



CYBERSICHERHEIT UND IHR UNTERNEHMEN

Die Kosten der Cyberkriminalität und wie Sie Ihre Daten schützen

03 | Einführung

05 | Widerlegung von Mythen über Cybersicherheit

13 | Die Auswirkungen der Cyberkriminalität auf Unternehmen

24 | Die Zukunft der Cybersicherheit in Unternehmen

28 | Glossar und Literaturhinweise

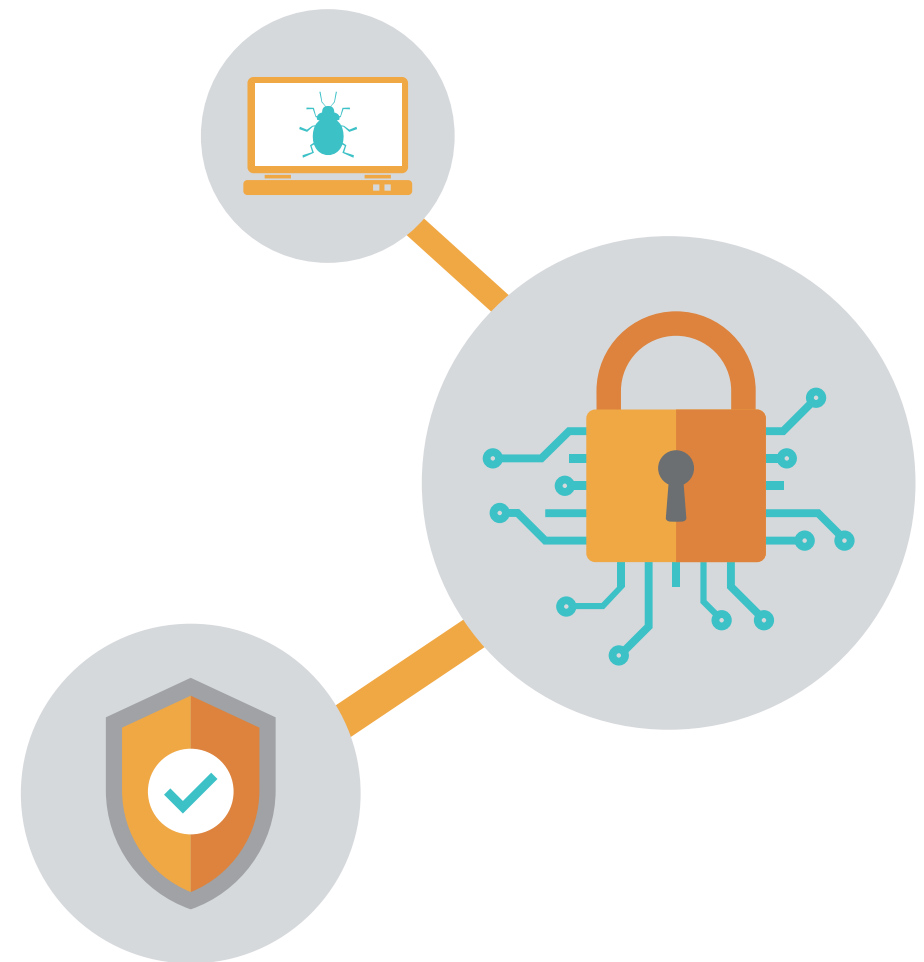
„Viele Führungskräfte erklären Cyberangriffe zu der Gefahr, die unsere Generation prägen wird.“ – Dennis Chesley, Global Risk Consulting Leader, PwC¹

Cybersicherheit ist keine neue Bedrohung. Aber 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 den einfachsten Zugriffspunkt darstellen. Die Ziele werden immer grösser und Störungen nehmen neue Dimensionen an.

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 hat nichts bestätigt, aber es halten sich hartnäckige Gerüchte, dass ein DDoS-Angriff die Ursache war.³





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/Effizienz und 26 Prozent benannten längere Systemausfallzeiten als ein 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 darüber reden, was zu erwarten ist und wie wir uns darauf vorbereiten können.

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 fünf Mythen über die Cybersicherheit, die Unternehmen für Hacker anfällig machen können.



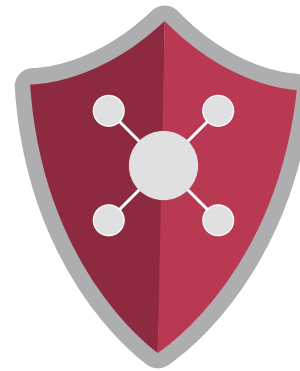
Sicherheits-
verletzungen



Sicherheits-
lücken



Sicherheits-
praktiken



Antivirus-
Software



Cyber-
angriff

1 UNTERNEHMEN KÖNNEN SICH SCHNELL VON JEDEM ANGRIFF ERHOLEN



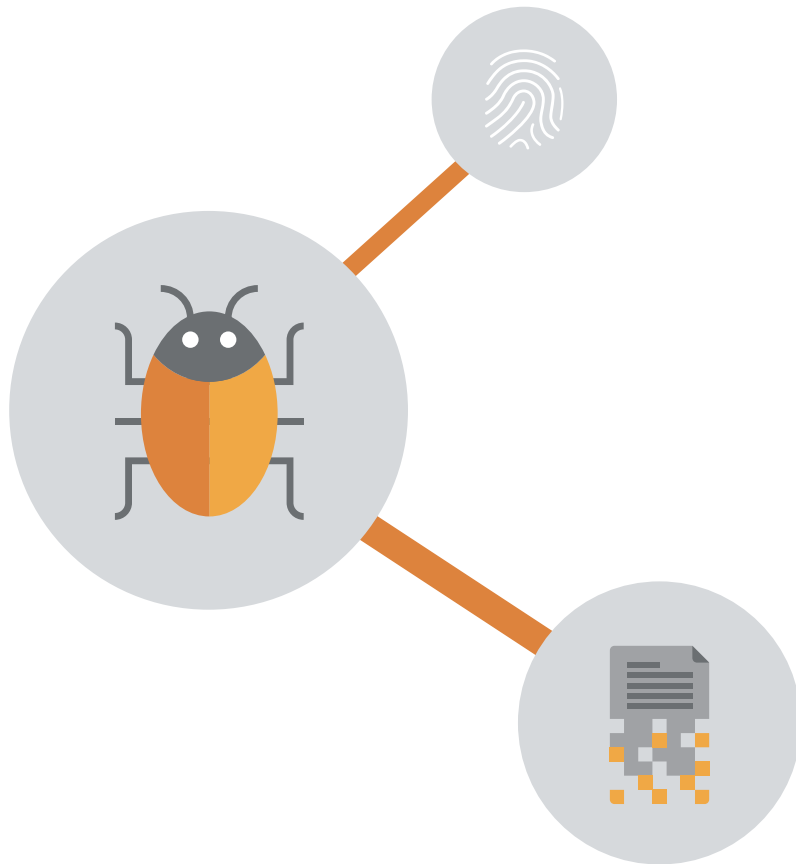
Es ist noch immer sehr schwierig, die Kosten von Angriffen auf die Cybersicherheit für kommerzielle Unternehmen zu messen. Früher nahm man an, dass die Auswirkungen von Angriffen an den sinkenden Aktienkursen zu erkennen seien.

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. Nach einer kürzlich erschienenen Ponemon-Studie stiegen die durchschnittlichen, auf Jahresbasis umgerechneten Kosten eines Angriffs von **USD 7,7 Mio.** 2015 auf **USD 9,5 Mio.** im Jahr 2016.⁷



2 SICHERHEITSLÜCKEN SIND SELTEN, DESHALB IST EIN ERNSTHAFTER SCHUTZ NICHT NOTWENDIG



Die IDC hat ermittelt⁸, dass 2016 der Anteil der Unternehmen, bei denen eine Sicherheitsverletzung aufgetreten ist, 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 können durchaus 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.

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.

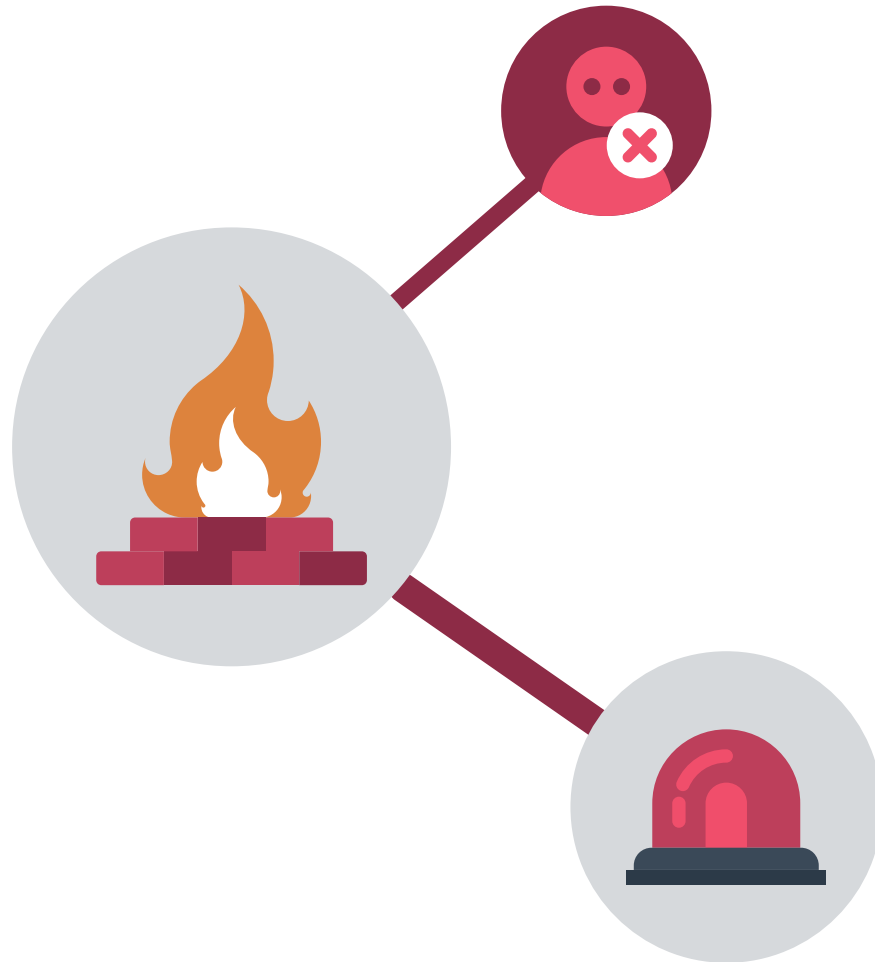
Denken Sie an den Kollegen, der nichts ahnend einen bösartigen E-Mail-Anhang herunterlädt oder eine unsichere Website aufruft und damit ein Unternehmensnetzwerk mit Malware infiziert, die Computer verlangsamt oder sensible Daten an einen Cyberkriminellen sendet.

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 gehindert hat, sich selbst vor Sicherheitsbedrohungen zu schützen. Dieser Punkt wurde höher bewertet als „das Fehlen finanzieller Mittel“ und „das Fehlen qualifizierter Fachkräfte“.¹⁰



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:

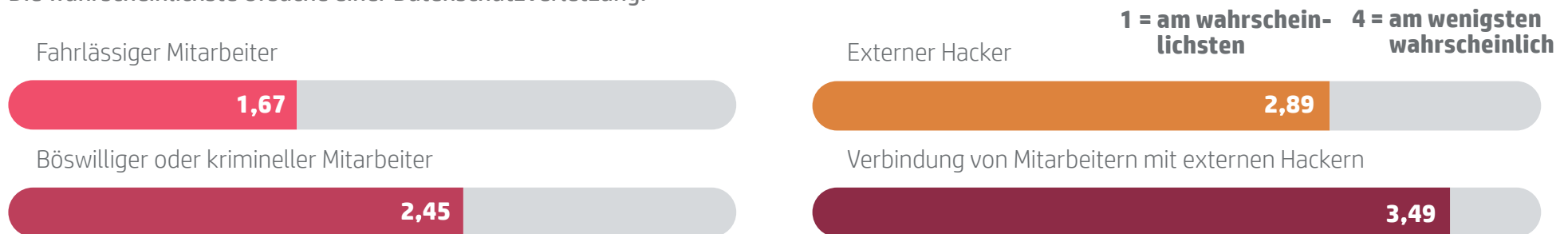
Entscheiden Sie sich für Sicherheitssoftware mit Datenschutz, wie zum Beispiel HP SureStart, die automatisch – wenn ein Malware-Angriff festgestellt wird – das BIOS eines Computers wiederherstellt und damit Sicherheitsverletzungen stoppt, bevor Daten betroffen sind.



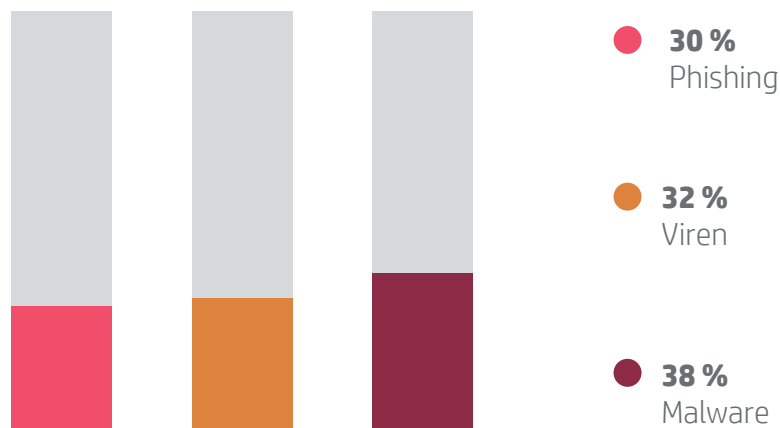
WO LIEGT DER URSPRUNG DER GEFAHREN?

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

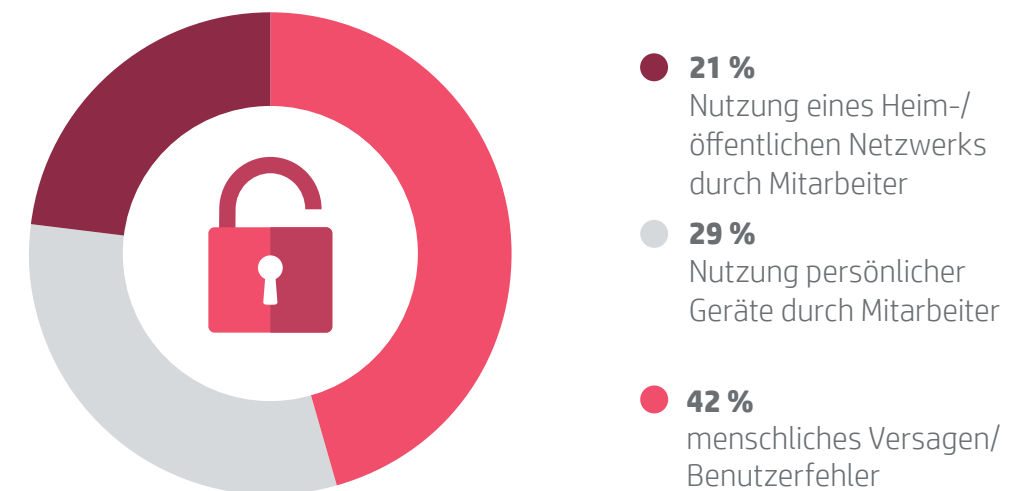
Die wahrscheinlichste Ursache einer Datenschutzverletzung:¹¹



Die üblichsten Formen externer Bedrohungen:



Wie interne Datenschutzverletzungen auftreten:¹²



WIE VIEL KOSTET DIE WIEDERHERSTELLUNG NACH EINER CYBERSTRAFTAT?

Die teuersten Arten von Cyberangriffen:

25 %

1,133,000 EUR

Bösartiger Code und Malware

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

24 %

1,088,000 EUR

Distributed Denial of Service (verteilter Überlastangriff)

„DDoS“-Angriffe sind Fluten von Internetverkehr, welche die Website und die Server eines Unternehmens lahmlegen

16 %

725,000 EUR

Webbasierte Angriffe

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

13 %

589,000 EUR

Gestohlene Geräte

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

9 %

408,000 EUR

Phishing und Social Engineering

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

9 %

408,000 EUR

Böswillige Mitarbeiter

Mitarbeiter, die sensible Daten preisgeben

4 %

181,000 EUR

Botnets

Netzwerke infizierter Computer, die gesteuert werden, um bösartige Aktivitäten, zum Beispiel das Versenden von Spam, auszuführen

DIE AUSWIRKUNGEN DER CYBERKRIMINALITÄT AUF UNTERNEHMEN

Die wahren Kosten der Cyberkriminalität gehen weit über die Kosten für das Beheben der Schäden durch einen Hackerangriff hinaus

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 Arbeitszeitaufwand 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) 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 führt.



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“ (Wächter des Friedens) (GOP) – 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 hat keine Vorkehrungen getroffen, um den physischen Zugriff auf Unternehmensdaten durch Eindringlinge zu verhindern, und es hat 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, die so gestaltet sind, dass sie wie rechtmässige Dokumente aussehen.

Cyberkriminalität: die Wiederherstellungszeit

- Geschätzte Kosten für britische Unternehmen aufgrund von Cyberkriminalität: 21 Mrd. USD¹⁵
- Durchschnittliche Kosten für ein britisches Unternehmen aufgrund von Cyberkriminalität im Jahr 2016: 5,7 Mio. GBP¹⁶
- Britische Unternehmen, die 2015–2016 Opfer einer Sicherheitsverletzung oder eines Angriffs geworden sind: 66 %¹⁷

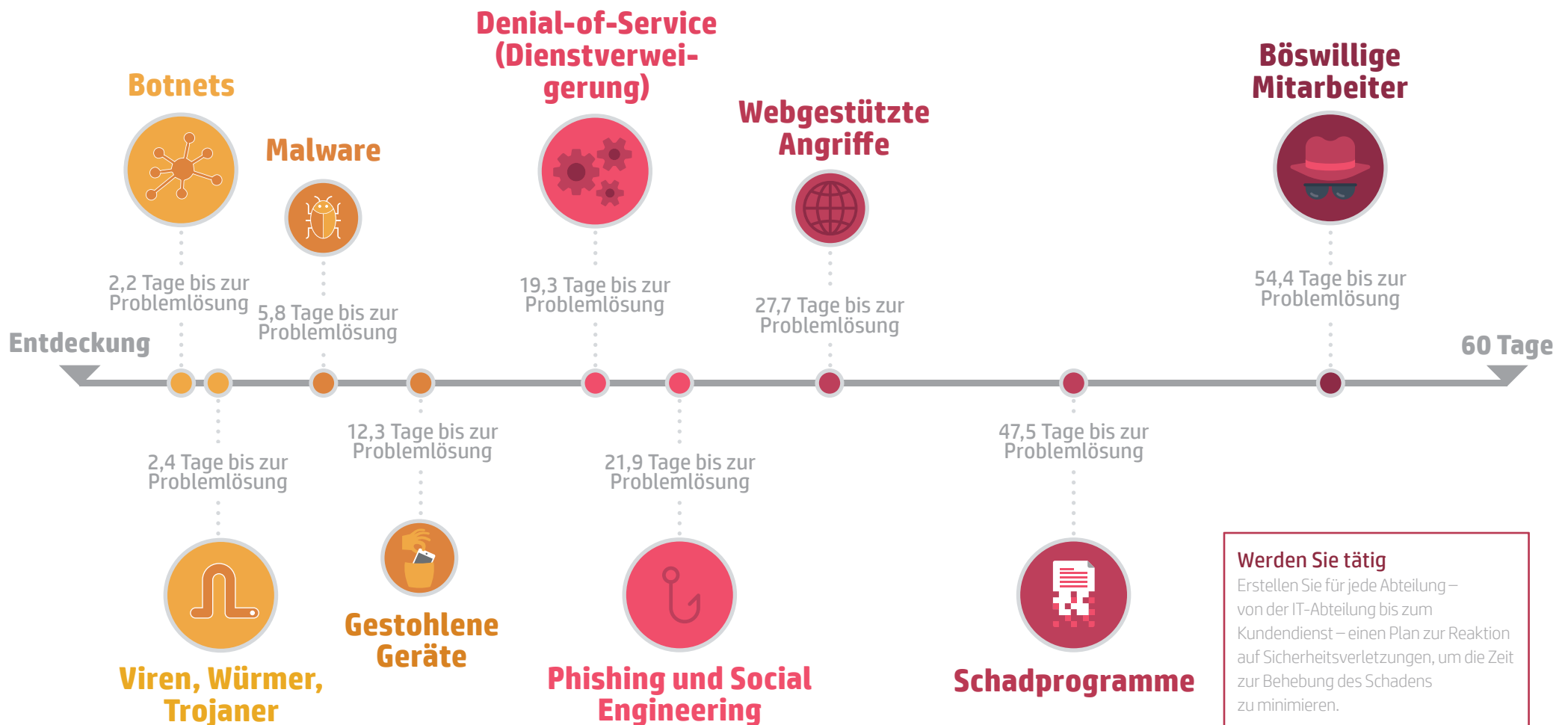
Quellen: ¹⁴ <http://www.businessinsider.com/how-the-hackers-broke-into-sony-2014-12?IR=T> ¹⁵ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

¹⁶ <https://www.statista.com/statistics/293274/average-cyber-crime-costs-to-companies-in-selected-countries/> Stat. ist 7,21 Mio. USD – wurde in GBP umgerechnet

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 Institute¹⁸ schätzt durchschnittlich 46 Tage, ein Zeitraum, der das Aus für ein KMU bedeuten kann, das sich darauf verlässt, ohne Unterbrechung Geschäfte zu machen.



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 bössartigen Websites oder aus E-Mails heruntergeladen wurden, können den Code freigeben, den Hacker benötigen, um einzudringen und Daten zu stehlen.

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 Daten Ihrer Kunden

- 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 berechnete 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 zufolge¹⁹ 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.

86 % der Unternehmen nutzen die Cloud oder planen Cloud-Initiativen.

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 wurden²¹ gerade 7 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. Aber eine sichere Cloud ist nach wie vor auf eine robuste interne Sicherheitskoordination angewiesen. Denken Sie einfach an die Eingangstür von Sony.

Quellen:

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/>²⁰

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.

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 an Bedrohungen, die auf ihre Mobilgeräte abzielen.²³

Mitarbeiter, deren Smartphone gestohlen wurde, können dadurch Hackern unwissentlich 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).

4 MENSCHLICHES FEHLVERHALTEN



So helfen Sie ihren Mitarbeitern

- Schulen Sie Ihre Mitarbeiter zu bewährten Methoden in Bezug auf die 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 gegenwärtig schätzungsweise 13 Milliarden.²⁵

Während Bürocomputer zumindest durch Kennwörter und idealerweise auch durch ein Sicherheitsprogramm geschützt sind, fehlen bei Druckwarteschlangen und Druckaufträgen häufig entsprechende Sicherheitsvorkehrungen.

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

Es ist einen Hinweis wert, 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.²⁶ Die einzige Möglichkeit, die Sicherheit zu gewährleisten, besteht darin, dass alle Unternehmen über Sicherheitsvorkehrungen für alle Endpunkt-Geräte verfügen.

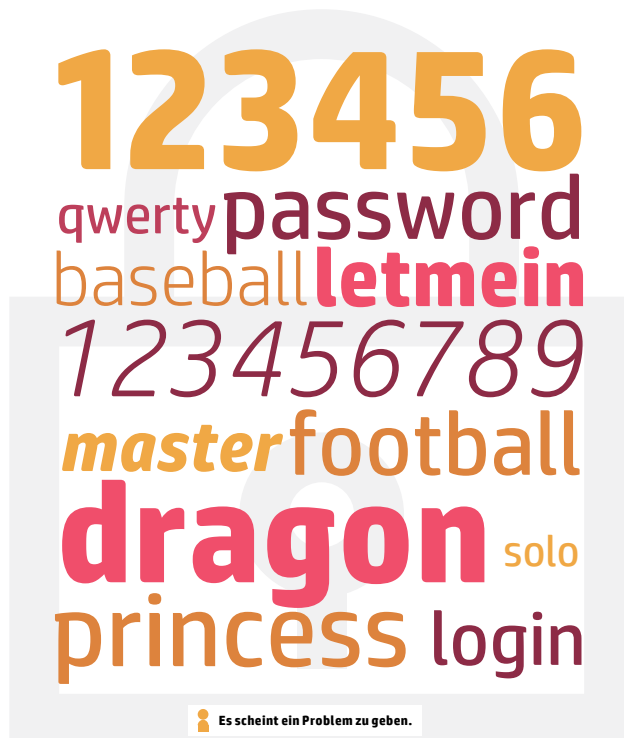
So bereiten Sie sich auf das Internet der Dinge vor

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

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 diese überaus gängigen Passwörter gegen einen entschlossenen Hacker?



* Splashdata

Was ist Ransomware?

Cyberkriminelle nutzen immer öfter Ransomware, eine Form von Malware, die ein System lahmlegt und nur mit Lösegeld in Form von Bitcoins 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 über eine E-Mail oder eine bösartige Website auf Ihrem Computer ein.
	2. Benachrichtigt den Versender	Die Ransomware verbindet sich mit ihrem Home-Server und empfängt einen Verschlüsselungscode.
	3. Verschlüsselt Ihre Daten	Die Ransomware liest die Daten in Ihrem Netzwerk und verschlüsselt diese. Das macht sie unlesbar.
	4. Erpressung	Meistens erscheint eine Nachricht auf dem betroffenen Computer. Sie enthält ein Zeitlimit, bis zu dem das Lösegeld bezahlt werden muss, um die Daten zu entschlüsseln, bevor sie gelöscht werden.
	5. Lösegeldzahlung	Der Geschädigte kann digitale Währung, wie Bitcoins, erwerben, um den Angreifer zu bezahlen. Dieser entschlüsselt im besten Fall die Dateien wieder.

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, das Daten an den Server der Cyberkriminellen weiterleitet, geschuldet sein könnte.
- 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. Unternehmen nutzen Cloud-Computing-Plattformen und gliedern wichtige technische Dienstleistungen an externe Anbieter aus. Und mehr Mitarbeiter arbeiten heute von ausserhalb des Firmengeländes. 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.

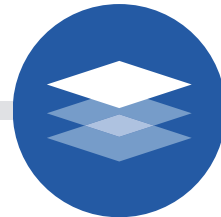


DIE ZUKUNFT DER CYBERSICHERHEIT IN UNTERNEHMEN



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?

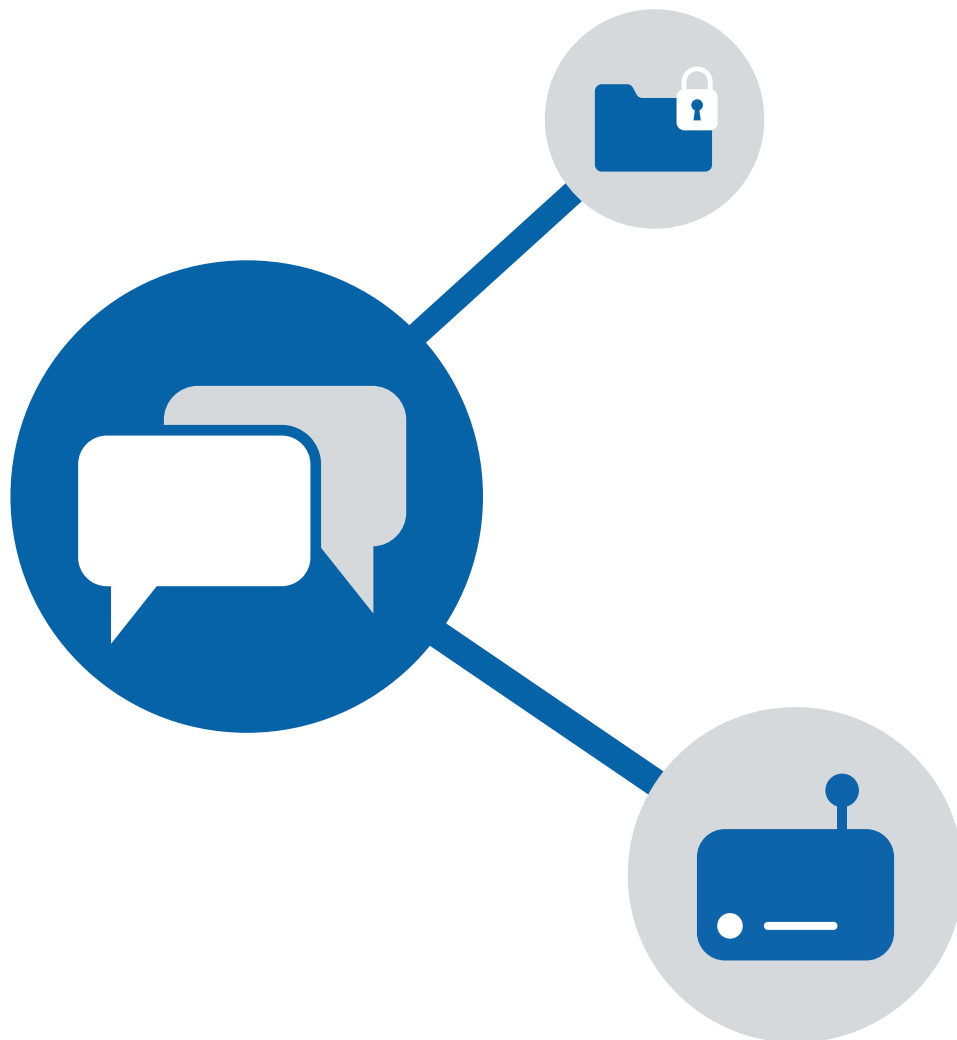
Schliesslich können Sie auch unsere Sicherheitsexperten hier bei HP Inc. kontaktieren. Unsere gemeinsame Wissensbasis ist darauf ausgerichtet, der Bedrohung stets voraus zu sein, nicht nur auf sie zu reagieren. Um mehr zu erfahren, besuchen Sie uns auf [HP Business Computer Security](#).

TIPP:

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

ÜBERLEGUNGEN ZUR SICHERHEIT VON ENDPUNKTGERÄTEN

Die Sicherung jedes einzelnen Geräts in Ihrem Netzwerk



Nach einer von Spiceworks durchgeführten Sicherheitsstudie²⁷ 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 Laptops. Aber das Risiko ist dasselbe. Es ist bekannt, dass Hacker Dinge wie Drucker ins Visier nehmen, oder auch Smartgeräte, die mit Ihrem Netzwerk verbunden sind. Sie wissen, dass diese Geräte in der Regel nicht besonders gut gesichert sind, aber die gleiche Zugangsstufe zu Ihrem Netzwerk bieten.

HP: RICHTUNGSWEISEND IN EINEM NEUEM 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. Die HP Premium Elite-Gerätereihe umfasst marktführende Sicherheitsfunktionen, die Sie anderswo vergeblich suchen, wie zum Beispiel HP SureStart – das weltweit erste „selbstheilende“ BIOS.

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.
- **Biometrische Sicherung:** Durch Gesichts- und Fingerabdruckerkennung erhalten nur Benutzer Zugriff, die sich biometrisch authentifizieren können.
- **HP SureView-Bildschirme*:** Der abgedunkelte Bildschirm verhindert, dass Zuschauer Ihren Bildschirm erkennen können, so wird vertrauliches Material geschützt, wenn Sie unterwegs arbeiten.
- **HP SureStart – selbstheilendes BIOS:** 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. Erfahren Sie [hier](#) mehr über die gesamte HP Elite-Serie.

Für einfachen Zugriff auf jedes Gerät und jeden Dienst, je nach Bedarf Ihres Unternehmens, werfen Sie einen Blick auf HPs Device as a Service. Sie können dort eine Kombination aus Gerät und Zubehör wählen, die sich individuell an Ihre Bedürfnisse anpasst, und von HP über Fernzugriff verwaltet, optimiert und gewartet wird. Erfahren Sie mehr über HP Device as a Service [hier](#).

* Ausgewählte Modelle

** Basierend auf PC-Konkurrenten mit Stand 1. Dezember 2016 mit >1 Mio. Einheiten jährlich mit Erkennung und Selbstheilung auf BIOS-Ebene, Angriffserkennung im Laufzeitspeicher, BIOS-Konfiguration und Richtlinienschutz

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 Einbruchversuche 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.

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**.

GLOSSAR UND LITERATURHINWEISE

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.

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.

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-Plattformen sind dafür bekannt, Würmer verbreitet zu haben; Skype war 2012 von dieser Schmach betroffen.