Cybersicherheit und Ihr Unternehmen

So hoch sind die Kosten durch Cyberkriminalität und so schützen Sie Ihre Daten

Präsentiert von

Inhalt

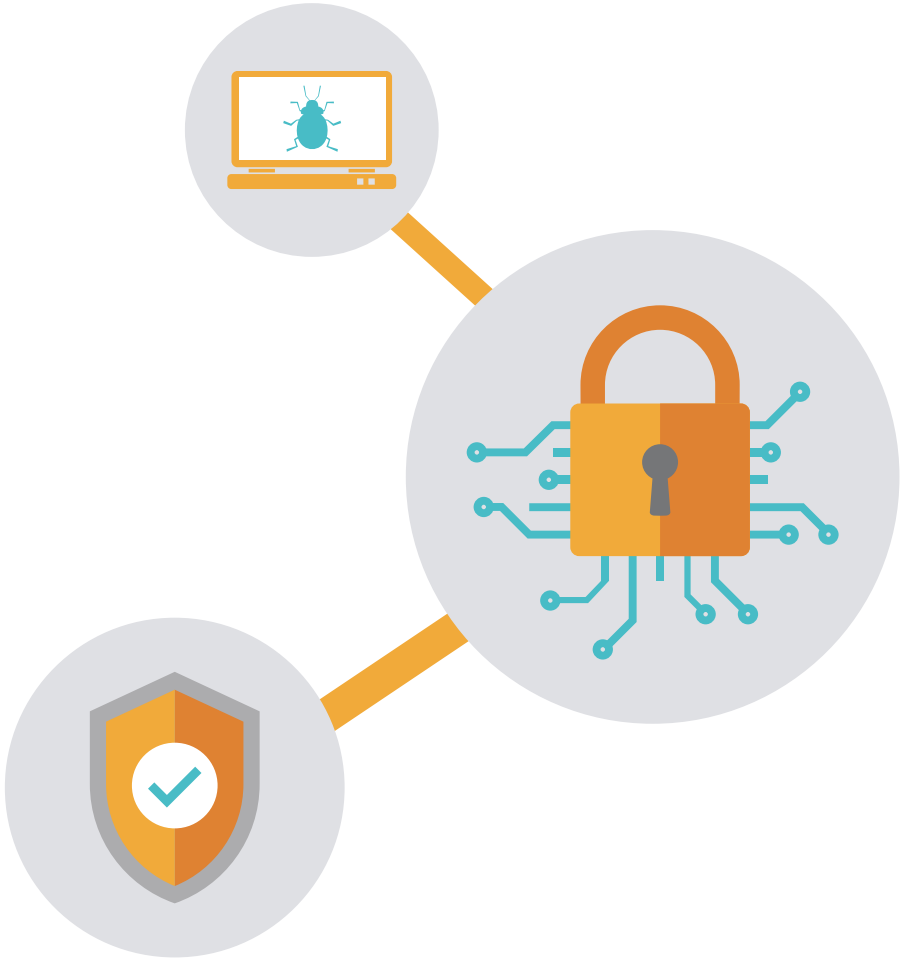
Einführung

„Viele Führungskräfte erklären Cyberangriffe zu der Gefahr, die unsere Generation prägen wird.“ – Dennis Chesley, Global Risk Consulting Leader, PwC[1]

Cybersicherheit ist keine neue Bedrohung. Und sie nimmt zu. Hacker werden immer besser. Und sie haben mehr Ansatzpunkte, über die sie in ein Netzwerk eindringen können. Das Internet der Dinge vervielfacht die Anzahl der Endgeräte, die häufig der einfachste Angriffspunkt sind. Hinzu kommt, dass die Ziele immer größer werden und Störungen neue Dimensionen annehmen.

Am 21. Oktober 2016 wurde der in den USA ansässige DNS Provider Dyn Opfer des bisher größten Distributed-Denial-of-Service (DDoS)-Angriffs (verteilter Überlastangriff). Einige der größten Websites der Welt – darunter Netflix,[2] Amazon und Twitter – mussten mehrere Stunden offline gehen.

Im Januar 2017 kam es bei der Lloyds Bank zu erheblichen Ausfällen der Online-Dienste. Kunden konnten weder ihre Kontostände abrufen noch Zahlungen vornehmen. Der Zugriff über mobile Apps war ebenfalls unterbrochen. Lloyds bestätigte zwar nix, aber dennoch halten sich hartnäckig Gerüchte, dass ein DDoS-Angriff die Ursache war.[3]



Quelle: [1] PwC: The Global State of Information Security Survey 2016 [2] http://thehackernews.com/2016/10/dyn-dns-ddos.html [3] https://www.theguardian.com/business/2017/jan/23/lloyds-bank-accounts-targeted-cybercrime-attack

Einführung

Attacken wie diese sind mehr als schlechte Publicity. Sie kosten richtig Geld.

Im Spiceworks-Umfragebericht von 2016 zur Sicherheit von Druckern gaben 34 Prozent der Unternehmen an, dass ein Angriff zu vermehrten Help-Desk-Anrufen und einem höheren Zeitaufwand für Support-Leistungen führte. 29 Prozent gaben an, die Angriffe beeinträchtigten die Produktivität bzw. Effizienz und 26 Prozent benannten längere Systemausfallzeiten als Problem.[4]

Fast 60 Prozent der für ein IBM CSO Bewertungspapier befragten Sicherheitsexperten erklärten, dass die Angreifer immer ausgeklügelter und raffinierter vorgingen und damit die hochentwickelten Schutzvorkehrungen ihrer Unternehmen aushebelten.[5] Besorgte CIOs zählen die Cybersicherheit seit mehr als einem Jahrzehnt zu den zehn wichtigsten Problemen, heute rangiert sie in der jährlichen Trendstudie der Gesellschaft für Informationsmanagement (SIM) auf Platz zwei.[6]

Viele dieser Schäden sind vermeidbar. Auf den folgenden Seiten werden wir uns mit weit verbreiteten Irrtümern in Bezug auf die Cybersicherheit auseinandersetzen, wir werden die Auswirkungen der Cyberkriminalität genauer unter die Lupe nehmen und Ihnen Anregungen geben, was Sie besser machen können, um sich vor Angriffen zu schützen. Abschließend werden wir einen Blick in die Zukunft werfen und eine Prognose wagen: Was ist zu erwarten und wie können wir uns darauf vorbereiten?

Quelle: [4] HP Printer Security Research 2016, Spiceworks [5] IBM CSO Assessment 2014 [6] SIM IT Trends Survey 2015

Widerlegung von Mythen über Cybersicherheit

Fünf weit verbreitete Irrtümer,
die Unternehmen der Gefahr von Cyberkriminalität aussetzen können

Bekannte Namen gelangen bei Datenschutzverletzungen eher in die Schlagzeilen, aber das Risiko besteht für alle Arten von Unternehmen. Nachfolgend finden Sie sechs Mythen über die Cybersicherheit, die Unternehmen für Hacker anfällig machen können.

Security Breach

Security Leaks

Security Practices

Antivirus Software

Cyber Attack

1 Unternehmen können sich schnell von jedem Angriff erholen

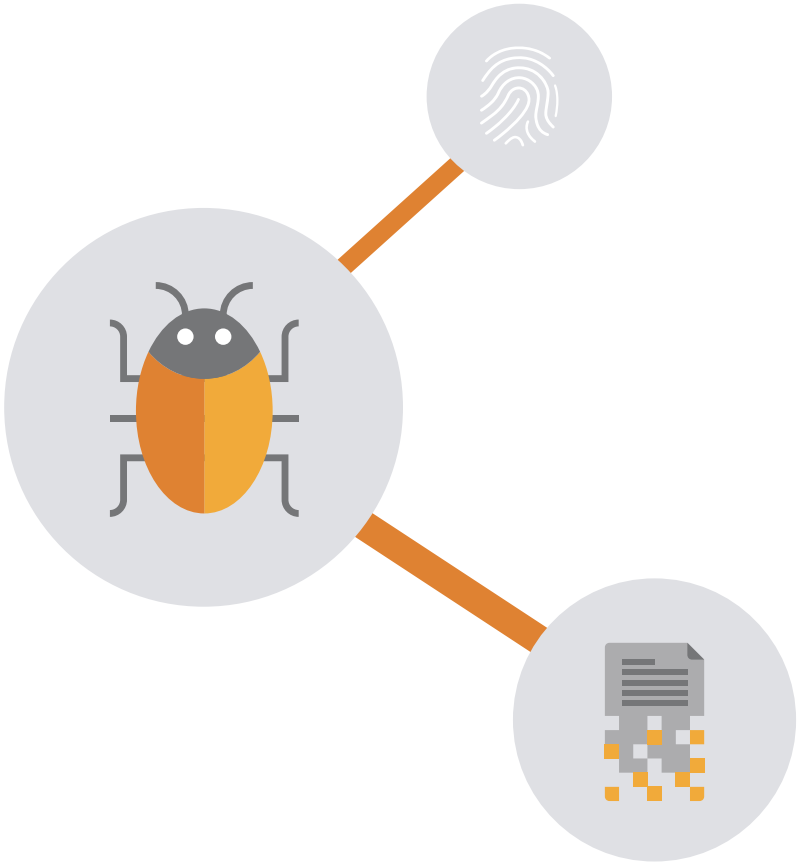
Es ist noch immer sehr schwierig, die Kosten von Angriffen auf die Cybersicherheit für kommerzielle Unternehmen zu messen. Früher nahm man an, dass die Auswirkungen von Angriffen an den sinkenden Aktienkursen zu erkennen seien.

Aber Aktienkurse sind nur ein Teil der Geschichte – und sie sind nur der Anfang. Während sich die Aktien innerhalb einiger Wochen erholen können, summieren sich die langfristigen Kosten. Neue Sicherheitsprogramme, personelle Neubesetzungen, Rechtskosten - all diese Faktoren können ein Unternehmen über lange Zeit nach einem Angriff erheblich beeinträchtigen.

Und die Kosten steigen weiter. Nach einer kürzlich erschienenen Ponemon-Studie stiegen die durchschnittlichen, auf das Jahr umgerechneten Kosten eines Angriffs von **EUR 7,2 Mio**. im letzten Jahr auf **EUR 8,9 Mio**. in diesem Jahr.[7]

Quelle: [7] Ponemon Institute Cost of Cyber Crime Study 2016

2 Sicherheitslücken sind selten, deshalb ist ein ernsthafter Schutz nicht notwendig



Die IDC ermittelte,[8] dass 2016 der Anteil der Unternehmen, bei denen eine Sicherheitsverletzung auftrat, 99 Prozent erreicht hat. Dabei ist die Anzahl der Unternehmen, die sechs bis zehn Sicherheitsverletzungen in einem Jahr berichten, von 9 Prozent im Jahr 2014 auf 18,9 Prozent im Jahr 2016 gestiegen.[9]

Diese Zahlen könnten durchaus sogar noch zu niedrig sein. Die Berichterstattung über Sicherheitsverletzungen ist häufig völlig unzureichend, da Unternehmen bestrebt sind, die damit einhergehende negative Presse zu vermeiden.

Der andere Aspekt, den dieser Mythos ausblendet, sind die kräftezehrenden Auswirkungen, die von einer Sicherheitslücke ausgehen können. Möglicherweise ist Ihr Unternehmen wirklich nur von einer Sicherheitslücke betroffen. Aber schon eine einzige Sicherheitslücke kann eine erhebliche Herausforderung darstellen.

Quelle: [8] IDC [9] Ponemon Institute Cost of Cyber Crime Study 2016

3 Wir haben einen IT-Spezialisten eingestellt, damit er sich um die Sicherheit kümmert; wir benötigen daher keine weiteren Kenntnisse

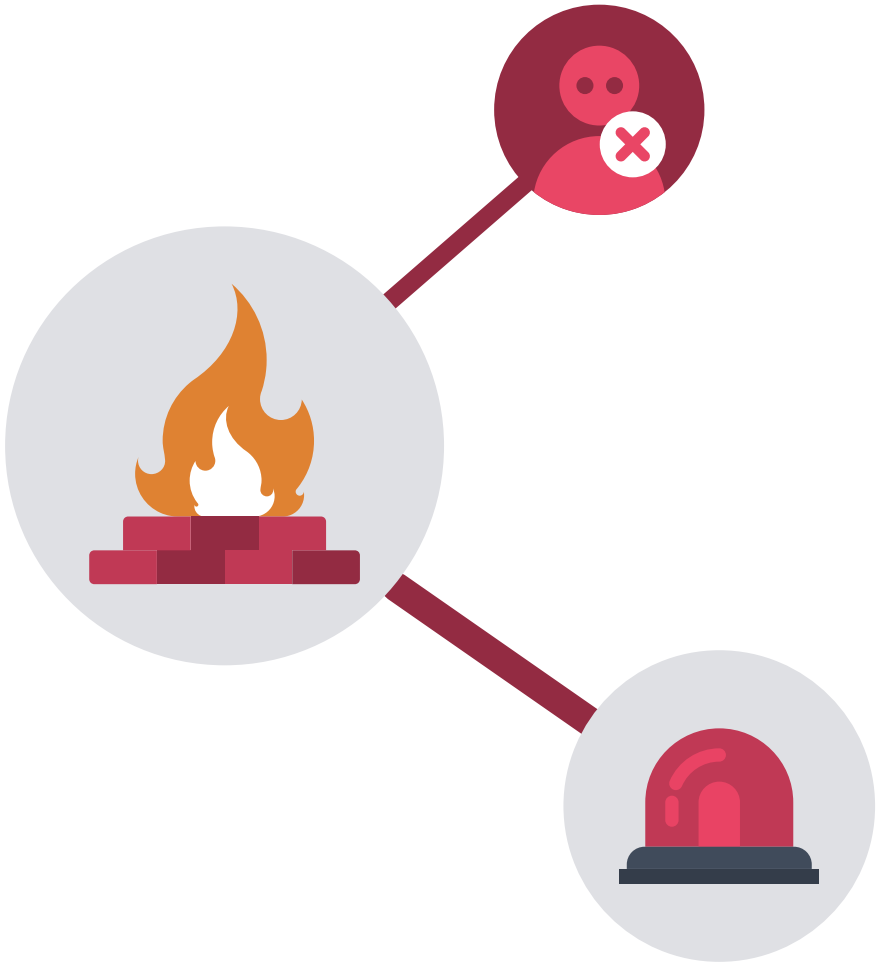
Es ist natürlich eine gute Idee, einen Spezialisten einzustellen, aber auch alle Mitarbeiter sollten im Hinblick auf gute Cybersicherheitspraktiken geschult werden.

Denken Sie an den Kollegen, der nichts ahnend einen bösartigen E-Mail-Anhang herunterlädt oder eine unsichere Website aufruft und damit ein Unternehmensnetzwerk mit Malware infiziert, welche die Computer verlangsamt oder sensible Daten an einen Cyberkriminellen sendet.

Der Cyber Threat Report von CyberEdge für 2016 kommt zu dem Ergebnis, dass Unternehmen das „geringe Sicherheitsbewusstsein unter den Mitarbeitern“ als wichtigstes Problem ansehen, das sie daran hindert, sich selbst vor Sicherheitsbedrohungen zu schützen. Dieser Punkt wurde höher bewertet als „das Fehlen finanzieller Mittel“ und „das Fehlen qualifizierter Fachkräfte“.[10]

Quelle: [10] Ponemon Institute Cost of Cyber Crime Study 2016

4 Unsere Systeme sind mit einer leistungsfähigen Virenschutzsoftware gesichert, sodass wir ausreichend geschützt sind



Virenschutzsoftware funktioniert so, dass sie Systeme nach Malware durchsucht, die von Websites oder durch E-Mails heruntergeladen wurde. Aber Angreifer haben andere Mittel, um diesen Schutz zu umgehen.

Zu den Cyberattacken, die durch Virenschutzsoftware nicht blockiert werden können, zählen unter anderem folgende: Distributed-Denial-of-Service-Attacken (verteilte Überlastangriffe) (DDoS) – das Überfluten einer Website mit Junk-Traffic, sodass diese immer langsamer wird oder gar nicht mehr funktioniert; webbasierte Angriffe, bei denen Hacker einen bösartigen Code in eine Website einschleusen, um auf diese Weise Daten zu stehlen oder auszuspähen; und der Zugriff durch Hacker mithilfe gestohlener Geräte.

5 Wenn jemand in unser Netzwerk eindringt, bemerken wir es sofort

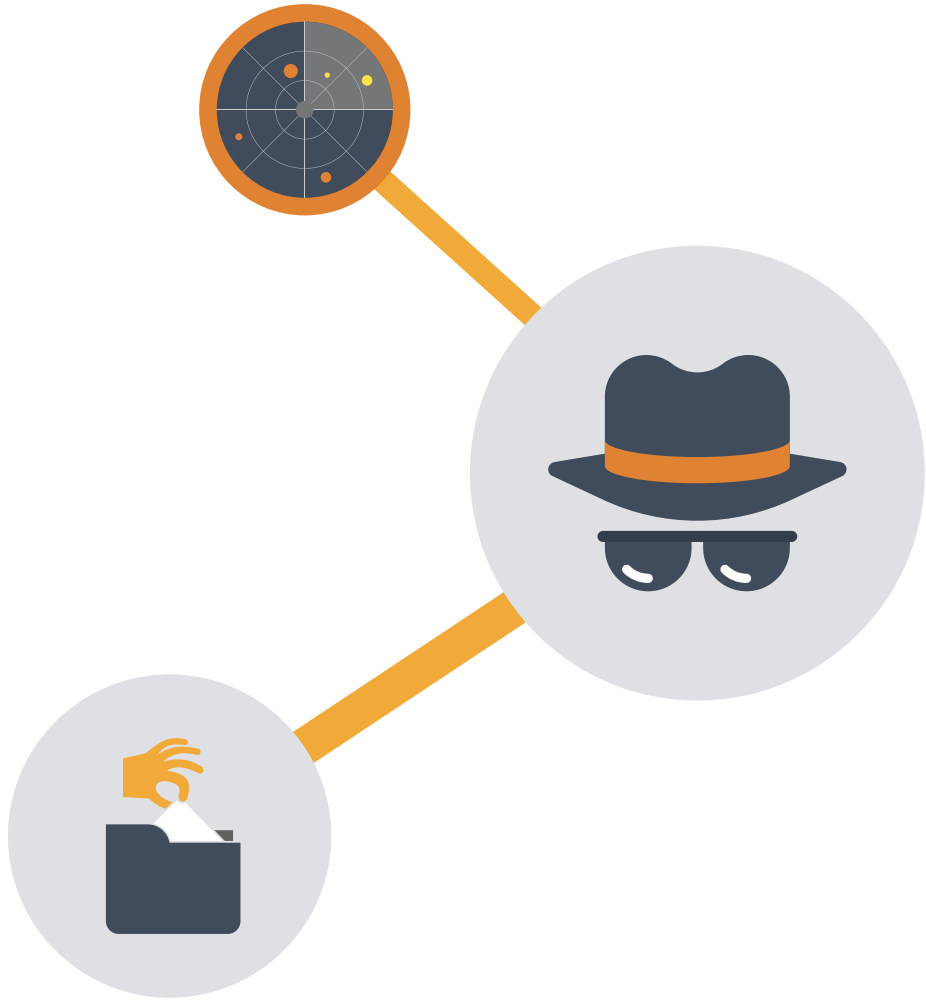
Es ist nicht leicht, einen Cyberangriff zu entdecken. Malware, die in ein System eindringt, muss nicht sofort den Betrieb stören; stattdessen kann sie das System ausspähen und dem Hacker Informationen liefern, mit deren Hilfe dieser noch gezieltere Angriffe planen kann, häufig, um Zugriff auf das gesamte Netzwerk zu erlangen.

Solche Attacken auf bestimmte Systeme werden als „fortgeschrittene, andauernde Bedrohungen“ (Advanced Persistent Threats, APT) eingestuft. APT-Attacken bedeuten, dass Daten aus einer bestimmten Computerinfrastruktur überwacht und abgerufen werden, und zwar kontinuierlich, über einen längeren Zeitraum und in der Regel unbemerkt.

Nach Schätzungen des IT-Beratungskonzerns Daisy Group könnte die Hälfte der britischen Unternehmen in weniger als einer Stunde gehackt werden.

TIPP:
Um einen Datendiebstahl festzustellen, ist es hilfreich zu überwachen, ob der ausgehende Datenverkehr den üblichen Umfang übersteigt – möglicherweise handelt es sich dabei um einen APT-Angriff.

WERDEN SIE TÄTIG:
Entscheiden Sie sich für Sicherheitssoftware mit Datenschutz, wie zum Beispiel HP SureStart, die automatisch – wenn ein Malware-Angriff festgestellt wird – das BIOS eines Computers wiederherstellt und damit Sicherheitsverletzungen stoppt, bevor Daten betroffen sind.

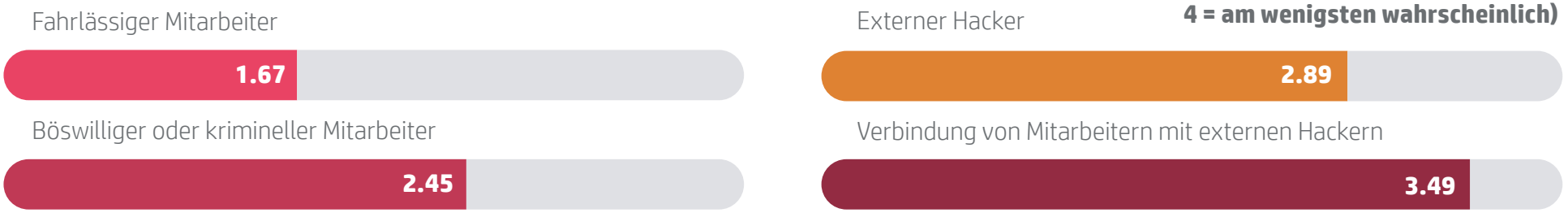


Wo liegt der Ursprung der Gefahren?

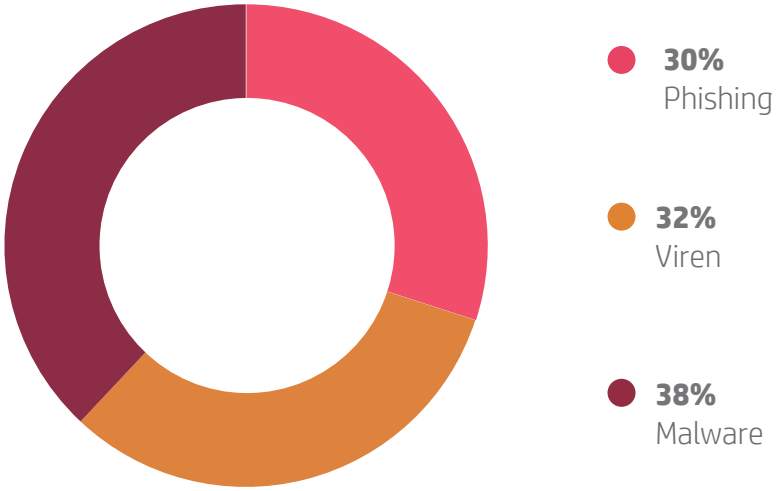
Der Schutz Ihres Netzwerks beginnt damit, dass Sie Ihre größten Schwachstellen kennen.

Die wahrscheinlichste Ursache einer Datenschutzverletzung:[11]

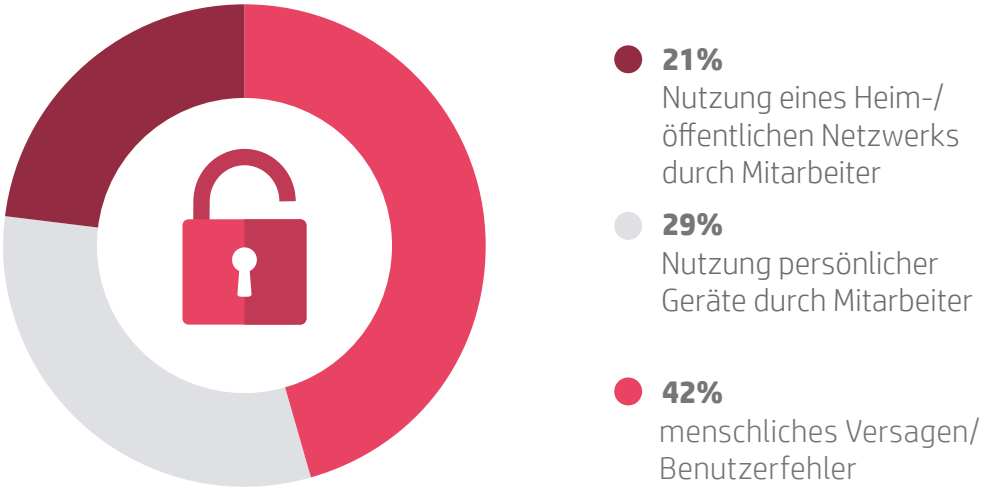
(1 = sehr wahrscheinlich, 4 = am wenigsten wahrscheinlich)



Die üblichsten Formen externer Bedrohungen:



Wie interne Datenschutzverletzungen auftreten:[12]



Quelle: [11] http://www.kilpatricktownsend.com/_assets/Kilpatrick%20Townsend%20Report%20Final.pdf [12] Ponemon Institute Cost of Cyber Crime Study 2015

Wie viel kostet die Wiederherstellung nach einer Cyberstraftat?

Die teuersten Arten von Cyberangriffen:

25 %

1.200.000 EUR

Bösartiger Code und Malware

Software, die ein System durch die Schaffung von Sicherheitslücken, die Beschädigung von Dateien oder den Diebstahl von Daten beeinträchtigt (unter anderem Skripte, Viren und Würmer).

24 %

1.125.000 EUR

Distributed Denial of Service (verteilter Überlastangriff)

Gestohlene oder verloren gegangene Geräte von Mitarbeitern mit Zugang zu Unternehmens-Anmeldedaten können zu Datendiebstahl und Identitätsbetrug führen.

16 %

750.000 EUR

Webbasierte Angriffe

Angriffe, deren Ziel Besucher Ihrer Website sind, zum Beispiel ein eingeschleuster Code, der Browser zu mit Malware infizierten Seiten umleitet.

13 %

610.000 EUR

Gestohlene Geräte

Verloren gegangene Geräte von Mitarbeitern mit Zugang zu Unternehmens-Anmeldedaten können zu Datendiebstahl und Identitätsbetrug führen.

9 %

360.000 EUR

Phishing und Social Engineering

E-Mails oder Pop-up-Fenster, die den falschen Anschein erwecken, rechtmäßig die Anmeldedaten abzufragen.

9 %

422.000 EUR

Böswillige Mitarbeiter

Mitarbeiter, die sensible Daten preisgeben.

4 %

187.000 EUR

Botnets

Netzwerke infizierter Computer, die gesteuert werden, um bösartige Aktivitäten, zum Beispiel Versandaktivitäten auszuführen.

Quelle: [13] Ponemon Institute, [2015] Cost of Cyber Crime study (Studie über die Kosten von Cyberkriminalität)

Die Auswirkungen der Cyberkriminalität auf Unternehmen

Die wahren Kosten der Cyberkriminalität liegen weit höher als die Reparaturkosten eines Hacks.

Sicherheitsverletzungen sind unglaublich teuer. Vereinfacht gesagt gibt es drei Wege, wie eine Sicherheitsverletzung sich auf die Finanzen Ihres Unternehmens auswirken könnte.

Unternehmensressourcen

Es ist klar, dass Sie die Dinge wieder in Ordnung bringen müssen. Dafür ist ein erheblicher Arbeitsaufwand erforderlich und es entstehen hohe Kosten. Dies bedeutet, dass Sie andere Arbeiten – die Gewinn erwirtschaften würden – auf Eis legen müssen.

Bußgelder/Strafmaßnahmen

Wegen Verstoßes gegen gesetzliche Vorschriften (z. B. der Health Insurance Portability and Accountability Act, HIPAA) müssen Sie gegebenenfalls ein Bußgeld zahlen. Mit dem Inkrafttreten der europäischen Datenschutz-Grundverordnung (EU DSGVO/GDPR) im nächsten Jahr können Unternehmen, denen Fahrlässigkeit nachgewiesen wird, zu einer Gesamtgeldstrafe von 4 % ihres weltweiten Umsatzes verurteilt werden. Es besteht sogar die Gefahr von Rechtsstreitigkeiten, wenn die Datenpanne zu einer Verletzung der Geheimhaltungsverpflichtungen gegenüber Mandanten/Kunden geführt hat.

Rufschädigung

Dies kann eine der schädlichsten Auswirkungen einer Sicherheitsverletzung sein. Kunden, die Presse und die breite Öffentlichkeit haben ein langes Gedächtnis für Sicherheitsverstöße. Es kann lange dauern, bis das Vertrauen wiederhergestellt ist.

Anatomie des unerwarteten Hackerangriffs

Als Sony Pictures im Jahr 2014 gehackt wurde, nahmen die Hacker einfach den Weg durch die Eingangstür.[14]

Nach Angaben von „Lena“ von der Hackergruppe „Guardians of Peace“ (GOP - Wächter des Friedens) – die die Verantwortung für die Attacke übernommen hat – „unternimmt Sony nichts mehr, um die physische Sicherheit zu gewährleisten“. Die Gruppe erlangte Zugriff auf das Netzwerk von Sony, indem jemand persönlich in das Gebäude gegangen ist und die Computer-Zugangsdaten eines Systemadministrators gestohlen hat.

Nachdem sie in das Netzwerk eingedrungen waren, schleusten sie Malware ein, die ihnen private Dateien, den Quellcode und Kennwörter für Oracle- und SQL-Datenbanken verschaffte. Von dort stahlen sie Filmproduktionspläne, E-Mails, Finanzdokumente und anderes – und veröffentlichten vieles davon im Internet.

Die Hacker drohten, weitere geheime und streng geheime Daten zu veröffentlichen, wenn das Unternehmen den Film „Das Interview“ nicht aus den Kinos zurückzieht.

Sony kapitulierte schließlich, verlor damit Einnahmen aus dem Verkauf von Kinokarten in beträchtlicher Höhe und erlitt einen unglaublichen Reputationsschaden.

Sony hat zwei Fehler gemacht. Das Unternehmen hatte keine Vorkehrungen getroffen, um den physischen Zugriff auf Unternehmensdaten durch Eindringlinge zu verhindern, und es hatte nicht in ein mehrschichtiges Sicherheitssystem investiert, das nach der ersten Sicherheitsverletzung den Zugriff auf sensible Daten hätte verhindern können.

Sicherheitsexperte Bruce Schneier schrieb dazu nach der Attacke: „Ist ein Angreifer ausreichend qualifiziert, mit den entsprechenden Mitteln ausgestattet und motiviert, dann sind alle Netzwerke verwundbar“. Der Trick besteht darin zu erkennen, wo Ihr Netzwerk angreifbar ist. Das kann die Eingangstür sein.

WERDEN SIE TÄTIG:
Erstellen Sie für jede Abteilung – von der IT-Abteilung bis zum Kundendienst – einen Plan zur Reaktion auf Sicherheitsverletzungen, um die Zeit zur Behebung des Schadens zu minimieren.

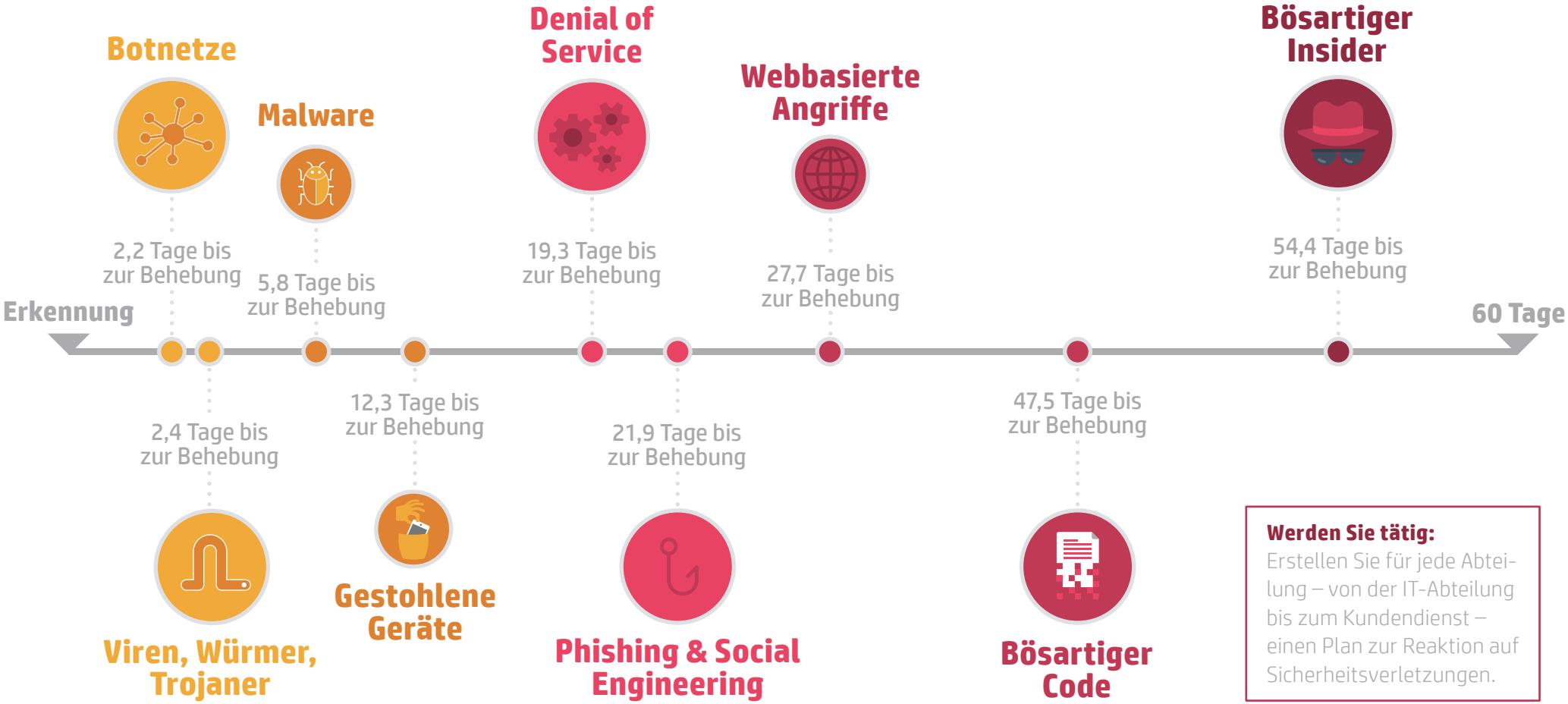
TIPP:
Viele Formen von Malware werden in Form von E-Mail-Anhängen weitergeleitet. Schulen Sie Ihre Mitarbeiter, damit diese verdächtige Dateien erkennen, welche auf den ersten Blick wie rechtmäßige Dokumente aussehen.

- Geschätzte Kosten für Unternehmen aufgrund von Cyberkriminalität: 22,4 Mrd. EUR[15]
- Durchschnittliche Kosten für ein deutsches Unternehmen aufgrund von Cyberkriminalität im Jahr 2016: 7,84 Mio. EUR[16]
- Deutsche Unternehmen, die für 2017 eine Verletzung der Datensicherheit befürchten: 51%[17]

Quelle: [14] http://www.businessinsider.com/how-the-hackers-broke-into-sony-2014-12?IR=T [15] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
[16] https://www.statista.com/statistics/293274/average-cyber-crime-costs-to-companies-in-selected-countries/ Stat is $7.21m – have converted to £
[17] https://www.gov.uk/government/news/two-thirds-of-large-uk-businesses-hit-by-cyber-breach-or-attack-in-past-year

Cyberkriminalität: die Wiederherstellungszeit

Wie lange dauert es, den Schaden einer Datenverletzung zu reparieren? Das Ponemon Institute[18] schätzt durchschnittlich 46 Tage - ein Zeitraum, der das Aus für jedes KMU bedeuten kann.



Werden Sie tätig:
Erstellen Sie für jede Abteilung – von der IT-Abteilung bis zum Kundendienst – einen Plan zur Reaktion auf Sicherheitsverletzungen.

Quelle: [18] Ponemon Institute Cost of Cyber Crime Study 2015

So schützen Sie Ihr Unternehmen vor Cyberkriminalität

Wichtige Tipps und Strategien für die Cybersicherheit von Unternehmen

Hier finden Sie sechs häufige Ziele für Hacker, die in Unternehmenssysteme eindringen – und was Sie jetzt dagegen tun können.

Kunden-datenbanken

Cloud-Dienste

Smartphones und Tablets von Mitarbeitern

Menschliches Fehlverhalten

Internet der Dinge

Netzwerk-zugänge

Da wir uns immer mehr in Richtung einer digitalen Welt bewegen, in der Daten einen höheren Wert besitzen als je zuvor, kann die Cyberkriminalität viele Formen annehmen. Cyberkriminelle sind häufig auf Informationen aus und angesichts einer wachsenden Zahl vernetzter Geräte, die am Arbeitsplatz genutzt werden – von Smartphones und Tablets bis hin zu WLAN-Druckern – gibt es immer mehr Zugriffspunkte, die Hacker anvisieren können.

1 Kundendatenbanken

Finanzdaten sind bei weitem nicht das einzige Ziel von Hackern – Informationen, wie zum Beispiel Namen und E-Mail-Adressen können zum Identitätsdiebstahl, zum Versenden von Spam oder zum Hacken anderer Konten genutzt werden.

Ein lohnendes Ziel für ernsthafte Hacker besteht darin, Unternehmen zu „knacken“, die mit noch größeren Unternehmen verbunden sind. Stellen Sie sich das digitale Äquivalent eines Einbruchs in einen Baumarkt vor, nur um Zugang zu einer Kellerwand zu erhalten, auf deren Rückseite sich der Tresorraum einer benachbarten Nationalbank befindet.

Wenn die Angreifer sich erst einmal in einem kleineren System befinden, sind sie besser positioniert, sich Zugang zu den Kundendaten des verbundenen Großunternehmens zu verschaffen. Wie kann Ihrer Kundendatenbank Schaden zugefügt werden? Viren, Würmer und trojanische Pferde, die von bösartigen Websites oder aus E-Mails heruntergeladen wurden, können den Code freigeben, den Hacker zum Einbruch und Datendiebstahl benötigen.

So schützen Sie die Daten Ihrer Kunden

- Nutzen Sie für Unternehmen entwickelte Sicherheitssoftware, die Ihnen Netzwerk-, E-Mail- und Endpunktschutz bietet.
- Aktualisieren Sie regelmäßig Ihre Sicherheitssoftware, um weiterentwickelte Malware zu blockieren.
- Laden Sie Software-Updates für Ihre Systemprogramme herunter, da ältere Programme Schwachstellen enthalten können, die Angreifer möglicherweise ausnutzen.

2 Cloud-Dienste

So schützen Sie die Informationen in der Cloud

- Verschlüsseln Sie Ihre wichtigsten Informationen mithilfe von Programmen wie Smartcrypt von PKWARE, das basierend auf Zugangsrichtlinien die Komplexität für die Verschlüsselung festlegt. Auf diese Weise sehen berechtigte Nutzer die Daten, die sie sehen sollen – und unbefugte Nutzer sehen gar nichts.
- Erstellen Sie ein starkes Kennwort für Ihr Cloud-Konto. Legen Sie außerdem in den Einstellungen für Ihr Cloud-Konto genau fest, wer auf Ihre Daten zugreifen kann und was diese Personen mit den Daten machen dürfen.
- Fordern Sie eine Zwei-Faktor-Authentifizierung – zum Beispiel einen Smartphone-Code und ein Kennwort – um Änderungen an den Cloud-Daten vorzunehmen, wie etwa das Herunterladen, Löschen oder Verschieben von Dateien.

Cloud-Computing ist zu einer Säule der Unternehmensinfrastruktur geworden.

Der IDG-Cloud-Computing-Umfrage aus dem Jahr 2016[19] zufolge haben 70 Prozent der Unternehmen mindestens einen Teil ihrer Infrastruktur in die Cloud verlegt, während Tripwire zu dem Ergebnis kam, dass 90 Prozent die Cloud für ihre Infrastruktur und/oder für die Datenspeicherung nutzen – einschließlich geschäftskritischer Daten.[20]

Natürlich bestehen Sicherheitsbedenken, aber in Wirklichkeit sind die Daten in der Cloud in der Regel sicherer – gespeichert auf Servern außerhalb des Firmengeländes von einem Unternehmen, dessen Ruf davon abhängt, wie es die Sicherheit der Daten gewährleistet.

Deshalb halten 64 Prozent der von Tripwire befragten Unternehmen die Cloud für sicherer als traditionelle Systeme.

Glücklicherweise ist dieses Vertrauen nicht ungerechtfertigt: Laut der BIS-Umfrage von 2015[21] wurden gerade sieben Prozent der Unternehmen (große und kleine) Opfer einer schwerwiegenden Sicherheitsverletzung im Zusammenhang mit ihren Cloud-Diensten, und diese resultieren hauptsächlich aus Schwachstellen bei Zugriffsrechten oder Kennwörtern. Eine sichere Cloud ist nach wie vor auf eine robuste interne Sicherheitskoordination angewiesen. Denken Sie einfach an die Eingangstür von Sony.

Quelle:
[19] https://www.scribd.com/document/329518100/IDG-Enterprise-2016-Cloud-Computing-Survey
[20] https://www.tripwire.com/state-of-security/security-data-protection/enterprise-impressions-of-cloud-security-in-2016/
[21] 2015 Small Business Survey. Department for Business, Innovation & Skills

3 Smartphones und Tablets von Mitarbeitern

Viele Menschen nutzen ihre persönlichen Geräte auch für berufliche Zwecke.

Viele Menschen nutzen ihre persönlichen Geräte auch für berufliche Zwecke. Richtlinien für BYOD (Bring Your Own Device) sind eine effektive Strategie zur Nutzung von Smartphones, die Mitarbeiter bereits besitzen. Dieser Trend verstärkt sich, innerhalb der nächsten zwei Jahre werden 53,2 Prozent aller Unternehmen eine BYOD-Richtlinie einführen. [22] Aber diese Geräte können ein willkommenes Ziel für Hacker sein.

Schätzungen zufolge enthält jede fünfte Android-App irgendeine Form invasiver Malware, die auf Unternehmensdateien und Systeme übertragen werden könnte, um Aktivitäten zu überwachen oder Informationen zu stehlen.

Diese Gefahr wird größer: 64,9 Prozent der Unternehmen berichten über ein wachsendes Ausmaß der Bedrohungen, die auf ihre Mobilgeräte abzielen.[23]

Mitarbeiter, deren Smartphone gestohlen wird, können dadurch unwissentlich Hackern die Tür öffnen. Ein Telefondieb könnte das Gerät auf dem Schwarzmarkt an einen Hacker verkaufen, der es dann auf Daten durchsucht, um sich Zugang zum Unternehmen des Opfers zu verschaffen oder in die Systeme eines größeren Kunden einzudringen. Unternehmen bewerteten ihre Fähigkeit, sich vor Sicherheitsgefahren zu schützen, die von Mobilgeräten ausgehen, mit 3,54 von 5. Das war die niedrigste Bewertung unter allen potenziellen Ausgangspunkten für Bedrohungen, nach denen sie gefragt wurden.[24]

So sichern Sie die Geräte Ihrer Mitarbeiter

- Installieren Sie ein Softwareprogramm zur Bedrohungserkennung, wie z. B. X-Ray von Duo für Android-Geräte. Damit ist es leichter, gefährliche Apps und verdächtigen Code zu verfolgen.
- Fordern Sie Ihre Mitarbeiter auf, die Remote-Wipe-Funktion ihrer Geräte zu aktivieren (kostenlos für Android, iPhone und Windows Phone und gegen Gebühr auch für BlackBerry erhältlich). Im Falle des Verlusts können so sensible Daten, sowohl geschäftliche als auch persönliche, per Fernlöschung vernichtet werden.
- Weisen Sie Ihre Mitarbeiter an, die Verschlüsselung ihrer Smartphones zu aktivieren, sodass die Daten darauf geschützt sind (bei den neuen iOS und Android Smartphones ist dies Standard).

Quelle: [22] 2016 Cyberthreat Defense Report. CyberEdge [23] ibid [24] ibid

4 Menschliches Fehlverhalten

So helfen Sie Ihren Mitarbeitern

- Schulen Sie Ihre Mitarbeiter in puncto Cybersicherheit und bieten Sie ihnen regelmäßige Weiterbildungen an, damit sie stets über neue Bedrohungen informiert sind.
- Verfassen Sie ein Sicherheitsprotokoll, das speziell auf Ihr Unternehmen und die Datenarten, die es verarbeitet, abgestimmt ist.
- Bilden Sie eine Arbeitsgruppe, deren Aufgabe es ist, Mitarbeiter, Kunden und Geschäftspartner über Ihre Cybersicherheitsrichtlinien zu informieren.

Gute Kennwortregeln sind die wichtigste Grundlage für Cybersicherheit. Und dennoch lassen sich 31 Prozent der schlimmsten Sicherheitsvorfälle im Jahr 2015 auf das Verhalten von Mitarbeitern zurückführen.

Vom Hacken schwacher Kennwörter über den Diebstahl von Dokumenten, die per E-Mail über ungesicherte Verbindungen versandt wurden, bis hin zu Phishing-E-Mails, die auf bestimmte Mitarbeiter abzielen – Angreifer nutzen häufig menschliches Fehlverhalten.

5 Bereiten Sie sich auf das Internet der Dinge vor

Das Forschungsunternehmen IDC prognostiziert, dass 2020 die Anzahl der mit dem Internet verbundenen Geräte 30 Milliarden erreichen wird – ein Anstieg von schätzungsweise 13 Milliarden im Vergleich zum heutigen Stand[25]

Während Bürocomputer zumindest durch Kennwörter und idealerweise auch durch ein Sicherheitsprogramm geschützt sind, fehlen bei Druckwarteschlangen und Druckaufträgen häufig entsprechende Sicherheitsvorkehrungen – auch könnte die wachsende Anzahl der Mobilgeräte und die Zunahme der Telearbeit bedeuten, dass nicht alle persönlichen Geräte so gesichert sind, wie sie es sein sollten.

Solche ungesicherten Drucker – und andere vernetzte Geräte – können Opfer von „Sniffern" (Schnüffelprogrammen) werden, die Druckaufträge, aber auch den Netzwerkverkehr, Benutzernamen und Informationen über Kennwörter aufzeichnen können, um sie dann zu dem für den Cyberangriff genutzten Server zurückzusenden.

Beachten Sie auch den Hinweis, dass der in den Medien vielbeachtete Angriff auf Dyn Berichten zufolge im Zusammenhang mit internetfähigen CCTV-Kameras stand, die alle von einem Unternehmen, von XiongMai Technologies, hergestellt wurden. Nach Angaben der Sicherheitsfirma Flashpoint.

Dieses Beispiel zeigt, dass jedes Gerät in Ihrem Netzwerk ein Endpunkt ist und Ihr Netzwerk ist nur so stark wie das am wenigsten gesicherte Gerät. Etwa 97 Prozent der Unternehmen treffen Sicherheitsvorkehrungen für Bürocomputer und Laptops, für mobile Geräte 77 Prozent, aber nur bei 57 Prozent der Unternehmen sind Sicherheitsvorkehrungen für Drucker in Kraft.

TIPP:

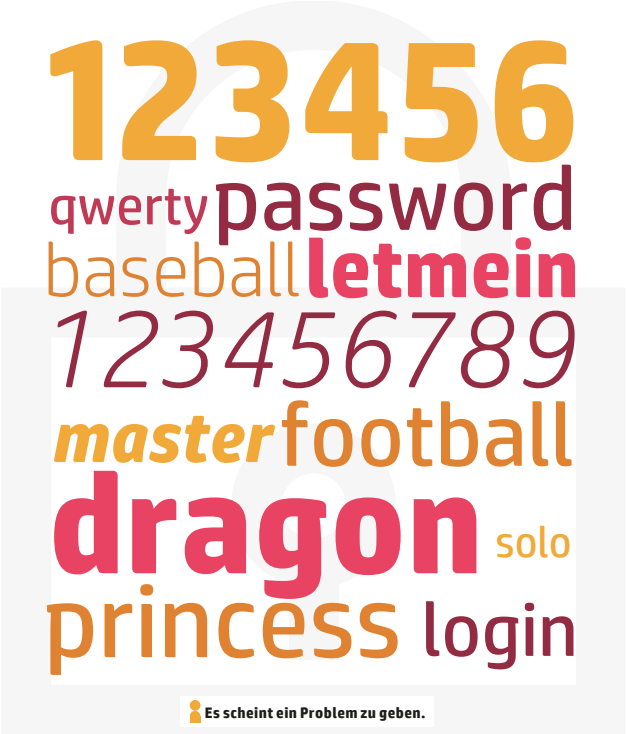
- Entfernen oder deaktivieren Sie nicht benötigte Funktionen auf Geräten, da mehr Funktionen mehr Zugriffsmöglichkeiten für Angreifer bieten können.

Quelle: [25] Turnaround and transformation in cybersecurity [Trendwende und Wandel bei der Cybersicherheit], PwC: The Global State of Information Security Survey 2016 [26] HPI Printer Security Research, Spiceworks 2016

Passwörter und Ransomware

Die gängigsten Passwörter

Anfang 2013 knackte ein Ars Technica Reporter, der weder Erfahrung als Cyberkrimineller noch mit Passwort-geschützten-Systemen hatte, 8.000 von mehr als 16.000 verschlüsselten Passwörtern in nur einem Tag*. Welche Chance haben also die gängisten Passwörter gegen einen versierten Hacker?



Was ist Ransomware?

Cyberkriminelle nutzen immer öfter Ransomware, eine Form von Malware, die ein System lahmlegt und nur mit Lösegeld aufgehoben werden kann. Tausende waren 2013 betroffen als ein Trojaner namens Cryptolocker auch die Aufmerksamkeit der britischen Kriminalpolizei und ihrer Abteilung für Cyberkriminalität auf sich zog. So funktionieren diese Angriffe im Detail:

	1. Installation	Ein schädlicher Code nistet sich, nach einem unbeabsichtigten Download nach dem Öffnen einer E-Mail oder einer bösartigen Website, auf Ihrem Computer ein.
	2. Benachrichtigt den Versender	Die Ransomware verbindet sich mit ihrem Home-Server und empfängt einen Verschlüsselungsschlüssel.
	3. Verschlüsselt Ihre Daten	Die Ransomware liest die Daten in Ihrem Netzwerk und verschlüsselt sie. Das macht sie unlesbar.
	4. Erpressung	Meistens erscheint eine Nachricht auf dem betroffenen Computer. Sie stellt ein Ultimatum bis zu dem das Lösegeld gezahlt werden muss um die Daten zu entschlüsseln.
	5. Lösegeldzahlung	Der Geschädigte kann Bitcoin erwerben um den Erpresser zu bezahlen. Dieser schaltet im besten Fall die Daten wieder frei.

* Splashdata

6 Netzwerkzugänge

Wenn Hacker Zugang zu einem Netzwerk erhalten wollen, können sie einen DDoS-Angriff starten. Dabei werden Tausende mit Malware infizierte Computer verbunden und dazu genutzt, so viel Junk-Traffic zu generieren, dass das ganze Netzwerk unter der Last des Angriffs zusammenbricht.

DDoS-Angreifer wollen Standortadministratoren mit einem „hängenden" System häufig einfach nur ablenken, damit sie unbemerkt Daten stehlen oder Malware installieren können, um zukünftige Datenraubzüge zu planen. Manche DDoS-Angriffe sind auch den sogenannten „Scriptkiddies" geschuldet. Dabei handelt es sich um meist jugendliche, unerfahrene Hacker, die es einfach als Herausforderung ansehen, eine Website außer Betrieb zu setzen. Bereits wenige Stunden, in denen eine Website nicht funktioniert, können schwere Konsequenzen für die Umsätze und den Ruf eines Unternehmens haben.

TIPP:
Investieren Sie in Hardware, die über eingebaute Sicherheitslösungen verfügt, wie z. B. fortgeschrittene Authentifizierungs- und Verschlüsselungsfunktionen.

So schützen Sie Ihr Netzwerk

- Setzen Sie Systeme ein, die den ein- und ausgehenden Verkehr in Ihrem Netzwerk überwachen. Ein plötzlicher Anstieg könnte auf einen Angriff hinweisen, während ein ständiger, unerklärlicher Datenverkehr einem Trojanerprogramm geschuldet sein könnte, das Daten an den Server der Cyberkriminellen weiterleitet.
- Filtern Sie den gesamten Datenverkehr, sodass nur der Verkehr, der für Ihr Unternehmen wichtig ist, Zugang zu Ihrem Netzwerk erhält.
- Sorgen Sie dafür, dass alle Router, Schalter und sonstigen Netzwerkgeräte dieselbe Software- und Funktionsgrundlage haben und installieren Sie immer die neuesten Software-Updates.

Die Zukunft der Cybersicherheit in Unternehmen

Da Unternehmen stark von ihrer Internetpräsenz abhängig sind, wird es immer wichtiger, solide Maßnahmen zum Schutz der Cybersicherheit zu etablieren.

Heutzutage bringen Mitarbeiter ihre eigenen Geräte mit zur Arbeit. Unternehmer nutzen Cloud-Computing-Plattformen und gliedern wichtige technische Dienstleistungen an externe Anbieter aus. 12% der deutschen Berufstätigen arbeiten im Home Office. Die Cybersicherheit stellt Sie damit vor immer größere Herausforderungen, wenn Sie weder die Geräte, die Infrastruktur noch das Arbeitsumfeld kontrollieren.

Andererseits haben wir – seit wir Smartphones nutzen – gelernt, dass man wirklich von überall aus und zu jeder Zeit Geschäfte machen kann. Ein Café eignet sich dazu genauso gut wie ein Büro. Wir verlassen uns auf öffentliche WLAN-Netzwerke, um riesige Mengen an geschäftlichen und persönlichen Daten zu verarbeiten – häufig auch über Smartphones, die schlecht gesichert sind. Den Cyberkriminellen ist dieser Trend natürlich bereits aufgefallen. Die Sicherheit leidet, wenn wir nicht auf das Umfeld unserer Arbeit achten.

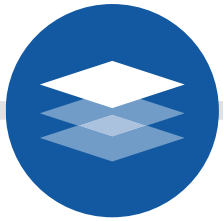
In den kommenden Jahren wird es definitiv nicht mehr ausreichen, unsere Geräte mit einem Virenschutzprogramm auszustatten oder alle sechs Monate die Kennwörter zu aktualisieren. Stattdessen werden Unternehmen ausgereifte Sicherheitsvorkehrungen treffen müssen, die an externen Standorten genauso funktionieren wie in einem Büro unter der Kontrolle eines IT-Administrators.

Für die verzweigten Unternehmen von morgen ist die Cybersicherheit von aufschlussreichen Analysen abhängig, durch die ungewöhnliche Vorkommnisse erkannt und isoliert werden können. Darüber hinaus wird eine mehrstufige Sicherheitsstruktur benötigt, die alle Zugangspunkte schützt.

Die Zukunft der Cybersicherheit in Unternehmen

Analytik: Der Cybersicherheitsdetektiv

Selbst wenn Ihre Website nicht häufig besucht wird, lassen sich im Datenverkehr Muster erkennen. Der Einsatz von Analysesoftware, die Aktivitäten misst und dokumentiert, erleichtert es zu erkennen, wenn etwas nicht stimmt. Diese Programme funktionieren, indem sie zuerst den Normalzustand verfolgen und dokumentieren, um später Abweichungen erkennen zu können. Wird eine solche Abweichung festgestellt, können die Administratoren in die Offensive gehen und die Angriffe abwehren, bevor diese die Gelegenheit haben, ein Chaos im Netz anzurichten.



Schichtenarchitektur: Den Angreifern einen Schritt voraus

Das mehrschichtige Sicherheitskonzept wird auch als „tief gestaffelte Verteidigung" bezeichnet und schützt die Zugangspunkte durch eine Anzahl verschiedener Methoden. Dazu zählen häufig SSL-Zertifikate mit erweiterter Validierung, mit denen es schwieriger ist, Anmeldedaten zu fälschen, um in ein gesichertes Netzwerk einzuloggen. Es kann auch zweckmäßig sein, dieses Verfahren mit einer Multifaktor-Authentifizierung zu kombinieren, bei der die Hacker mehr als nur ein einzelnes Kennwort knacken müssen.

Unabhängig von den spezifischen Technologien, die eingesetzt werden, besteht das Prinzip einer Schichtenarchitektur darin, dass jeder sensible Bereich Ihres Unternehmensnetzwerks individuell geschützt ist. Für Ihre Nutzer und Geschäftspartner wird es vielleicht etwas aufwendiger, Zugang zu wichtigen Daten zu erhalten, doch diese minimalen Einbußen in Sachen Bequemlichkeit sollten dadurch kompensiert werden, dass Sie sich weniger Sorgen um Ihr Geschäft machen müssen.

Jetzt handeln

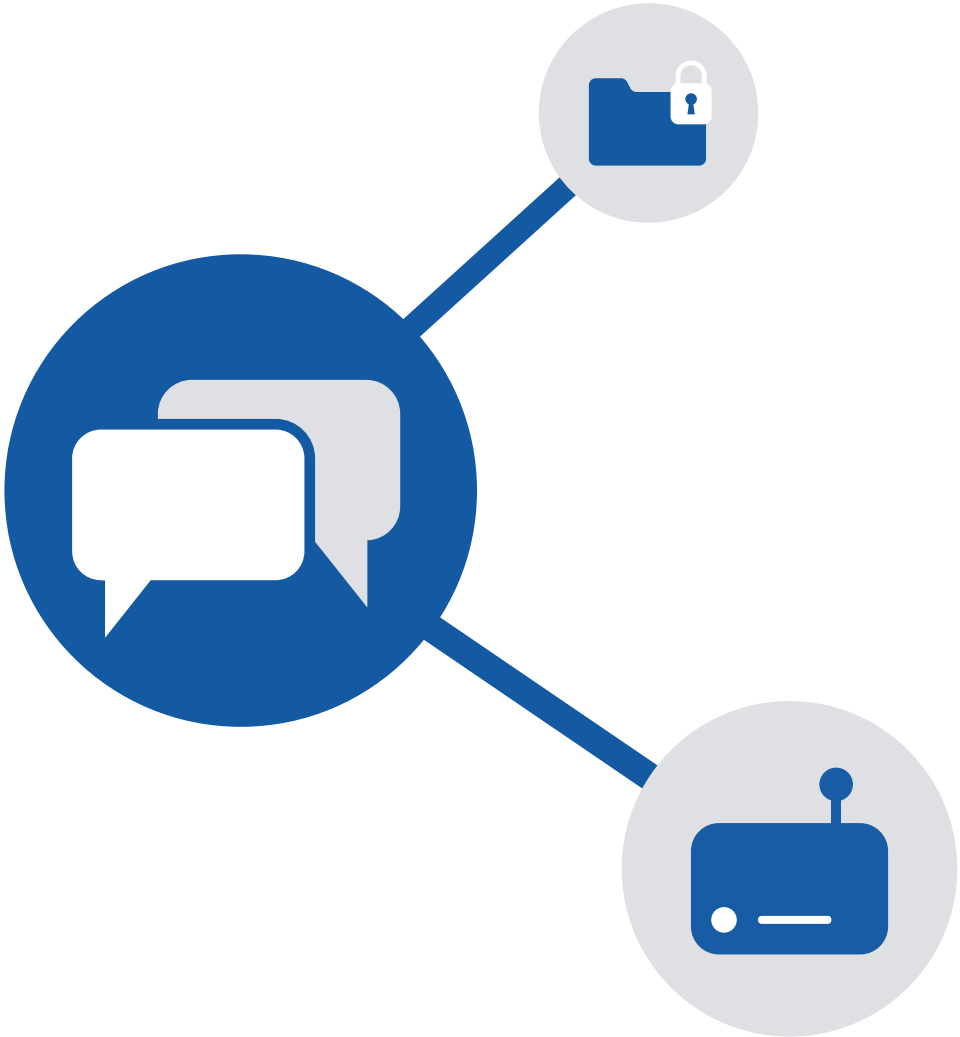
Die beste Verteidigung ist es, in Cybersicherheitssoftware und die entsprechenden Schulungen zu investieren. Beginnen Sie mit einer Überprüfung Ihrer Systeme und Infrastruktur. Tun Sie genug? Was könnten Sie noch verbessern?

Schließlich können Sie auch unsere Sicherheitsexperten hier bei HP Deutschland GmbH kontaktieren. Unsere gemeinsame Wissensbasis ist darauf ausgerichtet, der Bedrohung stets voraus zu sein, nicht nur auf sie zu reagieren. Um mehr zu erfahren, besuchen Sie uns auf hp.de/computer-security.

TIPP:
Verfolgen und dokumentieren Sie zuerst den Normalzustand, um später Abweichungen erkennen zu können.

Überlegungen zur Endpunktsicherheit

Die Sicherung jedes einzelnen Geräts in Ihrem Netzwerk



Nach einer von Spiceworks durchgeführten Sicherheitsstudie stammten die Sicherheitsbedrohungen, denen Unternehmen ausgesetzt sind, hauptsächlich aus folgenden Quellen:

- Laptops und Desktop-Computer: 81 % externe und 80 % interne
- Mobile Geräte 36 % externe und 38 % interne
- Drucker 16 % externe und 16 % interne

Welche dieser Bedrohungen muss besonders dringend beseitigt werden? Alle – das ist die sehr einfache Antwort. Obwohl diese Tatsache absolut offensichtlich ist, gibt es eine besorgniserregende Anzahl von Unternehmen, in denen noch immer nur ausgewählte Geräte ausreichend gesichert werden.

HP vertritt die Ansicht, dass jedes Gerät, das mit Ihrem Netzwerk verbunden ist, gesichert werden muss. Einfach gesagt: Ihr Netzwerk ist nur so sicher wie das am wenigsten gesicherte Gerät.

Die intuitive Logik könnte suggerieren, dass die Sicherung eines vernetzten Druckers nicht so wichtig ist wie die Sicherung all Ihrer Notebooks. Aber das Risiko ist dasselbe. Es ist bekannt, dass Hacker Geräte wie Drucker ins Visier nehmen, oder auch Smart Devices, die mit Ihrem Netzwerk verbunden sind. Denn sie wissen, dass diese Geräte in der Regel nicht besonders gut gesichert sind, aber die gleiche Zugangsstufe zu Ihrem Netzwerk bieten.

Quelle: [27] HP Printer Security Research 2016, Spiceworks

HP: Richtungsweisend in einem neuen Umfeld

Die Cybersicherheit verändert sich. Wir haben die Instrumente, die Ihnen helfen, sich zu verteidigen.

Es gibt keine schnellen Lösungen bei der Cybersicherheit. Eine robuste Verteidigungsstrategie erfordert einen mehrstufigen Ansatz, der Netzwerke, Geräte und Menschen einschließt. Die Auswahl der richtigen Technologie ist ein guter Start.

Bei HP steht Sicherheit an erster Stelle. Unsere HP Elite-Reihe umfasst marktführende Sicherheitsfunktionen, die Sie anderswo vergeblich suchen, wie zum Beispiel HP Sure Start Gen3 – das weltweit erste „selbstheilende" BIOS – und den HP SureView-Datenschutzbildschirm.

HP stattet die Geräte mit folgenden Funktionen aus:

- **HP WorkWise:** Mithilfe von Bluetooth wird das Gerät automatisch gesperrt, wenn Sie weggehen und entsperrt, wenn Sie zurückkommen.
- **HP Multi-Factor Authenticate:** Durch Gesichts- und Fingerabdruckerkennung erhalten nur Benutzer Zugriff, die sich biometrisch authentifizieren können.
- **HP SureView-Bildschirme*:** Die elektronische Blickschutztechnologie begrenzt den Einblickwinkel des IPS-Panels mit einer Tastenkombination und schützt Sie so vor visuellem Datendiebstahl, dem Visual Hacking.
- **HP SureStart – selbstheilendes BIOS:** Jeder HP Elite überwacht alle 15 Minuten sein BIOS. Wird eine Abweichung entdeckt, versetzt das Programm den PC wieder in seinen Originalzustand, wodurch Eindringlinge zurückgewiesen werden.

HP Elite-Computer werden Ihr Unternehmen nicht allein schützen. Aber sie werden eine starke Verteidigungslinie bilden. Hier erfahren Sie mehr über die gesamte HP Elite-Serie.

* Ausgewählte Modelle

HP: Richtungsweisend in einem neuen Druckerumfeld

Schützen Sie Ihr Netzwerk mit der weltweit höchsten Drucksicherheit gegen Angriffe*

„Aufgrund seiner langjährigen Investition in Drucksicherheit ist HP der Anbieter mit dem breitesten und umfassendsten Portfolio an Sicherheitslösungen und -diensten auf dem Markt.“

– Quocirca, Jan. 2017**

HP stattet die Geräte mit folgenden Funktionen aus:

- **Angriffserkennung im laufenden Betrieb (HP run-time intrusion detection):** Die Angriffserkennung im laufenden Betrieb von HP (HP run-time intrusion detection) überwacht Geräte im laufenden Betrieb dann, wenn sie mit dem Netzwerk verbunden sind, also wenn typischerweise die meisten Angriffe erfolgen.
- **Jet Advantage Security Manager:** Bietet der IT-Abteilung optimierte Lösungen, die Sicherheitseinstellungen zu bewerten und – wenn nötig – anzupassen, um dafür zu sorgen, dass die Druckerflotte den Sicherheitsrichtlinien des Unternehmens entspricht.
- **HP SureStart – BIOS mit automatischer Fehlerbehebung:** Beim Neustart erkennt und verhindert HP SureStart die Ausführung schadhaften Codes und nimmt eine automatische Fehlerbehebung des BIOS vor. Es erfolgt ein Neustart auf Basis einer integrierten „Golden Copy“ des BIOS.
- **Whitelisting:** Gewährleistet, dass nur authentischer, bekannter HP-Code in den Speicher geladen wird. Bei Abweichungen startet das Gerät neu, fährt in einen gesicherten Offline-Modus hoch und benachrichtigt die IT-Abteilung.

Quellen: *5 „Höchste Drucksicherheit“ – so das Urteil eines Tests von HP 2016, bei dem die Sicherheitsfunktionen gleichwertiger Drucker verglichen wurden. Nur HP bietet eine Kombination von Sicherheitsfunktionen, die im Überwachungsmodus Angriffe entdecken, diese automatisch abwehren und anschließend beim Neustart die Softwareintegrität prüfen. **Quocirca, “Print security: An imperative in the IoT era”, (Drucksicherheit: unerlässlich im IoT-Zeitalter) quocirca.com/content/print-security-imperative-iot-era, Januar 2017.

Glossar und Literaturhinweise

Zugriffsmanagement-Lösungen

Botnet:
Bezeichnet allgemein ein automatisiertes Computerprogramm, das entwickelt wurde, um ohne Wissen des Eigentümers auf Computer, die mit dem Internet verbunden sind, zuzugreifen und diese zu kontrollieren. Die Computer sind häufig mit Malware infiziert. Hacker setzen Botnets für **Denial-of-Service-Angriffe** auf eine Website ein.

Data Loss Prevention Tools (Programme zur Verhinderung von Datenverlust):
Eine umfassende Gruppe von Computerprogrammen, deren Ziel es ist, sensible Daten zu überwachen und Zugriffs- oder Kopierversuche durch nicht autorisierte Nutzer zu verhindern. Verschiedene Sicherheitslösungen konzentrieren sich entweder auf den Zugriffspunkt (d. h. den Endpunkt) innerhalb eines Netzwerks oder in einem Dateisystem. Gartner zufolge wuchs dieser Markt 2013 **um 25 Prozent**.

Firewall-Technologien:
Ein weiterer breit gefasster Begriff, der einen Gerätetyp beschreibt, der Algorithmen und andere Techniken einsetzt, um unerwünschten Netzwerkverkehr und den Netzwerkzugriff durch unbefugte Nutzer zu verhindern. **Modernere Versionen dieser** Geräte werden leistungsfähig sein, weil sie Funktionen kombinieren, für die bisher verschiedene Geräte erforderlich waren. Dazu zählen zum Beispiel Intrusion Detection Systeme, die Einbruchsversuche erkennen und melden. Firewalls sind in vielen Fällen „anwendungssensibel" und erkennen deshalb den Unterschied zwischen dem Datenverkehr einer Salesforce.com-Implementierung und einer Facebook-Seite.

GRC-Lösungen:
GRC steht für „Unternehmensführung, Risikomanagement und Compliance". Sie beinhalten umfangreiche und abgestimmte Initiativen innerhalb eines Unternehmens, die darauf ausgerichtet sind, betriebliche Vorgänge unter Einhaltung der gesetzlichen Bestimmungen durchzuführen und zu steuern, wodurch im Ergebnis Risiken reduziert werden.

Malware:
Eine umfangreiche Kategorie von Software, die andere Systeme beschädigen oder gänzlich deaktivieren kann. Viren, Würmer und Trojaner sind Beispiele für Malware. Die Ponemon-Studie, die in diesem e-Book mehrfach zitiert wird, unterscheidet zwischen Malware und Viren. Letztere befinden sich laut der Studie „am Endpunkt und haben noch kein Netzwerk infiltriert".

Perimeter-Kontrollen:
Eine allgemeine Kategorie, die sich mit der Abwendung von Cyberrisiken an der Schnittstelle zwischen dem öffentlichen Internet oder anderen öffentlichen Netzwerken und privaten und lokalen Netzwerken beschäftigt. In der **Regel sind mehrere Schichten und verschiedene** Arten von Geräten notwendig.

Phishing:
Wird in der Regel über E-Mail ausgeführt, dabei verlangen die Angreifer die Eingabe von identifizierenden Informationen in ein legitim erscheinendes Dialogfeld.

Richtlinien-Management-Programme:
Im Allgemeinen legen Richtlinien-Management-Programme einen Standard fest, was bestimmte Nutzer sehen dürfen und was nicht, anschließend sorgen sie für die Einhaltung dieser Richtlinie in einem gesamten Netzwerk. Diese Konsistenz soll zumindest theoretisch für mehr Sicherheit sorgen.

Security Intelligence Systeme:
Eine Vielzahl von Security-Intelligence-Programmen kann helfen, Informationen über Bedrohungen zu erfassen und darzustellen. Die Bandbreite reicht von Protokollmanagern bis hin zu Systemen zum Erkennen von Anomalien im Netzwerk.

Glossar und Literaturhinweise

Social Engineering:
Eine Methode, bei der ein Cyberkrimineller einen befugten Nutzer verleitet, Informationen preiszugeben, die er nicht preisgeben dürfte, wodurch ein Hacker Zugang erhält.

Trojanische Pferde:
Trojaner verursachen ähnliche Schäden wie Viren oder Würmer, jedoch müssen sie vom Nutzer installiert werden, weshalb sie meist geschickt getarnt sind. Die Auswirkungen reichen von veränderten Computereinstellungen über Datenverluste bis zum Anlegen einer „Hintertür“, die ein Hacker später nutzen kann.

Verschlüsselungstechnologien:
Programme, die **Daten nur unter Verwendung** eines entsprechenden Dekodierers lesbar machen. Der britische Information Commissioner hat sich in den **letzten Jahren** sehr positiv über verschiedene Verschlüsselungsarten geäußert. In jüngster Vergangenheit war die **Regierung jedoch angesichts massiver** Kritik gezwungen, ihre Meinung zu Verschlüsselungstechnologien zu revidieren.

Viren:
Bösartiger Code, der sich in einem ganzen Netzwerk replizieren und ausbreiten kann.

Webbasierte Angriffe:
In den meisten Fällen wird bei einem webbasierten Angriff ein Browser zu einer schädlichen Website weitergeleitet.

Würmer:
Im Gegensatz zu Viren, die sich verbreiten, wenn die Host-Datei weitergeleitet wird, können sich Würmer unabhängig von einer solchen Host-Datei – z. B. einem Word-Dokument oder einem Excel-Arbeitsblatt – vervielfältigen und deshalb ohne weitere Nutzeraktionen Chaos anrichten. Instant Messaging Programme sind dafür bekannt, Würmer verbreitet zu haben; Skype war 2012 von dieser Schmach betroffen.

4AA7-1085DEE