist, dass sie weniger in die alltäglichen Aufgaben eingebunden sind.

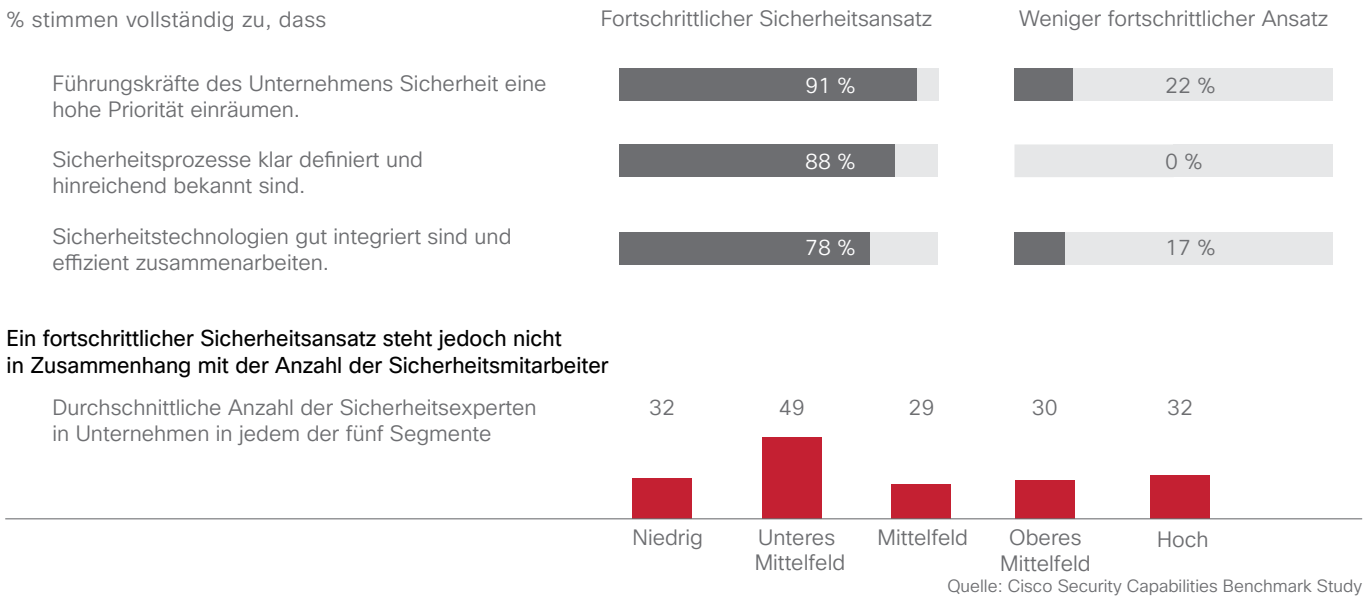
Quelle: *Cisco Security Capabilities Benchmark Study*

Abbildung 23 zeigt: Bei 91 Prozent der Befragten ist eine Führungskraft direkt mit dem Bereich Sicherheit betraut, in den meisten Fällen ein CISO oder Chief Security Officer (CSO). Die hohe Anzahl an Unternehmen mit einem Sicherheitsbeauftragten macht Mut: Gibt es keinen Sicherheitsverantwortlichen, sind die Prozesse meist unzureichend definiert, und sie werden nicht ausreichend kommuniziert und umgesetzt. Wahrscheinlich haben die schwerwiegenden Sicherheitslücken in jüngster Vergangenheit die Unternehmen wach gerüttelt, und sie räumen dem Sicherheitsmanagement deshalb mehr Platz in ihren Führungsebenen ein.

78 % der Befragten aus Unternehmen mit einem fortschrittlichen Sicherheitsansatz stimmten vollständig zu, dass Sicherheitstechnologien gut integriert sind und effektiv zusammenarbeiten, bei den Befragten fortschrittlichen Unternehmen waren es nur 17 %.

Um ihren Sicherheitsansatz zu optimieren, müssen sich Unternehmen allerdings nicht unbedingt nach neuen Sicherheitsfachleuten umsehen. Denn in weniger gut aufgestellten Unternehmen sind genauso wie in solchen mit einem fortschrittlichen Sicherheitsansatz im Schnitt 32 Sicherheitsexperten im Einsatz. Die Einstellung neuer Fachkräfte hat somit nicht automatisch eine Optimierung des Sicherheitsmanagements zur Folge. Vielmehr gilt es, ein optimales Verhältnis zwischen Sicherheitspersonal und der Gesamtzahl der Mitarbeiter zu finden.

Abbildung 24: Priorität von Cybersicherheit in Unternehmen



Quelle: Cisco Security Capabilities Benchmark Study

Abbildung 24 zeigt: Unternehmen mit einem weniger fortschrillichen Sicherheitsansatz räumen dem Thema Cybersicherheit weder eine hohe Priorität ein, noch sind ihre Sicherheitsprozesse klar definiert und hinreichend bekannt.

Der Landesvergleich zeigt ein positives Ergebnis: In jedem Segment sind die Unternehmen mit einem fortschrittlichen Sicherheitsansatz in der Mehrzahl. In einigen Ländern sind die Befragten jedoch mehr von der Zuverlässigkeit der eigenen Sicherheitsmechanismen überzeugt als unabhängige Außenstehende. Zurückzuführen ist diese übermäßig positive Einschätzung unter Umständen auf ein kulturell verortetes Bedürfnis, sich selbst – und damit das eigene Unternehmen – in einem möglichst vorteilhaften Licht darzustellen.

Vorsicht vor Selbstüberschätzung

CISOs und Sicherheitsteams vertrauen auf ihre Sicherheitskonzepte. Gleichzeitig geben sie aber an, dass sie keine Standardtools verwenden, um Sicherheitsverletzungen vorzubeugen. Weniger als 50 % der Befragten verwenden folgende Tools:

- Identity-Administration oder User-Provisioning
- Patching und Konfigurationsmanagement
- Penetrationstests
- Endpunktforensik
- Schwachstellen-Scans

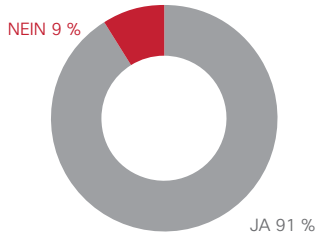
Ressourcen für Unternehmenssicherheit

Abbildung 25: Anzahl der Sicherheitsexperten

In Unternehmen sind im Schnitt 123 Sicherheitsexperten beschäftigt, in Regierungsbehörden wird dieser Bereich tendenziell eher ausgelagert.

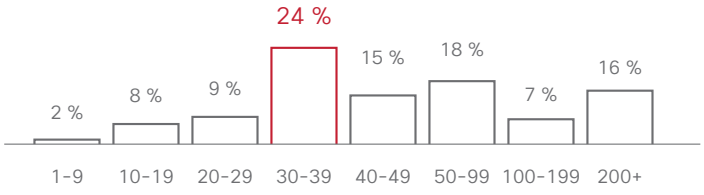
Überblick über die Sicherheitsressourcen

Gibt es in Ihrem Unternehmen ein Incident-Response-Team?



Durchschnittliche größe des Sicherheitsteams

Durchschnittlicher Anteil der Zeit in Prozent, der für Sicherheitsaufgaben aufgewendet wird



Anzahl der Sicherheitsexperten

In Regierungsbehörden werden tendenziell mehr Sicherheitsdienste ausgelagert als in anderen Branchen.

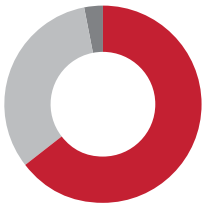
Quelle: *Cisco Security Capabilities Benchmark Study*

Abbildung 26: Eingesetzte Sicherheitstechnologien

Etwa zwei Drittel der Befragten gaben an, dass ihre Sicherheitstechnologien auf dem neuesten Stand sind und häufig aktualisiert werden.

Wie würden Sie Ihre Sicherheitsinfrastruktur beschreiben?

Basis: n=1.738



64 %	Unsere Sicherheitsinfrastruktur ist immer auf dem neuesten Stand und wird laufend durch die leistungsfähigsten am Markt verfügbaren Technologien aktualisiert.
33 %	Wir erneuern oder aktualisieren unsere Sicherheitstechnologien regelmäßig, haben derzeit jedoch nicht die aktuellsten und leistungsfähigsten am Markt verfügbaren Tools im Einsatz.
3 %	Wir erneuern oder aktualisieren unsere Sicherheitstechnologien nur, wenn die bestehenden ihren Zweck nicht mehr erfüllen/veraltet sind oder wenn neue Anforderungen ein Upgrade erfordern.

Im Vergleich zu Sicherheitsteams (57 %) geben wesentlich mehr CISOs (70 %) an, dass die Infrastruktur ihres Unternehmens auf dem neuesten Stand ist.

Telekommunikationsunternehmen geben am häufigsten an, dass ihre Sicherheitsinfrastruktur stets auf dem neuesten Stand ist.

Quelle: *Cisco Security Capabilities Benchmark Study*

Abbildung 27: Maßnahmen zum Schutz vor Bedrohungen

Zum Schutz vor Bedrohungen haben Unternehmen im Jahr 2014 folgende Maßnahmen implementiert.

	Eingesetzte Maßnahmen zum Schutz vor Bedrohungen		Schutz, der über Cloud-basierte Services verwaltet wird	
	Sicherheitsexperten n=797	CISO n=941	Sicherheitsexperten n=797	CISO n=887
Netzwerksicherheit, Firewalls/Intrusion Prevention	57 %	64 %	30 %	39 %
Web-Sicherheit	56 %	62 %	33 %	41 %
E-Mail-/Messaging-Sicherheit	53 %	58 %	33 %	41 %
Schutz vor Datenverlust	55 %	55 %	-	-
Verschlüsselung/Datenschutz	52 %	55 %	-	-
Zugangskontrolle/Autorisierung	55 %	52 %	24 %	24 %
Authentifizierung	54 %	51 %	24 %	22 %
Mobile Sicherheit	48 %	54 %	24 %	32 %
Sicherer Wireless-Zugriff	47 %	52 %	22 %	30 %
Endgeräteschutz/Anti-Malware	45 %	52 %	24 %	27 %
Schwachstellen-Scans	44 %	51 %	24 %	26 %
VPN	49 %	46 %	25 %	27 %
Identity-Administration/User-Provisioning	43 %	47 %	16 %	23 %
Management von Sicherheitsinformationen und -vorfällen (Security Information and Event Management, SIEM)	39 %	46 %	-	-
Netzwerkforensik	41 %	43 %	-	-
Patching und Konfigurationsmanagement	38 %	40 %	-	-
Penetrationstests	39 %	37 %	20 %	19 %
DDoS-Verteidigung	35 %	37 %	-	-
Endpunktforensik	29 %	33 %	-	-

Befragte, die Bedrohungsschutz verwenden; n = 1.646

13 Prozent der Befragten gaben an, dass keine Cloud-basierten Sicherheitslösungen zum Einsatz kommen. Dies gilt insbesondere für Befragte in den Bereichen Gesundheitswesen, Finanzdienstleistungen und Pharmaindustrie.

Quelle: *Cisco Security Capabilities Benchmark Study*

Sicherheitsrichtlinien und -verfahren

Abbildung 28: Selbsteinschätzung der Effektivität von Sicherheitsrichtlinien und der Fähigkeit zur Eindämmung von Kompromittierungen

Unternehmen halten ihre Sicherheitsrichtlinien für effektiv, von ihren Fähigkeiten zur Eindämmung von Kompromittierungen sind sie jedoch deutlich weniger überzeugt.

Selbsteinschätzung der Effektivität von Sicherheitsrichtlinien

Sicherheitsrichtlinien n=1.738	Sicherheitsexperten n=797			CISO n=941		
	Stimme nicht zu/Stimme zu/ Stimme vollständig zu			Stimme nicht zu/Stimme zu/ Stimme vollständig zu		
Informationen werden inventarisiert und nach einem eindeutigen Verfahren klassifiziert.	11 %	40 %	49 %	4 %	38 %	58 %
Wir haben hervorragende Maßnahmen für die Mitarbeitersicherheit implementiert.	9 %	45 %	46 %	4 %	36 %	60 %
Unsere Computersysteme sind gut geschützt.	10 %	39 %	51 %	4 %	34 %	62 %
Die Sicherheitskontrollen in unseren Systemen und Netzwerken werden effektiv verwaltet.	6 %	41 %	53 %	3 %	31 %	66 %
Zugriffsrechte auf Netzwerke, Systeme, Anwendungen, Funktionen und Daten werden angemessen überwacht.	8 %	35 %	57 %	4 %	32 %	64 %
Wir integrieren Sicherheit gut in Systeme und Anwendungen.	10 %	38 %	52 %	4 %	32 %	64 %
Wir integrieren Sicherheit gut in unsere Verfahren zur Beschaffung, Entwicklung und Wartung von Systemen.	9 %	41 %	50 %	4 %	35 %	61 %

Selbsteinschätzung der Fähigkeit zur Eindämmung von Kompromittierungen

Sicherheitsimplementierung n=1.738	Sicherheitsexperten n=797			CISO n=941		
	Stimme nicht zu/Stimme zu/ Stimme vollständig zu			Stimme nicht zu/Stimme zu/ Stimme vollständig zu		
Wir prüfen und verbessern unsere Sicherheitsvorkehrungen regelmäßig, formell und strategisch.	7 %	42 %	51 %	3 %	36 %	61 %
Wir verfügen über Tools, mit denen wir die Funktionen unserer Sicherheitsvorkehrungen prüfen und Feedback geben können.	10 %	41 %	49 %	4 %	39 %	57 %
Alle Sicherheitsvorfälle werden bei uns systematisch untersucht.	11 %	40 %	49 %	3 %	37 %	60 %
Falls erforderlich können wir Sicherheitskontrollen für wertvolle Ressourcen erhöhen.	10 %	43 %	47 %	3 %	38 %	59 %
Wir prüfen regelmäßig die Verbindungsaktivität im Netzwerk, um sicherzustellen, dass die Sicherheitsmaßnahmen wie gewünscht funktionieren.	8 %	39 %	53 %	4 %	33 %	63 %
Unsere Funktionen zur Erkennung und Blockierung von Angriffen sind stets auf dem neuesten Stand.	9 %	38 %	53 %	3 %	36 %	61 %
Unsere Sicherheitstechnologien sind gut integriert und arbeiten effizient zusammen.	9 %	40 %	51 %	3 %	37 %	60 %
Sicherheit ist gut in die Ziele unseres Unternehmens und unsere Geschäftsprozesse integriert.	10 %	39 %	51 %	2 %	34 %	64 %
Der Umfang einer Kompromittierung lässt sich leicht ermitteln und eingrenzen, und Exploits lassen sich beseitigen.	15 %	44 %	41 %	8 %	42 %	50 %

Im Vergleich zu Befragten aus großen Unternehmen stimmen mehr Befragte aus mittelständischen Unternehmen vollständig zu, dass sie ihre „Sicherheitsvorkehrungen regelmäßig, formell und strategisch prüfen und verbessern“.

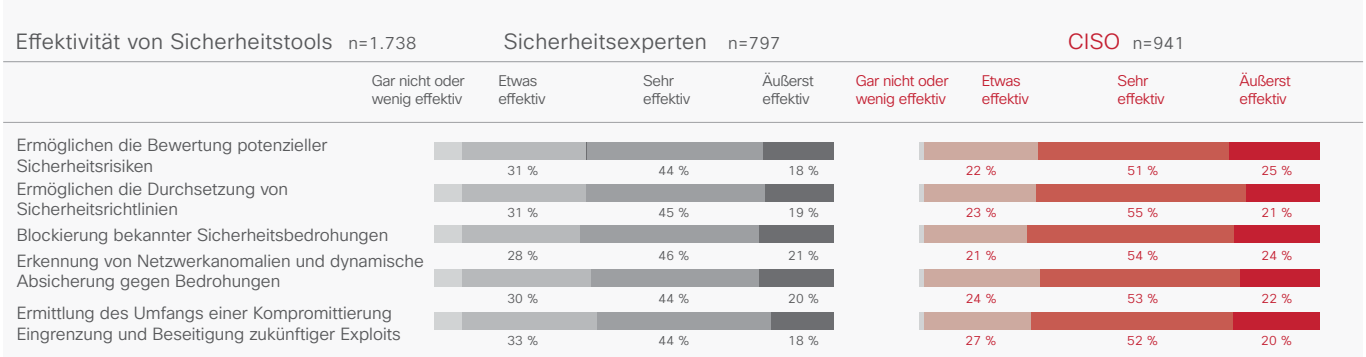
Quelle: *Cisco Security Capabilities Benchmark Study*

Abbildung 29: Bewertung der Sicherheitskontrollen und Sicherheitstools

Sicherheitsverantwortliche bewerten ihre Sicherheitskontrollen als angemessen, ein Viertel von ihnen stuft ihre Sicherheitstools jedoch nur als „einigermaßen effektiv“ ein.

Sicherheitskontrollen n=1.738	Sicherheitsexperten n=797			CISO n=941		
	Stimme nicht zu/Stimme zu/ Stimme vollständig zu			Stimme nicht zu/Stimme zu/ Stimme vollständig zu		
Wir wenden ein standardisiertes Incident-Response-Verfahren an, z. B. RFC2350, ISO/IEC 27035:2011 oder U.S.-Zertifizierung.	15 %	42 %	43 %	6 %	40 %	54 %
Wir verfügen über effiziente Prozesse zur Auswertung und Priorisierung von eingehenden Berichten über Vorfälle und deren Analyse.	11 %	46 %	43 %	4 %	39 %	57 %
Mit unseren Systemen lässt sich leicht feststellen, ob Sicherheitsvorfälle tatsächlich aufgetreten sind.	11 %	41 %	48 %	4 %	36 %	60 %
Wir verfügen über ein leistungsfähiges System zur Kategorisierung von Informationen zu Vorfällen.	10 %	43 %	47 %	4 %	37 %	59 %
Wir sorgen für eine effektive Kommunikation und Zusammenarbeit im Hinblick auf Sicherheitsvorfälle.	10 %	46 %	44 %	3 %	40 %	57 %
Wir verfügen über sorgfältig dokumentierte Prozesse und Verfahren zur Reaktion auf und Nachverfolgung von Vorfällen.	9 %	40 %	51 %	4 %	35 %	61 %
Risikoanalysen für die IT-Sicherheit sind standardmäßig in unseren gesamten Risikoanalyseprozess integriert.	10 %	37 %	53 %	4 %	36 %	60 %

Deutlich mehr Befragte aus Versorgungsunternehmen stimmen vollständig zu, dass sie über sorgfältig dokumentierte Incident-Response-Prozesse verfügben als die Vertreter der meisten anderen Branchen.



Sicherheitsverantwortliche im Transportwesen sind im Hinblick auf die Möglichkeiten ihrer Unternehmen, bekannte Sicherheitsbedrohungen zu erkennen und abzuwehren, eher pessimistisch.

Quelle: *Cisco Security Capabilities Benchmark Study*

Report teilen

Abbildung 30: Verfahren zur Analyse kompromittierter Systeme und zur Ursachenbeseitigung nach Sicherheitsvorfällen

Sicherheitsverantwortliche verwenden zur Analyse von kompromittierten Systemen am häufigsten Firewall-Protokolle. Diese liefern jedoch nur begrenzt Daten und keinen Kontext. Eine umfassendere Analyse ermöglicht die regelmäßige Nutzung von IDS- und IPS-Protokollen, Proxy- und Host-basierten Intrusion-Prevention-Systemen (HIPS), Anwendungsprotokollen und NetFlow.

Überraschend war auch, dass die korrelierte Ereignis-/Protokollanalyse nur selten als Tool zur Analyse von kompromittierten Systemen genutzt wurde. Dies bedeutet möglicherweise, dass die Befragten Daten oder die Quellen von Daten nicht miteinander korrelieren, was jedoch eine detailliertere Analyse von Sicherheitsvorfällen ermöglicht.

Prozesse zur Analyse von kompromittierten Systemen	Sicherheitsexperten	CISO
	n=797	n=941
Firewall-Protokoll	59 %	62 %
Systemprotokollanalysen	58 %	60 %
Analyse der Malware- oder Dateiregression	51 %	58 %
Analyse der Netzwerkstatistik	51 %	54 %
Analyse der Registry	48 %	51 %
Vollständige Paketerfassungsanalyse	44 %	48 %
Korellierte Analyse von Ereignissen/Protokollen	40 %	44 %
Speicherforensik	39 %	43 %
Festplattenforensik	38 %	41 %
Erkennung von Indicators of Compromise (IoC)	38 %	38 %
Externe Teams [oder Drittanbieter] zur Reaktion auf/Analyse von Vorfällen	36 %	38 %

Befragte Mitarbeiter aus Regierungsbehörden verwenden tendenziell mehr Prozesse zur Analyse kompromittierter Systeme als Befragte der meisten anderen Branchen.

Verfahren zur Beseitigung der Ursachen von Sicherheitsvorfällen	Sicherheitsexperten	CISO
	n=797	n=941
Quarantäne oder Entfernen der schädlichen Anwendung	55 %	60 %
Ursachenanalyse	55 %	56 %
Unterbinden der Kommunikation von bösartiger Software	51 %	55 %
Zusätzliche Überwachung	51 %	53 %
Anpassung von Richtlinien	50 %	51 %
Unterbinden der Kommunikation der angegriffenen Anwendung	47 %	49 %
Maßnahmen zur langfristigen Absicherung gegen ein Problem	46 %	48 %
Wiederherstellung des Systems auf vorherigen Zustand	43 %	47 %

Mit Ausnahme der Kategorie „Unterbinden der Kommunikation von bösartiger Software“ decken sich die Antworten von CISOs und Sicherheitsteams weitestgehend.

Quelle: *Cisco Security Capabilities Benchmark Study*

Abbildung 31: Angaben von CISOs und Sicherheitsteams zu Kontrollmaßnahmen nach Sicherheitsvorfällen

CISOs gaben häufiger als Sicherheitsexperten an, dass nach Sicherheitsvorfällen zusätzliche Kontrollen implementiert wurden.

Prozesse zur Wiederherstellung betroffener Systeme	Sicherheitsexperten	CISO
	n=797	n=941
Implementierung zuätzlicher/neuer Erkennungsmethoden und Kontrollen nach einem Vorfall als Reaktion auf ermittelte Schwachstellen	55 %	65 %
Patching und Aktualisierung von Anwendungen, die als angreifbar eingestuft wurden	59 %	60 %
Systemwiederherstellung anhand eines Backups	53 %	60 %
Differenzierende Wiederherstellung	53 %	58 %
Gold Image-Wiederherstellung	33 %	36 %

Bei den Befragten aus Telekommunikations- und Versorgungsunternehmen kommt die Gold-Image-Wiederherstellung häufiger zum Einsatz als bei den Vertretern anderer Branchen.

Abbildung 32: Wer wird bei Sicherheitsvorfällen benachrichtigt?

Üblicherweise bestehen formelle Prozesse, bei denen Betriebspersonal und Technologiepartner über Sicherheitsvorfälle informiert werden.

Gruppen, die bei einem Vorfall benachrichtigt werden	Sicherheitsexperten	CISO
	n=797	n=941
Betriebspersonal	44 %	48 %
Technologiepartner	42 %	47 %
Entwicklung/Technik	38 %	37 %
Personalabteilung	37 %	35 %
Rechtsabteilung	37 %	35 %
Alle Mitarbeiter	38 %	33 %
Produktion	31 %	36 %
Geschäftspartner	31 %	33 %
Marketing	30 %	31 %
Public Relations	30 %	27 %
Externe Parteien	25 %	20 %

Regierungsbehörden verfügen deutlich häufiger über klar definierte Benachrichtigungsprozesse mit mehreren Gruppen als andere Branchen.

Quelle: *Cisco Security Capabilities Benchmark Study*

Bewertung des Sicherheitsansatzes

Abbildung 33: Niveau von Sicherheitsprozessen

Die meisten Unternehmen verfügen über fortschrittliche Sicherheitsprofile. Dies gilt über alle Länder (Abbildung 34) und Branchen hinweg (Abbildung 35).

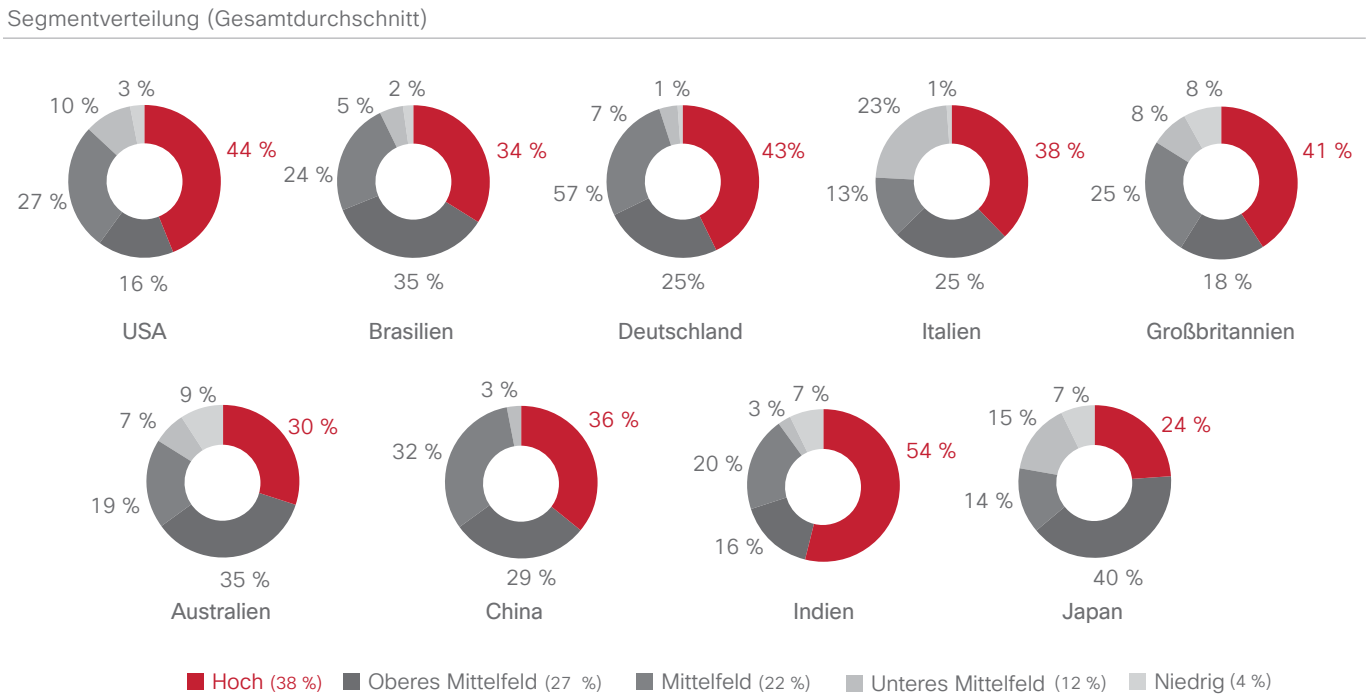
Die hohe Priorität von IT-Sicherheit in der Mehrzahl der Unternehmen und die in der Folge implementierten Prozesse und Verfahren zeigen eine Tendenz hin zu fortschritttlichen Sicherheitsprofilen.

Segmentverteilung

Hoch	39 %
Oberes Mittelfeld	23 %
Mittelfeld	26 %
Unteres Mittelfeld	8 %
Niedrig	4 %

Quelle: *Cisco Security Capabilities Benchmark Study*

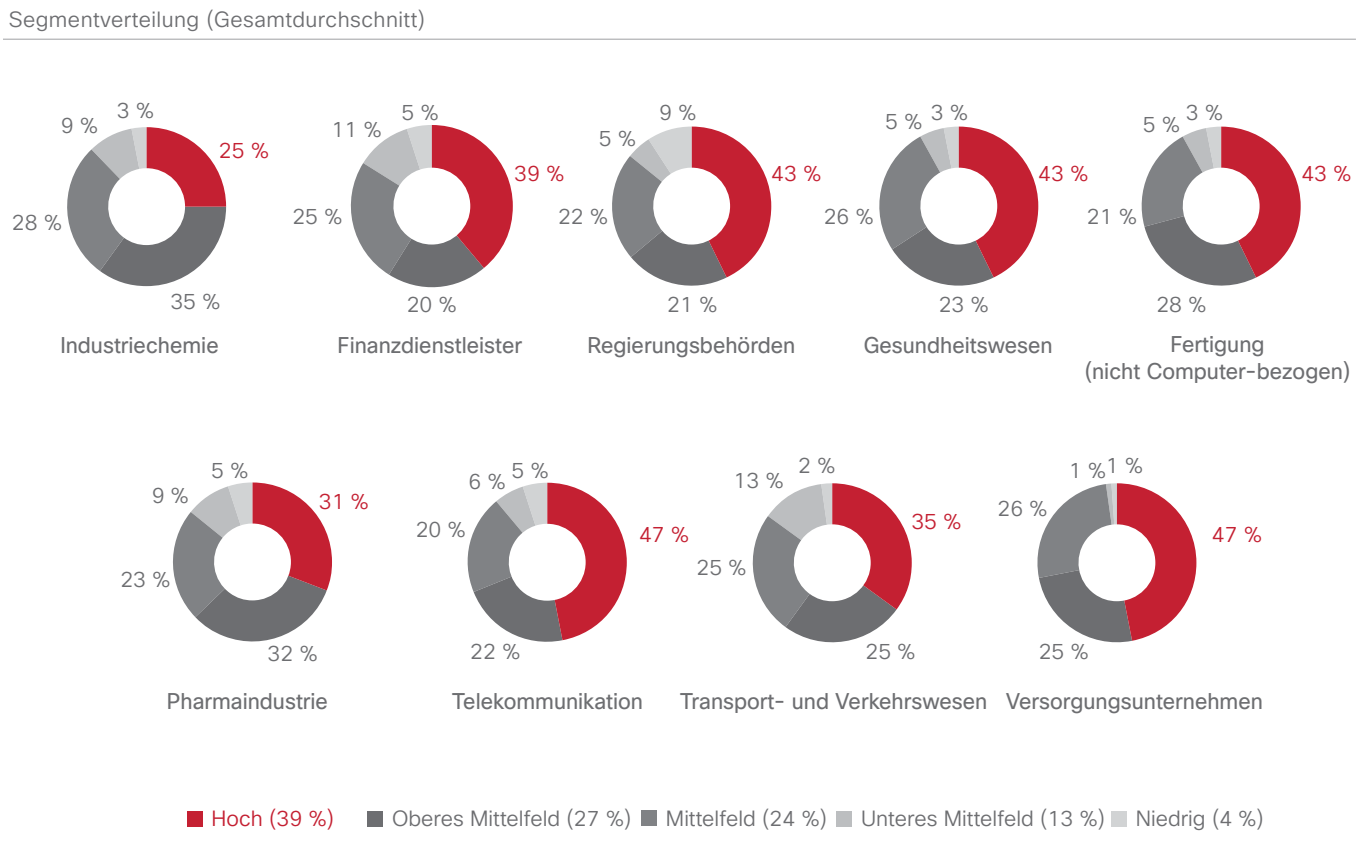
Abbildung 34: Niveau von Sicherheitsprozessen nach Land



Quelle: *Cisco Security Capabilities Benchmark Study*

Abbildung 35: Niveau von Sicherheitsprozessen nach Branche

Fast die Hälfte der Telekommunikations-, Versorgungs- und Energieunternehmen erzielen ein hohes Sicherheitsniveau.



Quelle: *Cisco Security Capabilities Benchmark Study*

Mittelstand in Sachen Sicherheit gut aufgestellt

Von sehr großen Unternehmen wird ein erfolgreiches Sicherheitsmanagement erwartet, da ihnen die meisten Ressourcen zur Verfügung stehen: das Budget zum Kauf der neuesten Technologie und hochqualifizierte Mitarbeiter, die sie verwalten. Man könnte annehmen, dass größere mittelständische Unternehmen (in der Studie definiert als Unternehmen mit 500 bis 999 Mitarbeitern) schlechter auf Sicherheitsvorfälle reagieren können als Großunternehmen (1000 oder mehr Mitarbeiter). Die *Cisco Security Capabilities Benchmark Study* zeigt jedoch: Mittelständische Unternehmen liegen beim Thema Sicherheit in vielen Bereichen nicht nur mit großen Unternehmen gleichauf, sie übertreffen diese sogar oftmals. Dies liegt möglicherweise an der höheren Flexibilität dieser Unternehmen.

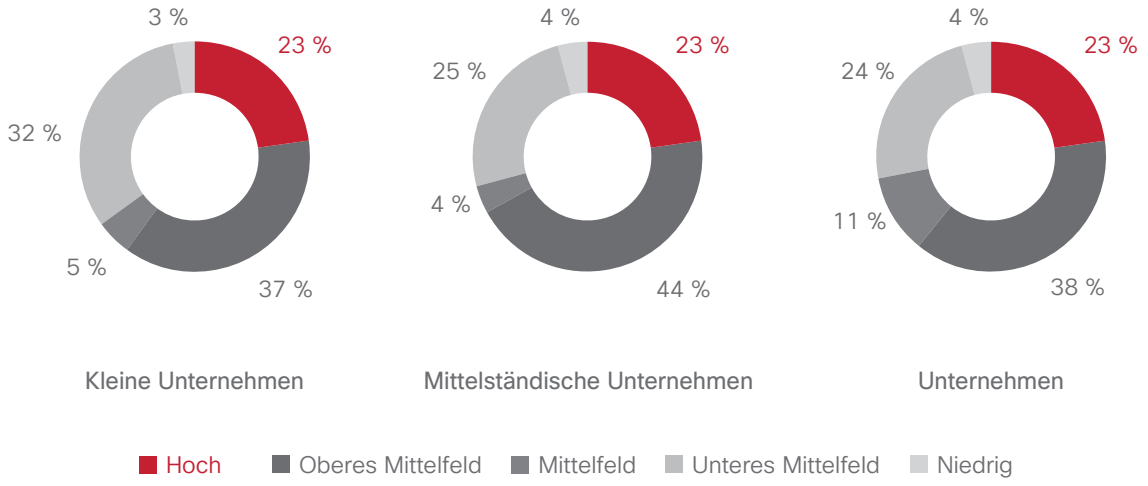
Tatsächlich weisen größere mittelständische Unternehmen der Studie zufolge sogar häufiger einen starken Sicherheitsansatz auf. Wie in Abbildung 36 dargestellt, erreichen größere mittelständische Unternehmen im Gegensatz zu kleineren mittelständischen (250–499 Mitarbeiter) und großen Unternehmen (1000 oder mehr Mitarbeiter) deutlich häufiger ein hohes Sicherheitsniveau.

Äußerst positiv zu bewerten ist auch, dass mittelständische Unternehmen ähnlich hohe Werte erzielen wie Großunternehmen, da gerade der Mittelstand dazu beiträgt, dass sich die Wirtschaft wieder erholt.

Wichtigste Erkenntnisse zum Sicherheitsniveau in mittelständischen Unternehmen:

- Bei 92 Prozent der mittelständischen Unternehmen ist ein internes Team für die Behebung on Sicherheitsvorfällen im Einsatz, bei großen Unternehmen sind es 93 Prozent.
- Bei 94 Prozent der mittelständischen Unternehmen ist eine Führungskraft direkt mit dem Bereich Sicherheit betraut, bei größeren Unternehmen sind es 92 Prozent.

Abbildung 36: Sicherheitsniveau von großen mittelständischen Unternehmen



Die hohe Priorität von IT-Sicherheit in der Mehrzahl der Unternehmen und die in der Folge implementierten Prozesse und Verfahren zeigen eine Ter hin zu fortschrittlichen Sicherheitsprofilen.

In die hohen Stufen und das obere Mittelfeld fallen deutlich mehr mittelständische Unternehmen als kleine und große Unternehmen.

Mindestens 60 Prozent verfügen über fortschrittliche Sicherheitsprofile.

Quelle: *Cisco Security Capabilities Benchmark Study*

3. Geopolitische und Branchentrends

Die Experten von Cisco beobachten laufend die globalen Entwicklungen und stellen dabei aktuelle geopolitische Trends heraus, die Unternehmen – insbesondere multinationale Konzerne – im Auge behalten sollten. Ebenfalls untersucht werden zudem aktuelle globale Entwicklungen in den Bereichen Datensouveränität, Datenlokalisierung, Verschlüsselung und Datenkompatibilität.

Schwache staatliche Strukturen – idealer Nährboden für Cyberkriminalität

CISOs und andere Sicherheitsverantwortliche – insbesondere solche, die in multinationalen Unternehmen tätig sind – sollten geopolitische Dynamiken stets genau beobachten, denn diese können direkte Auswirkungen auf globale Lieferketten haben und zudem neue Anforderungen beim Umgang mit Kunden- und Mitarbeiterdaten in verschiedenen Ländern bedeuten. Möglich ist auch, dass zusätzliche Kosten durch veränderte gesetzliche oder regulatorische Bestimmungen entstehen, Geschäftsgeheimnisse besser vor Diebstahl geschützt oder neue Risiken für ausländische Niederlassungen oder den Ruf des Unternehmens kalkuliert werden müssen.

Cyberkriminalität floriert überall auf der Welt, insbesondere in Regionen mit schwachen staatlichen Strukturen. Ein Beispiel hierfür ist Osteuropa, das schon seit langem eine Brutstätte von organisiertem Verbrechen ist. In Regionen mit schwachen staatlichen Strukturen gibt es nicht selten Anzeichen für enge Verstrickungen der nationalen Nachrichtendienste mit organisierten Gruppen von Cyberkriminellen.

Einige der jüngst bekannt gewordenen Cyberangriffe in den USA sollen US-Behörden zufolge ebenfalls von diesen Regionen ausgegangen sein. Hinter einigen der Angriffe schienen dabei nicht finanzielle Interessen zu stehen, sondern das Abschöpfen von Informationen und die Infiltrierung von Infrastruktur aus politisch motivierten Gründen.[7] Dies ist ein Indiz dafür, dass die Hintermänner aus Regierungskreisen stammten und/oder dass die Aktionen von organisierten Verbrecherbanden ausgingen.

Immer mehr Regierungen richten Gesetzgebung und Bestimmungen mittlerweile darauf aus, den Cyber-Raum besser unter Kontrolle zu bekommen. China zum Beispiel: Unter dem Leitthema der Rechtsstaatlichkeit wurde auf der vierten Plenartagung des 18. Kongresses der kommunistischen Partei Chinas[8] beschlossen, Korruption zu bekämpfen und gesetzeskonformes Handeln in Wirtschaft und Verwaltung stärker zu kontrollieren. Diese Beschlüsse könnten dazu beitragen, nationale und internationale Bemühungen zum Aufspüren von Cyberkriminellen zu stärken und es ihnen zu erschweren, sich zu verstecken.

Internetnutzung durch Terrororganisationen

Die Entstehung transnationaler Terrororganisationen wie dem Islamischen Staat (auch bekannt als ISIS oder IS) müssen im Hinblick auf geopolitische Trends ebenfalls genau beobachtet werden. Cyberkriminalität scheint bei Organisationen wie ISIS zwar keine Rolle zu spielen. Für die Rekrutierung neuer Mitglieder sind sie jedoch stark auf das Internet, insbesondere soziale Medien, angewiesen. Derzeit scheint es, als seien die klassischen Methoden zur Geldbeschaffung wie Erpressung, Menschenhandel und Ölverkäufe noch einträglich genug für transnationale Terrororganisationen. Mit zunehmender Größe könnten sie jedoch auch Cyberkriminalität dazu nutzen, ihre weltweiten Aktivitäten zu finanzieren. Nicht auszuschließen ist außerdem, dass neue terroristische Gruppierungen, die weniger stark aufgestellt sind wie etablierte Vereinigungen, Cyberkriminalität als Möglichkeit zum schnellen Wachstum entdecken.

Im Blog-Beitrag „Cupcakes and Cyberespionage“ stellt Cisco einen neuen Ansatz zur Abwehr von Cyberspionage vor.

Das Dilemma von Datensouveränität, Datenlokalisierung und Verschlüsselung

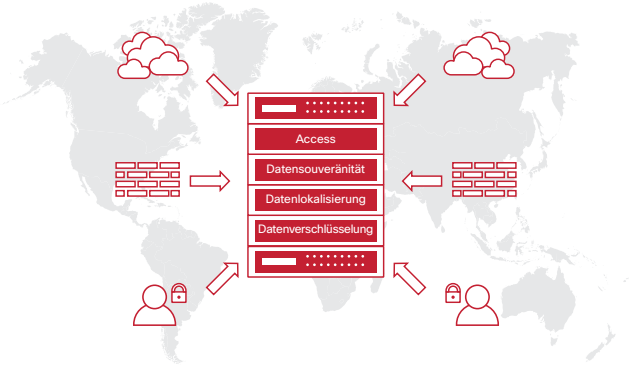
Edward Snowdens Anschuldigungen an die US-Regierung, den Kommunikations- und Datenverkehr bis über die Grenzen des Landes hinaus zu überwachen, sowie Themen wie Datensouveränität (Daten unterliegen der Rechtsprechung des Landes, in dem sie sich befinden; ausländische Regierungen oder Gerichte, die versuchen, sich Zugriff darauf zu verschaffen, haben keinerlei Handhabe) und Datenlokalisierung (per Gesetz vorgeschriebener Speicherort von Daten) werden heute heiß debattiert.

Einige Länder arbeiten bereits an Initiativen in Richtung Datenlokalisierung, um die Daten ihrer Bürger vor dem Zugriff durch ausländische Regierungen zu schützen. So soll per Gesetz festgelegt werden, dass Daten im eigenen Land gespeichert oder über bestimmte Wege umgeleitet werden müssen, oder dass Unternehmen ausschließlich Hardware von Herstellern aus dem eigenen Land verwenden dürfen.

Ein Beispiel hierfür ist Brasilien: Erst vor Kurzem hat das Land ein neues Gesetz verabschiedet, das „Datenschutzvorgaben enthält, die weitreichende Einschränkungen bei der Weitergabe der persönlichen Informationen, Kommunikation und Online-Protokolldaten der Benutzer für [betroffene] Unternehmen vorsehen."[9] Und auch Russland ändert seine Gesetze für Datenschutz und Informationssicherheit: Persönliche Daten russischer Staatsbürger (einschließlich Internetdaten) dürfen künftig nur noch auf Servern und Datenbanken innerhalb Russlands gespeichert werden. 2015 soll das Gesetz in Kraft treten.[10]

Aus Sicht multinationaler Unternehmen können gesetzliche Vorschriften zur Datenlokalisierung problematisch werden, wenn die Gesetze der einzelnen Länder miteinander in Konflikt stehen. Die Einhaltung der Vorschriften zur Generierung, Speicherung und Vernichtung von Daten im einen Land würde dann möglicherweise gegen die Gesetze eines anderen Landes verstoßen.

Abbildung 37: Das Dilemma von Datensouveränität, Lokalisierung und Verschlüsselung



Gesetzlich vorgeschriebene Datenlokalisierung kann außerdem bedeuten, dass ein grenzübergreifender Datenfluss nur noch eingeschränkt möglich ist und in der Folge Unklarheiten in der Abstimmung entstehen und die Netzwerkadministration erheblich erschwert wird. Ein weiterer Aspekt ist die Lieferkette: Hier kommen zunehmend Cloud-basierte Technologien zum Einsatz, die ein globales Partnernetzwerk miteinander verbinden. Ein solcher Datenaustausch zwischen Unternehmen wird durch Datenlokalisierung möglicherweise eingeschränkt oder verhindert, im Hinblick auf grenzübergreifende Aktivitäten zur Verfolgung von Cyberkriminellen kann sie sogar ein Hindernis darstellen.

Länder, die sich gegen Technologien von ausländischen Anbietern abschotten oder die Gesetze zur Nutzung der Daten ihrer Bürger sehr restriktiv gestalten, riskieren zudem, dass sie auf dem globalen Talentmarkt ins Abseits geraten und Innovationskraft verlieren, die durch länderübergreifenden Ideenaustausch entsteht.

Einige der führenden amerikanischen Technologieanbieter bieten mittlerweile End-to-End-Verschlüsselung. Damit, so hoffen sie, können sie die Forderung ihrer Kunden nach Sicherheit ihrer Daten im grenzenlosen Internet erfüllen. Die US-Regierung äußerte diesbezüglich Bedenken, da sie ihre Handlungsfähigkeit zum Schutz der Bürger eingeschränkt sieht. Der neue Direktor des GCHQ, Großbritanniens wichtigstem Abhördienst und in seiner Funktion vergleichbar mit der National Security Agency in den USA, ging sogar noch weiter: Nach seiner Ansicht unterstützten amerikanische Technologiekonzerne die Aktivitäten von Terroristen, indem sie ihnen eine weltweite verschlüsselte Kommunikation ermöglichen.[11]

Diese Kritik wird Technologieunternehmen jedoch kaum davon abbringen, die Verbesserung von Verschlüsselungstechniken voranzutreiben. Denn ihr wichtigstes Ziel lautet: Vertrauen zurückgewinnen – etwas, das Regierungen erst gelingen wird, wenn sie einen gesetzlichen Rahmen schaffen, der Meinungsfreiheit und sicheren Handel wirksam gewährleistet, und dabei individuelle und nationale Interessen effektiv schützen.

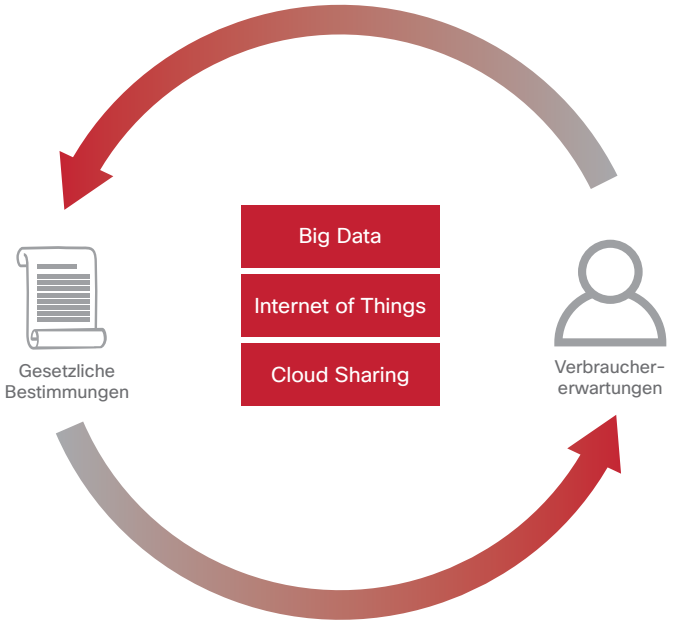
Das Vertrauen ist entscheidend: Technologieanbieter müssen erreichen, dass sich Regierungen und Bürger sicher fühlen, wenn sie ihre Daten mithilfe ihrer Produkte durch die globalen Datenautobahnen schicken. Mark Chandler, Cisco Senior Vice President, General Counsel and Secretary, brachte es bereits zu Jahresbeginn auf den Punkt: „Diese Themen müssen ernsthaft angegangen werden, um erstens Vertrauen zu schaffen und, was am wichtigsten ist, das Internet der nächsten Generation voranzutreiben, das durch die Vernetzung von Menschen und Geräten für alle Bürger der Erde Freiheit, Wohlstand und Chancen ermöglicht."[12]

Datenschutzkompatibilität

Die Einstellung einer Person oder eines Unternehmens zum Thema Datenschutz kann erheblich davon abhängen, in welchem Teil der Welt diese angesiedelt sind und arbeiten. Diese unterschiedlichen Standpunkte haben Einfluss darauf, wie Regierungen den Datenschutz regulieren und wie Unternehmen ihre Geschäfte durchführen, wenn gesetzliche Vorschriften verschiedener Länder im Widerspruch zu einander stehen. Der in Zusammenarbeit von Cisco und der Cloud Security Alliance erstellte ***Data Protection Heat Index Survey Report*** weist auf einige Herausforderungen für Unternehmen hin, die mit Daten arbeiten, die sich außerhalb der eigenen Landesgrenzen befinden, oder von Personen stammen, die in einem anderen Land angesiedelt sind als das Unternehmen selbst.

Datenschutzkompatibilität, d. h. die Schaffung einheitlicher globaler Datenschutzansätze, wird angesichts der immer umfangreicheren Nutzung von Cloud-Diensten ein zunehmend drängendes Thema. Erwirbt beispielsweise ein in den USA ansässiges Unternehmen Cloud-Datenspeicher von einem Anbieter in Indien und verwendet diesen zur Speicherung

Abbildung 38: Erfüllung diverser gesetzlicher Vorschriften und Verbraucheranforderungen



der Daten von Kunden, die in Deutschland leben, stellt sich die Frage, welche Datenschutzgesetze welchen Landes oder welcher Region zur Anwendung kommen.

Weitere wichtige Faktoren im Zusammenhang mit Datenschutzkompatibilität sind zudem das Internet of Things (IoT) und Big Data. Wenn Unternehmen neue Möglichkeiten für die Vernetzung von Geräten abwägen oder riesige Datensätze zur Entscheidungsfindung nutzen, benötigen sie klare Strukturen und Regeln für die Art und Weise, wie diese Daten auf globaler Ebene verarbeitet werden.

Aus diesem Grund sind mittlerweile unterschiedliche Maßnahmen für die Harmonisierung von Datenschutzanforderungen über Regionen oder Ländergruppen hinweg auf den Weg gebracht worden. So arbeitet die Europäische Union gegenwärtig an einer Aktualisierung des bestehenden Datenschutzrahmens – der *Allgemeinen Datenschutzverordnung* –, um Datenschutzrichtlinien besser aufeinander abzustimmen. Die Bemühungen für einen Konsens in Bezug auf Datenschutz- und Datenhoheitsgesetze nehmen immer mehr zu. Eine bessere Abstimmung ist natürlich wünschenswert, allerdings sollte die endgültige Fassung auch ergebnisorientiert sein, mit Bestimmungen anderen Regionen vereinbar sein und neue Technologien berücksichtigen. Für den Asien-Pazifik-Raum hat die Asia-Pacific Economic Cooperation (APEC) das Cross-Border Privacy Enforcement Arrangement entwickelt, um die Datenweitergabe zwischen den lokalen Märkten zu vereinfachen. Allerdings müssen Regierungen noch stärker daran arbeiten, kompatible Regelungen für Datenschutz und -sicherheit zu entwerfen, und diese in global anerkannten Standards verankern, die ein offenes Internet mit freiem Datenfluss über nationale und internationale Grenzen hinweg ermöglichen.

Wenn Länder und Regionen ihre Datenschutzansätze klar definieren, sind Unternehmen besser in der Lage, konsistente Datenschutzverfahren auf globaler Ebene anzuwenden. Gleichzeitig lassen sich effektivere Modelle für einen „eingebauten Datenschutz“ implementieren, sodass Produkte und Services von Anfang an mit integrierten Datenschutzfunktionen ausgestattet werden können. Klare und konsistente Datenschutzrichtlinien würden es Unternehmen zudem erleichtern, Datenschutzvorgaben einzuhalten oder sogar zu übertreffen, unabhängig davon, wo die Produkte eingesetzt werden. So werden gleichzeitig auch innovative Produktentwicklungen und Datennutzungsverfahren gefördert.

Datenschutz: Ein gemeinsames Verständnis

Im Rahmen der Datenschutzumfrage wurden Experten für den weltweiten Datenschutz aus Nordamerika, der Europäischen Union und dem Asien-Pazifik-Raum zu den Datenschutzbestimmungen ihrer jeweiligen Region, behördlichen Praktiken, Benutzerinhalten und Sicherheitsstandards befragt. Die Antworten sind weitestgehend deckungsgleich, was das Verständnis von Datenschutz und die Bedeutung globaler Datenschutzstandards betrifft.

- **Datenspeicherung und -hoheit:** Die Befragten der meisten Ländern gaben an, dass persönliche Daten sowie zur Identifizierung von Personen dienende Daten im jeweiligen Land verbleiben sollten.
- **Rechtmäßige Überwachung:** Hinsichtlich der Frage, wann und wie Daten überwacht werden dürfen, z. B. im Rahmen strafrechtlicher Ermittlungen, teilten die Befragten weitestgehend dieselbe Ansicht.
- **Benutzereinwilligungen:** 73 % der Befragten sprachen sich für eine globale Charta der Verbraucher-Grundrechte aus. 65 % gaben zudem an, dass eine solche Regelung unter Federführung der Vereinten Nationen entwickelt werden sollte.
- **Datenschutzgrundsätze:** Die Teilnehmer wurden gefragt, ob von der Organisation für die wirtschaftliche Zusammenarbeit und Entwicklung (OECD) verfasste Datenschutzgrundsätze eine Datenharmonisierung eher vereinfachen oder erschweren würden. Die befragten Experten begrüßten zum größten Teil die Einführung solcher Grundsätze.

Zusammengefasst zeigt die Umfrage, dass ein Großteil der Experten für die Einführung allgemeiner Datenschutzgrundsätze plädiert und dass eine standardisierte Anwendung auf globaler Ebene die Wirtschaft eher vorantreiben als bremsen würde. Die Ergebnisse zeigen auch, dass viele der Experten ein Interesse daran haben, Datenschutzgrundsätze von Anfang an in neue Technologien zu integrieren, anstatt Lösungen nachträglich an Datenschutzvorgaben anzupassen. Allerdings stecken derzeitige Datenschutzregelungen noch in den Kinderschuhen und unterliegen rapiden Veränderungen.

Ein höheres Maß an Harmonisierung würde sowohl Unternehmen als auch Verbrauchern zugutekommen. Doch solange auf globaler Ebene keine einheitlichen Regelungen bestehen, müssen Unternehmen Datenschutz- und Datensicherheitsfragen sorgfältig abwägen und ihre Produkte und Verfahren proaktiv an die unterschiedlichen gesetzlichen Vorschriften und Verbraucheranforderungen anpassen.

Mehr zum Thema Datenschutz erfahren Sie im Blog-Beitrag „Data Protection in the Balance – EU Citizen Protection and Innovation."

4. Cybersicherheit neu überdenken – vom Benutzer bis in die Führungsetage

Um Sicherheit heute effektiv gewährleisten zu können, müssen Unternehmen das Thema Cybersicherheit neu überdenken. Sie müssen Benutzer, Prozesse und Technologien besser miteinander abstimmen, Sicherheit zum Vorstandsthema machen. Sie müssen außerdem fortschrittliche Kontrollmechanismen einführen, damit die Angriffsfläche von Endpunkten und Systemen reduziert und Netzwerke nach einem Angriff wiederstandsfähiger gemacht werden können.

Sicherer Zugriff: Wer greift wann und wie auf das Netzwerk zu

CISOs und andere Sicherheitsverantwortliche sehen sich komplexen Herausforderungen gegenüber, wenn es darum geht, Zugriff auf Netzwerkinformationen und -services bereitzustellen. Aufgrund des zunehmenden Trends in Richtung Mobility und Bring-Your-Own-Device (BYOD) müssen sie sicherstellen, dass Mitarbeiter von jedem Standort und über jedes Gerät auf Unternehmensressourcen zugreifen können.

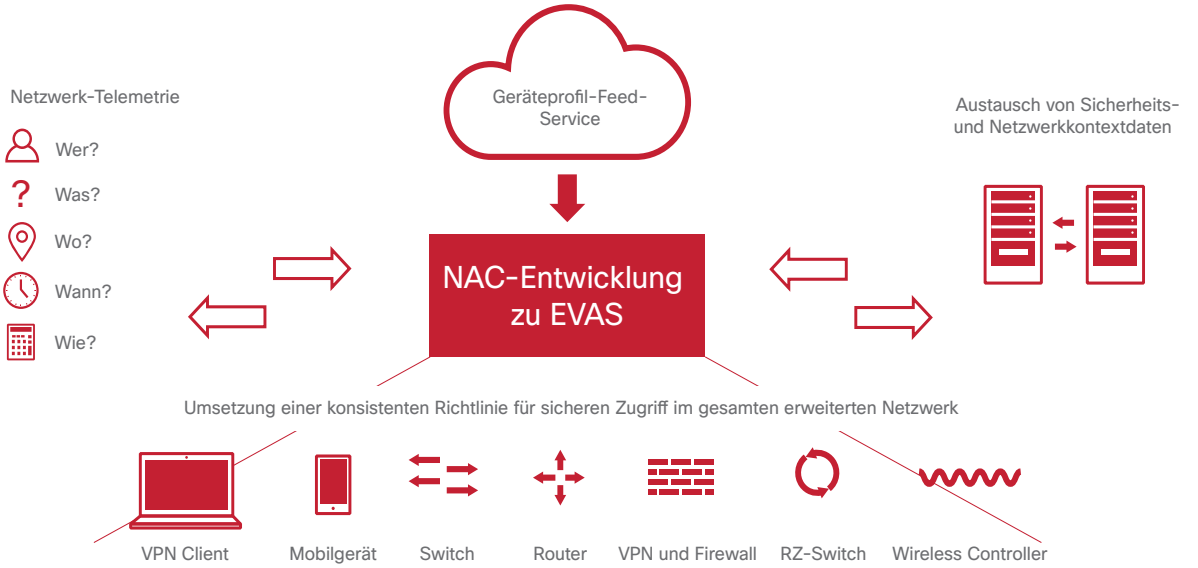
Darüber hinaus muss das Netzwerk gegen nicht autorisierte Zugriffe und Angriffe abgesichert werden, ohne jedoch den Zugriff für berechtigte Benutzer einzuschränken. Virtual Private Networks (VPNs) waren lange Zeit die Standardlösung für die Netzwerkzugriffskontrolle. Allerdings erfordern einige VPNs komplizierte Anmeldeverfahren seitens der Benutzer sowie spezielle Software und erlauben den Zugriff auf das Netzwerk nur zu bestimmten Zeiten und über bestimmte Geräte. Zudem können IT-Abteilungen bei vielen VPNs nicht festzustellen, wer von welchem Standort aus und mit welchem Gerät auf das Netzwerk zugreift. Mit der Weiterentwicklung von VPNs erhält die IT jedoch einen besseren Überblick und für die Benutzer wird eine transparentere Umgebung geschaffen, was ein höheres Maß an Endpunkt-Sicherheit ermöglicht.

Netzwerkzugriffskontrollen (Network Access Controls, NACs) entwickeln sich immer mehr von allgemeinen Sicherheitsfunktionen hin zu komplexeren Transparenz-, Zugriffs- und Sicherheitskontrollen für Endpunkte (Endpoint Visibility, Access and Security Controls, EVAS). Im Gegensatz zu älteren NAC-Technologien verwenden EVAS viel detailliertere Informationen zur Durchsetzung von Zugriffsrichtlinien, u. a. Daten zur Benutzerrolle sowie Informationen zu Standort, Geschäftsprozessen und Risikomanagement. EVAS-Kontrollen erlauben zudem nicht nur den Zugriff vom Computer, sondern auch von IoT- und Mobilgeräten aus.

Darüber hinaus kann mit EVAS das Netzwerk bei der Durchsetzung von Sicherheitsrichtlinien als Sensor fungieren. EVAS kontrollieren zudem den Zugriff auf Netzwerkservices im gesamten erweiterten Netzwerk – auch für standortferne Geräte (VPN) – oder auf vertrauliche Ressourcenpools innerhalb des Netzwerks. Mit EVAS kann außerdem die Angriffsfläche von Endpunkten und Netzwerken verkleinert werden. Ein weiterer Vorteil: Das Ausmaß und der Umfang von Angriffen lässt sich eindämmen, die Beseitung kann beschleunigt und das Netzwerk nach einem Angriff widerstandsfähiger gemacht werden.

Weitere Informationen zu EVAS-Lösungen und wie diese zur Verbesserung der Unternehmenssicherheit beitragen, finden Sie im Cisco Security Blog-Beitrag „New White Paper from Enterprise Strategy Group on the Evolution of and Need for Secure Network Access“.

Abbildung 39: Entwicklung von Network Access Controls (NACs) hin zu Endpoint Visibility, Access, and Security (EVAS) Controls



Vor einem Angriff ermöglichen EVAS:

- **Identifizierung risikoreicher Ressourcen:** Laufende Überwachung aller mit dem Netzwerk verbundenen Ressourcen, Identifizierung nicht konformer Benutzer, Geräte und Anwendungen und Abgleich der Informationen mit Drittanbieter-Tools zur Schwachstellenanalyse
- **Verbessertes Risikomanagement:** Erfassung aussagekräftiger Informationen, die an andere Sicherheits- und Netzwerkanwendungen weitergegeben werden können, um Workflows und Abläufe zu optimieren und Bereinigungsmaßnahmen zu priorisieren
- **Durchsetzung detaillierter Netzwerkzugriffsrichtlinien:** Bereitstellung kontextbezogener Informationen für die Durchsetzung detaillierter Sicherheitsrichtlinien und Einschränkung des Zugriffs auf vertrauliche Daten, Ressourcen oder Netzwerksegmente

Während eines Angriffs ermöglichen EVAS:

- **Integration mit erweiterten netzwerkbasierten Abwehrsystemen:** Informationsaustausch bei der Erkennung von Malware, um das Angriffsverhalten durch die Korellation von Daten zu Endpunktverbindungen und Konfigurationen zu bestimmen
- **Blockierung von „Kill Chain"-Taktiken kompromittierter Systeme:** Blockierung kompromittierter Systeme, um die Ausweitung des Angriffs auf empfindliche Netzwerkbereiche zu unterbinden, aus denen Anmeldeinformationen abgegriffen und sensible Daten ausgeschleust werden sollen
- **Eindämmung des Ausmaßes eines Angriffs:** Quarantänisierung von Systemen mit ungewöhnlichem Verhalten

Nach einem Angriff ermöglichen EVAS:

- **Schwachstellenanalyse bei Endgeräteprofilen:** Weitergabe von Informationen der EVAS-Datenbank an Tools zur Schwachstellenanalyse, um Fehlerbehebungsmaßnahmen zu priorisieren
- **Bereinigen kompromittierter Systeme:** Durch die Integration mit Systemen für das Management von Sicherheitsinformationen und -vorfällen (Security Information and Event Management, SIEM) sowie Systemen für die Endpunktsicherheit können EVAS Fehlerbehebungen automatisieren und fortlaufend überwachen.
- **Optimierung von Zugriffsrichtlinien und Sicherheitskontrollen:** Segmentierung von Anwendungsdatenverkehr und Hinzufügen neuer Firewall-Regeln und IPS-Signaturen mithilfe von Netzwerk- und Sicherheitshardware

Im Gegensatz zu den übermäßig komplexen Netzwerkzugriffskontrollen der Vergangenheit eröffnen EVAS-Lösungen neue Geschäftschancen. Je mehr Unternehmen BYOD-Modelle, Cloud Computing und Mobility-Initiativen nutzen, desto wichtiger werden transparente Einblicke in die verbundenen Geräte und Benutzer sowie eine effektive Durchsetzung von Sicherheitsrichtlinien. Laut Prognosen der Sicherheitsexperten von Cisco werden CISOs zunehmend auf EVAS-Lösungen zurückgreifen, um die komplexen Vernetzungen von Benutzern, Geräten, Netzwerken und Cloud-Services zu verwalten.

Cybersicherheit muss Chefsache werden

Wie aus der *Cisco Security Capabilities Benchmark Study* hervorgeht, ist in 91 % der befragten Unternehmen eine Führungskraft direkt mit Sicherheitsfragen betraut. Das Thema Sicherheit muss heute jedoch noch höher angesiedelt werden: in der Vorstandsetage.

Faktoren wie die aktuellen, massiven Datenschutzverletzungen bei namhaften Unternehmen, verschiedene Gesetze und Vorschriften in Bezug auf Datensicherheit, geopolitische Entwicklungen und nicht zuletzt die Erwartungen der Aktionäre machen Cybersicherheit zu einem Thema, mit dem sich der Vorstand befassen muss. Einem Bericht der Information Systems Audit and Control Association (ISACA) zufolge müssen mittlerweile 55 % der leitenden Angestellten Cybersicherheit als Risikobereich persönlich verstehen und verwalten.[13]

Das ist eine positive Entwicklung – nach Ansicht der Sicherheitsexperten von Cisco jedoch schon lange überfällig. Kein Unternehmen kommt heute mehr ohne IT aus. Aus diesem Grund geht die Sicherheit auch nicht nur diejenigen Mitarbeiter etwas an, die direkt mit IT-Sicherheitsfragen betraut sind, sondern alle – vom CEO bis zum Neuzugang. Jeder steht in der Verantwortung und sollte gewisse Grundlagen verinnerlichen, um nicht zum Opfer von Cyberangriffen zu werden.

Die Sicherheitsexperten von Cisco sind der Ansicht, dass für die Zukunft der Cybersicherheit eine stärkere Beteiligung der Vorstandsetage notwendig ist. Die Vorstände und Verwaltungsräte von Unternehmen müssen sich über die Cybersicherheitsrisiken und deren potenzielle geschäftliche Auswirkungen bewusst sein. Um das Ausmaß von Cybersicherheitsproblemen in vollem Umfang zu verstehen, müssen einige Vorstände unter Umständen Technologie- und Cybersicherheitsexperten zu Rate ziehen.

Vorstände müssen zudem anfangen, unbequeme Fragen zu Sicherheitskontrollen zu stellen: *Über welche Kontrollmechanismen verfügen wir? Wie gründlich sind diese getestet worden? Haben wir ein Reporting-Verfahren? Wie schnell können wir unvermeidliche Kompromittierungen erkennen und beheben?* Und wahrscheinlich die wichtigste Fragen von allen: *Was müssen wir sonst noch wissen?* CIOs müssen in der Lage sein, diese Fragen verständlich und nachvollziehbar zu beantworten und auch die möglichen geschäftlichen Auswirkungen klar darzulegen.

John Stuart, Chief Security and Trust Officer bei Cisco, gab vor Kurzem in einem Interview des FORTUNE Magazine[14] an, dass Fragen wie diese „interessante Entwicklungen" in der Security-Branche in Gang setzen werden. Der nächste Schritt – so zumindest die Hoffnung – wäre laut Stewart, dass Hersteller ihre Produkte von Anfang an mit Sicherheitsfunktionen ausstatten.

Stewart zufolge wird durch das Internet of Things (IoT) und die damit einhergehende Vernetzung von immer mehr Geräten, die keine menschliche Interaktion erfordern, unvermeidlich zu Zwischenfällen mit potenziell weitreichenden Folgen führen. Mit Produkten, die standardmäßig mit Sicherheitsfunktionen ausgestattet sind, ließen sich solche Probleme jedoch vermeiden.

Vorstände von Technologiekonzernen sollten daher gemeinsam mit ihren Sicherheitsexperten prüfen, wie sicher ihre aktuellen Produkte sind und ggf. so schnell wie möglich mit der Integration von Sicherheitsfunktionen beginnen.

Mehr hierzu erfahren Sie im Videoblog von John Steward, Chief Security and Trust Officer bei Cisco: http://blogs.cisco.com/security/ensuring-security-and-trust-stewardship-and-accountability.

Cisco Sicherheitsmanifest: Grundlagen für Sicherheit in der Praxis

CISOs stehen heute vor komplexen Herausforderungen: I*hr Team muss erster Ansprechpartner für alle Sicherheitsfragen des Unternehmens werden und es benötigt leistungsfähige Tools, um Sicherheitsprobleme priorisieren zu können. Benutzer müssen geschützt werden, unabhängig davon, ob sie am Unternehmensstandort oder mobil arbeiten.*

Mit dem Cisco Sicherheitsmanifest haben die Experten von Cisco Security Research eine Reihe von Prinzipien formuliert, die auf diese Herausfordeurngen ausgerichtet sind. Unternehmen, die diese Grundsätze einhalten, können eine solide Grundlage für einen dynamischen, anpassungsfähigen und innovativen Sicherheitsansatz schaffen.

1. **Sicherheit kann ein Motor für das Unternehmenswachstum sein:** IT-Sicherheit darf nicht zulasten der Produktivität der Benutzer oder der Innovationskraft des Unternehmens gehen. Häufig ist jedoch das der Fall. Der Grund: Sicherheitsteams werden erst spät (oder überhaupt nicht) in die Planung von Projekten des Unternehmens einbezogen, die neue Technologien erfordern. Allerdings: Sicherheitsteams müssen hier auch proaktiv vorgehen. Ebenfalls wichtig: Sie müssen Sicherheitsprozesse implementieren, die Flexibilität und Wachstum ermöglichen, dabei aber sicherstellen, dass die Daten, die Ressourcen und der Ruf des Unternehmens geschützt sind.
2. **Sicherheitsmaßnahmen müssen mit der bestehenden Architektur vereinbar und praktikabel sein:** Neue Sicherheitstechnologien dürfen keine neue Architektur erfordern, denn Architekturen sind grundsätzlich mit Einschränkungen verbunden. Die Einführung neuer Sicherheitstechnologien darf zudem keine Anpassung von Geschäftsprozessen erfordern. Genauso wenig darf sie verhindern, dass Betriebsabläufe entsprechend Unternehmensanforderungen angepasst werden könen. Sind zu viele Sicherheitsarchitekturen in Betrieb, behindern sie die Benutzer und führen dazu, dass sie die Sicherheitsmaßnahmen umgehen, was letztlich die Unternehmenssicherheit gefährdet. Unpraktikable, nur durch spezialisierte Fachleute bedienbare Sicherheitstechnologien nutzen Unternehmen nur wenig.
3. **Sicherheitsmaßnahmen müssen transparent und aussagekräftig sein:** Die Benutzer müssen nachvollziehen können, warum bestimmte Aktionen blockiert werden. Sie müssen geschult werden, wie sie ihre Arbeit ungehindert durchführen können, ohne Sicherheitsfunktionen zu umgehen. Erhält ein Benutzer z. B. beim Aufrufen einer Website die Meldung „Der Zugriff auf diese Seite wurde vom Administrator gesperrt", kann er nicht nachvollziehen, ob und warum diese Website ein potenzielles Risiko darstellt. Eine Meldung wie „Zugriff verweigert. Auf dieser Seite wurde in den letzten 48 Stunden Malware gefunden." hätte dagegen einen ganz anderen Effekt. Sicherheitstechnologien müssen Benutzer außerdem klare Empfehlungen geben und an Ressourcen verweisen, die sie dabei unterstützen, ihre Aufgaben sicher zu erledigen.
4. **Sicherheitsteams benötigen einen umfassenden Überblick und müssen angemessen reagieren können:** Offene Sicherheitsarchitekturen ermöglichen es Sicherheitsteams, die Effektivität ihrer Lösungen zu überprüfen. Sie benötigen außerdem Tools, mit denen sie den gesamten Datenverkehr sowie alle Ressourcen im Netzwerk im Blick haben. Wenn sie die Funktionsweise ihrer Sicherheitstechnologien verstehen und ungewöhnliches Verhalten in der IT-Umgebung erkennen können, reduziert sich der Administrationsaufwand, sie können Bedrohungen leichter identifizieren, dynamisch und adäquat darauf reagieren und Abwehrmechanismen entsprechend anpassen. So können sie außerdem wirksame Kontrollen implementieren, die eine gezielte Behebung von Problemen ermöglichen.
5. **IT-Sicherheit fängt bei den Benutzern an:** Unternehmen, die allein auf Technologien setzen, schwächen ihre Sicherheit eher. Denn diese sind lediglich Tools, die zur Sicherung der Umgebung dienen. Wichtiger sind jedoch die Benutzer: Sie müssen geschult werden, damit sie sowohl im Büro als auch zu Hause und im mobilen Einsatz die richtigen Entscheidungen treffen und bei Unsicherheiten rechtzeitig Expertenunterstützung einholen. Richtig aufgeklärte Benutzer verstehen, dass Sicherheitstechnologien allein nicht ausreichen, sondern das erst der Verbund aus Benutzern, Prozessen und Technologie wirksamen Schutz vor Bedrohungen bietet. Ein erfolgreicher Sicherheitsansatz hängt von der Veranbtwortung und Umsicht aller Benutzer im Unternehmen ab.

Das Cisco Sicherheitsmanifest bietet eine Grundlage für notwendige Veränderungen. Sicherheitstechnologien, Richtlinien und Best Practices sorgen für ein höheres Maß an Sicherheit für alle Mitarbeiter und ermöglichen jedem einzelnen Benutzer besser informierte Entscheidungen hinsichtlich Risiken. Und mithilfe solider Grundlagen gewinnen Benutzer ein besseres Verständnis darüber, warum sie bestimmte Aktionen nicht durchführen können und welche Auswirkungen das Umgehen von Sicherheitsmaßnahmen nach sich ziehen kann.

Das Cisco Sicherheitsmanifest oder ähnlich gelagerte Grundsätze versuchen sowohl Benutzern als auch Sicherheitsexperten das Thema Sicherheit in allen Aspekten zu vermitteln: Obwohl viele Bedrohungen abgewendet werden können, lassen sich Angriffe nicht komplett vermeiden. Jedoch kann die Beseitigung deutlich beschleunigt werden. Es geht nicht nur darum, Angriffe und Bedrohungen zu vermeiden, sondern kompromittierte Systeme so schnell wie möglich wiederherzustellen.

Über Cisco

Cisco bietet intelligente Lösungen für die IT-Sicherheit und verfügt über das branchenweit umfangreichste Portfolio an Systemen für eine fortschrttliche Bedrohungsabwehr, die unterschiedlichste Angriffsvektoren abdecken. Durch seinen bedrohungsorientierten und operationalisierten Ansatz verringert Cisco die Komplexität und verhindert die Fragementierung von Sicherheitstools. Dies ermöglicht ein hohes Maß an Transparenz, konsistente Kontrollen und einen intelligenten Bedrohungsschutz vor, während und nach einem Angriff..

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

Eine hochmoderne Infrastruktur, unterstützt durch branchenführende Systeme, wertet die Telemetriedaten aus. Dies ermöglicht maschinelles Lernen, Bedrohungen für Netzwerke, Rechenzentren, Endpunkte, Mobilgeräte, virtuelle Systeme, das Internet, den E-Mail-Verkehr und die Cloud können nachverfolgt, Ursachen können 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.

Das CSI-Netzwerk setzt sich aus verschiedenen Gruppen zusammen: Talos, Security & Trust Organization, Managed Threat Defense (MTD) und Security Research and Operations (SR&O).

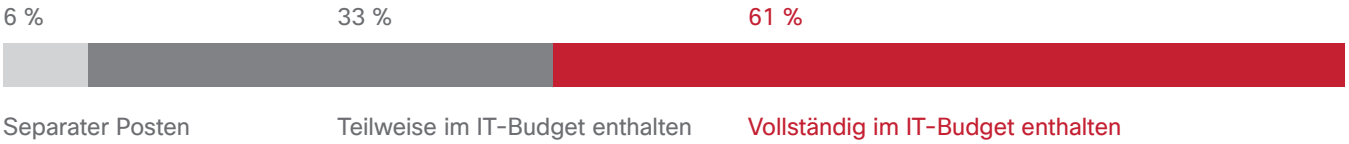
Weitere Informationen zum bedrohungsorientierten Sicherheitsansatz von Cisco finden Sie unter www.cisco.com/web/DE/products/security/index.html.

Anhang

Weitere Ergebnisse der Cisco Security Capabilites Benchmark Study

Ressourcen

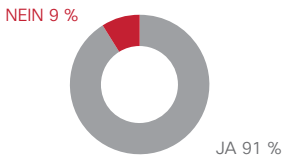
Werden Sicherheitsmaßnahmen als Teil des IT-Budgets veranschlagt? Mitarbeiter der Unternehmens-IT; n=1.720



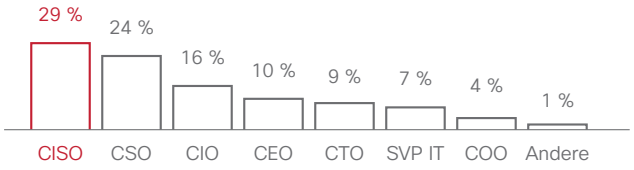
Sicherheitsrichtlinien und -verfahren

Für die Leitung der IT-Sicherheit ist in den meisten Fällen ein CISO oder CSO im Einsatz.

Ist in Ihrem Unternehmen eine Führungskraft direkt mit der IT-Sicherheit betraut?
Befragte, die eine klare Verteilung von Rollen und Verantwortlichkeiten angaben; n=1.603



Führungspositionen
Befragte, die angaben, dass eine Führungskraft in ihrem Unternehmen direkt für die IT-Sicherheit zuständig ist; n=1.465



Besonders im Gesundheitswesen sind tendenziell keine Führungskräfte direkt für die IT-Sicherheit zuständig.

Report teilen

Fast zwei Drittel gaben an, dass die Unternehmensführung der IT-Sicherheit eine hohe Priorität einräumt.

Sicherheitsbewusstsein auf Führungsebene n=1.738	Sicherheitsexperten n=797			CISO n=941		
	Stimme nicht zu/		Stimme vollständig zu	Stimme nicht zu/		Stimme vollständig zu
IT-Sicherheit hat für die Unternehmensführung eine hohe Priorität.	8 %	34 %	58 %	3 %	30 %	67 %
Die Rollen und Verantwortlichkeiten im Bereich der IT-Sicherheit sind in der Führungsebene klar verteilt.	9 %	39 %	52 %	2 %	32 %	64 %
Die Unternehmensführung hat eindeutige Kennzahlen für die Bewertung unseres Sicherheitsprogramms festgelegt.	11 %	44 %	45 %	4 %	37 %	59 %

Ein höherer Anteil der Befragten, deren Unternehmen noch nicht durch einen Sicherheitsvorfall für öffentliches Aufsehen gesorgt hat, stimmen zu, dass die Führungsebene ihres Unternehmens der IT-Sicherheit eine hohe Priorität einräumt.

Bei einem hohen Anteil der befragten Unternehmen werden die Mitarbeiter eng in die Sicherheitsprozesse einbezogen.

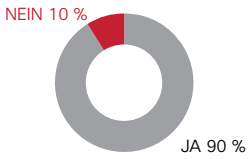
Sicherheitsprozesse n=1.738	Sicherheitsexperten n=797			CISO n=941		
	Stimme nicht zu/		Stimme vollständig zu	Stimme nicht zu/		Stimme vollständig zu
Geschäftsbereichsleiter werden aufgefordert, an den Sicherheitsrichtlinien und -verfahren mitzuwirken.	12 %	39 %	49 %	6 %	40 %	54 %
Mein Unternehmen kann Schwachstellen erkennen, bevor es zu schwerwiegenden Vorfällen kommt.	13 %	43 %	44 %	4 %	39 %	57 %
Mitarbeiter in meinem Unternehmen werden aufgefordert, Ausfälle und Sicherheitsprobleme zu melden.	11 %	34 %	55 %	4 %	36 %	60 %
Sicherheitsprozesse und -verfahren in meinem Unternehmen sind klar definiert und gut dokumentiert.	13 %	39 %	48 %	4 %	37 %	59 %
Dank der Sicherheitsprozesse in meinem Unternehmen können wir potenzielle Sicherheitsprobleme vorhersehen und proaktiv minimieren.	14 %	40 %	46 %	3 %	40 %	47 %
Sicherheitsprozesse in meinem Unternehmen werden mit quantitativen Daten bewertet und überwacht.	13 %	40 %	47 %	4 %	35 %	61 %
Mein Unternehmen hat seine Sicherheitsprozesse optimiert und konzentriert sich nun auf die Verfahrensoptimierung.	12 %	42 %	46 %	4 %	36 %	60 %

Im Vergleich zu den Befragten in großen Unternehmen bewertet ein größerer Anteil der Sicherheitsexperten aus dem Mittelstand die Sicherheitsprozesse ihres Unternehmens als effektiv.

Neun von zehn Befragten geben an, dass regelmäßig Weiterbildungsmaßnahmen für Sicherheitsmitarbeiter stattfinden. In der Regel werden diese Schulungen durch das Sicherheitsteam abgehalten.

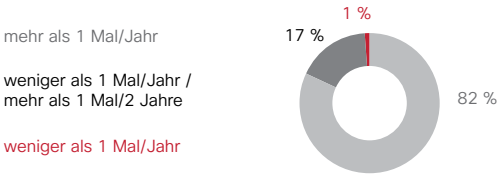
Werden für Sicherheitsmitarbeiter regelmäßig Schulungen zur Sensibilisierung zum Thema Sicherheit und/oder Schulungsprogramme angeboten?

Befragte, die für die Sicherheit verantwortlich sind; n=1.726



Wie oft werden Sicherheitsschulungen angeboten?

Befragte, die für die Sicherheit verantwortlich sind; n=1.556

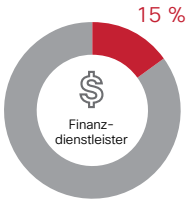


Wer hält die Sicherheitsschulungen ab?

Befragte, bei denen Schulungen für Sicherheitsteams angeboten werden; n=1.556

Internes Sicherheitsteam 79 % | Drittanbieter 38 % | Personalabteilung 25 % | Andere Mitarbeiter 10 % | Andere 1 %

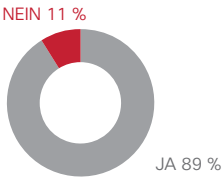
Bei 15 Prozent der befragten Mitarbeiter von Finanzdienstleistern werden Sicherheitsschulungen nicht regelmäßig angeboten.



Etwa zwei Drittel geben an, dass sie sich in Branchenverbänden mit Schwerpunkt auf IT-Sicherheit engagieren.

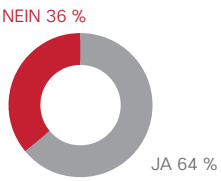
Nehmen Sicherheitsmitarbeiter an Konferenzen und/oder externen Schulungen teil, um ihre Kenntnisse zu erweitern und zu festigen?

Befragte, die für die Sicherheit verantwortlich sind; n=1.715



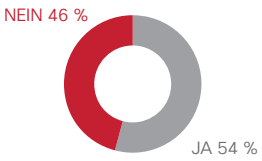
Arbeiten Mitarbeiter in Branchenverbänden oder mit Schwerpunkt auf IT-Sicherheit?

Befragte, die für die Sicherheit verantwortlich sind; n=1.690

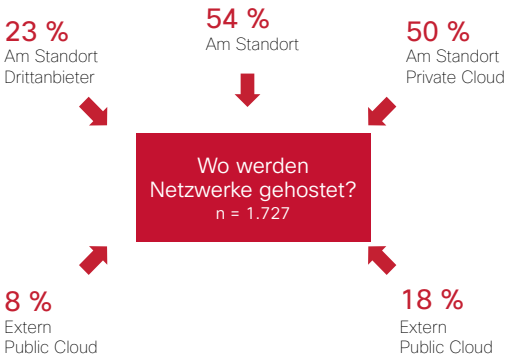


Über die Hälfte der Befragten gibt an, dass ihr Unternehmen durch schon einmal durch einen Sicherheitsvorfall für öffentliches Aufsehen gesorgt hat.

Hat Ihr Unternehmen schon einmal durch einen Sicherheitsvorfall für öffentliches Aufsehen gesorgt?
Befragte, die für die Sicherheit verantwortlich sind; n=1.701



Das Hosten der Unternehmensnetzwerke am Standort ist die am weitesten verbreitete Methode. Weniger als einer von zehn Befragten gibt an, dass das Netzwerk des Unternehmens in einer Public Cloud gehostet wird.



Im Vergleich zu Sicherheitsexperten geben deutlich mehr CISOs an, dass ihr Unternehmensnetzwerk extern gehostet wird (sowohl Private- als auch Public-Cloud).

Sicherheitsniveau

Erwartungsgemäß variieren die Segmente bei vielen Messgrößen für das Sicherheitsniveau.

	Niedrig	Unteres Mittelfeld	Mittelfeld	Oberes Mittelfeld	Hoch
Führungskräfte räumen Sicherheit eine hohe Priorität ein,	22 %	38 %	45 %	71 %	81 %
... und haben eindeutige Kennzahlen für die Bewertung der Effektivität der Sicherheitsmaßnahmen festgelegt.	17 %	19 %	32 %	52 %	79 %
Das Unternehmen verfügt über klar definierte und gut dokumentierte Sicherheitsprozesse/-verfahren,	0 %	22 %	15 %	72 %	88 %
... die mithilfe von quantitativen Daten gemessen und überwacht werden,	0 %	17 %	33 %	65 %	76 %
... und es überprüft regelmäßig die Sicherheitsvorkehrungen und -tools, um sicherzustellen, dass diese stets aktuell und effektiv sind.	0 %	17 %	33 %	65 %	76 %
Dank ausgereifter Prozesse wird die IT-Sicherheit bei Neueinstellungen, Abteilungswechseln und Ausscheiden von Mitarbeitern optimal gewährleistet.	16 %	27 %	36 %	52 %	76 %
Geistiges Eigentum wird inventarisiert und deutlich klassifiziert.	17 %	26 %	40 %	58 %	73 %
Die Computersysteme in meinem Unternehmen sind gut geschützt.	17 %	21 %	41 %	63 %	80 %
Sicherheitstechnologien sind gut integriert und arbeiten effizient zusammen,	17 %	21 %	38 %	59 %	78 %
... das Unternehmen erkennt Sicherheitsschwachstellen, bevor es zu schwerwiegenden Vorfällen kommt.	0 %	23 %	25 %	63 %	70 %

Einige Übereinstimmungen sind jedoch ebenfalls festzuhalten.

	Niedrig	Unteres Mittelfeld	Mittelfeld	Oberes Mittelfeld	Hoch
Eine Führungskraft ist direkt mit der IT-Sicherheit betraut.	85 %	91 %	88 %	93 %	93 %
Das Unternehmen verfügt über eine unternehmensweite, schriftlich fixierte Sicherheitsstrategie, die regelmäßig überprüft wird.	59 %	47 %	58 %	65 %	60 %
Das Unternehmen legt für seine Sicherheitsprozesse Standardrichtlinien (z. B. ISO 27001) zugrunde.	47 %	44 %	50 %	59 %	54 %

Endnoten

1. *Cisco 2014 Midyear Security Report:* http://www.cisco.com/web/offers/lp/midyear-security-report/index.html?keycode=000489027
2. Weitere Informationen zu CMS-Schwachstellen im Abschnitt „Wordpress Vulnerabilities: Who Is Minding the Store?", *Cisco 2014 Midyear Security Report:* http://www.cisco.com/web/offers/lp/midyear-security-report/index.html?keycode=000489027
3. „Goon/Infinity/RIG Exploit Kit Activity", Cisco IntelliShield: Security Activity Bulletin, Juli 2014: http://tools.cisco.com/security/center/mviewAlert.x?alertId=34999
4. *Cisco 2014 Midyear Security Report:* http://www.cisco.com/web/offers/lp/midyear-security-report/index.html?keycode=000489027
5. „Cisco Event Response: POODLE Vulnerability", 15. Oktober 2014: http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_Poodle_10152014.html
6. „OpenSSL Heartbleed vulnerability CVE-2014-0160 – Cisco products and mitigations", Cisco Security Blog, 9. April 2014: http://blogs.cisco.com/security/openssl-heartbleed-vulnerability-cve-2014-0160-cisco-products-and-mitigations
7. „JP Morgan and Other Banks Struck by Hackers", Nicole Perlroth, *The New York Times,* 27. August 2014: http://www.nytimes.com/2014/08/28/technology/hackers-target-banks-including-jpmorgan.html?_r=0; „'Trojan Horse' Bug Lurking in Vital U.S. Computers Since 2011", Jack Cloherty und Pierre Thomas, ABC News, 6. November 2014: http://abcnews.go.com/US/trojan-horse-bug-lurking-vital-us-computers-2011/story?id=26737476
8. „4 Things We Learned from China's 4th Plenum", Shannon Tiezzi, *The Diplomat,* 23. Oktober 2014: http://thediplomat.com/2014/10/4-things-we-learned-from-chinas-4th-plenum/
9. „Brazil's New Internet Law Could Broadly Impact Online Privacy and Data Handling Practices", *Chronicle of Data Protection,* 16. Mai 2014: http://www.hldataprotection.com/2014/05/articles/international-eu-privacy/marco-civil-da-internet-brazils-new-internet-law-could-broadly-impact-online-companies-privacy-and-data-handling-practices/
10. „Russian data localization law may now come into force one year ahead of schedule, in September 2015", Hogan Lovells, Natalia Gulyaeva, Maria Sedykh und Bret S. Cohen, Lexology.com, 18. Dezember 2014: http://www.lexology.com/library/detail.aspx?g=849ca1a9-2aa2-42a7-902f-32e140af9d1e
11. „GCHQ Chief Accuses U.S. Tech Giants of Becoming Terrorists' 'Networks of Choice'", Ben Quinn, James Ball und Dominic Rushe, *The Guardian,* 3. November 2014: http://www.theguardian.com/uk-news/2014/nov/03/privacy-gchq-spying-robert-hannigan
12. „Internet Security Necessary for Global Technology Economy", Mark Chandler, Cisco Blog, 13. Mai 2014: http://blogs.cisco.com/news/internet-security-necessary-for-global-technology-economy
13. „Cybersecurity: What the Board of Directors Needs to Ask", ISACA und The Institute of Internal Auditors Research Foundation, August 2014: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-What-the-Board-of-Directors-Needs-to-Ask.aspx
14. „It's Time for Corporate Boards to Tackle Cybersecurity. Here's Why", Andrew Nusca, FORTUNE Magazine, 25. April 2014: http://fortune.com/2014/04/25/its-time-for-corporate-boards-to-tackle-cybersecurity-heres-why/

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.