EIN BLICK AUF DIE HARTE REALITÄT IM ENDPOINT-MANAGEMENT

So lassen sich Lücken bei der geräteübergreifenden Sicherheit schließen

Central by LogMeIn

INHALT

EINFÜHRUNG

Eine der wichtigsten Entwicklungen im Sicherheitsbereich, die 2018 immer mehr an Bedeutung gewonnen hat, ist das Endpoint-Management. Endpoint-Management-Tools erleichtern Unternehmen die Verwaltung ihrer IT-Bestände, da sie ihnen helfen, all ihre Geräte – von Desktopcomputern und Laptops über Router bis hin zu Mobiltelefonen und mehr – zentral zu verwalten, zu aktualisieren und Fehler zu beheben.

Um aktuelle Trends auf dem Markt, Bedrohungen für Unternehmen und von ihnen ergriffene Maßnahmen zur Minderung dieser Risiken besser zu verstehen, haben wir eine Forschungsstudie durchgeführt, an der 1000 IT-Experten teilnahmen. Diese IT-Experten vertraten sowohl kleine als auch mittelständische Unternehmen in ganz Nordamerika und Europa.

Wie unsere Untersuchung ergab, erachtet eine eindeutige Mehrheit der IT-Experten das Endpoint-Management als eine Priorität für ihre Teams – nicht zuletzt angetrieben durch die zunehmende Verbreitung der unterschiedlichsten Endpunkte (d. h. Geräte) in ihren Organisationen. Die Umfrageteilnehmer sind sich der sehr öffentlichen und sehr kostspieligen Sicherheitsverletzungen im vergangenen Jahr bewusst (Equifax, der Hackerangriff auf den US-Auslandsgeheimdienst NSA, um nur einige zu nennen), die auf nicht gepatchte Systeme zurückzuführen sind. Sie wissen, dass mangelnde Vorkehrungen zum Schutz vor diesen Risiken beträchtliche Auswirkungen auf das Endresultat und den Ruf ihres Unternehmens haben können.

Das Bestreben, auf Online-Bedrohungen einzugehen und diese abzuwehren, ist jedoch nicht der einzige Grund, warum die IT-Community die Einführung von Endpoint-Management-Lösungen zu einer Priorität macht. Aktuelle Trends am Arbeitsplatz verlangen dies ebenfalls:

1. BYOD (Bring Your Own Device) und andere Richtlinien für Telearbeiter und deren Laptops und Mobilgeräte werden in kleinen wie auch großen Unternehmen verstärkt zur Norm. Auch im kommenden Jahr ist zu erwarten, dass die Beliebtheit dieser „neuen“ Arbeitsweisen weiter zunimmt.
2. Mit der Vielzahl an Geräten gehen auch unzählige Apps und diverseste Softwarelösungen einher, die auf diesen Geräten installiert sind und zum Schutz vor möglichen Gefahren zentral verwaltet werden müssen.
3. Unternehmen verlagern ihre Geschäftsprozesse zunehmend in die Cloud, was sensible Daten dem Risiko aussetzt, dass unbefugte Personen darauf zugreifen, sie anzeigen oder missbräuchlich verwenden.

Diese Entwicklungen mögen den Endbenutzern das Leben einfacher machen, erhöhen aber gleichzeitig die Gefahr von Sicherheitsverletzungen. Dazu kommen noch die täglichen Online-Bedrohungen, mit denen Unternehmen konfrontiert sind, und es wird offensichtlich, warum IT-Experten in aller Welt nach ganzheitlichen und umfassenden Lösungen zur zentralen Verwaltung sämtlicher Endpunkte Ausschau halten.

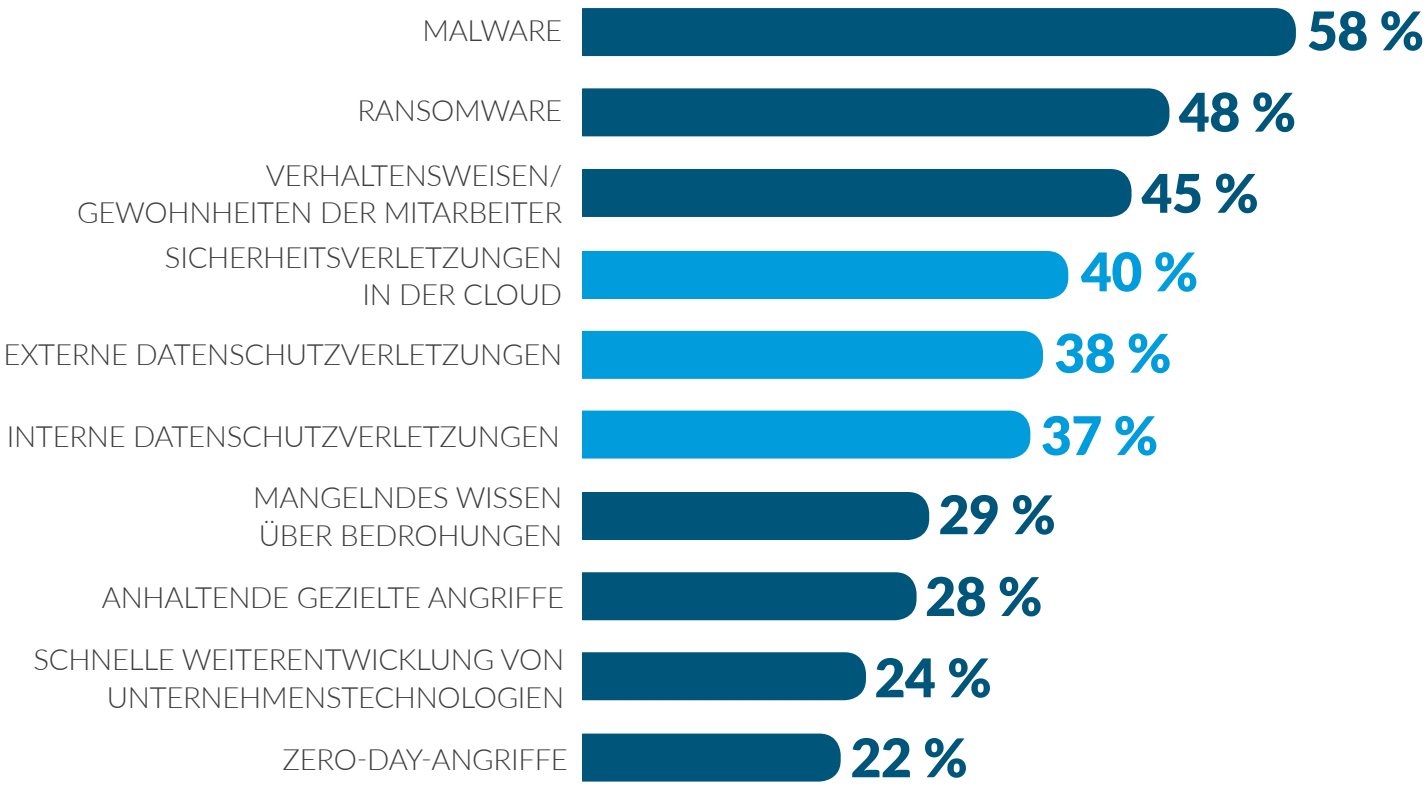
IT-Experten erachten das Endpoint-Management als eine Priorität und aktuelle Trends am Arbeitsplatz verlangen es, aber **NUR DIE HÄLFTE ERGREIFT IM VORFELD MASSNAHMEN** zum Schutz vor Sicherheitsverletzungen

MARKTTRENDS:
SICHERHEITSBEDROHUNGEN SIND REAL UND GREIFEN UM SICH

IT-Experten hatten zu Jahresbeginn 2018 eine Reihe von Sicherheitsbedenken, die durchaus berechtigt waren: Laut McAfee gab es bei Ransomware 2017 einen Anstieg von 56 Prozent.[5] Diese Art von Erpressungssoftware war in 39 Prozent aller Malware-bezogenen Fälle involviert.[5] In der Tat hat es Ransomware mittlerweile nicht mehr nur auf Desktopcomputer abgesehen, sondern auch auf andere Endpunkte wie Server und Netzwerke.[5]

Unsere Studie deutet darauf hin, dass IT-Experten ein gutes Stück Arbeit vor sich haben: Im Durchschnitt sind sie mit mindestens vier verschiedenen Arten von Sicherheitsbedenken konfrontiert; sowohl interne als auch externe. Malware steht dabei ganz oben in der Liste, gefolgt von Ransomware und den Verhaltensweisen/Gewohnheiten der Mitarbeiter. Direkt dahinter kommt das „Triumvirat" der Sicherheitsverletzungen: Cloud-, externe und interne Sicherheitsverletzungen. Diese Bedenken sind real und machen ein umfassendes Endpoint-Management in Unternehmen umso notwendiger. Wenn es Ihnen gelingt, diese IT-Sicherheitsbedrohungen zu isolieren, ist der erste Schritt zum Schutz Ihres gesamten Netzwerks getan.

IT-TEAMS STEHEN VERSCHIEDENEN SICHERHEITSRISIKEN UND -BEDENKEN GEGENÜBER – ALLEN VORAN MALWARE UND RANSOMWARE



BUSINESS-TRENDS:
MIT GEÄNDERTEN TRENDS AM ARBEITSPLATZ SOLLTE SICH AUCH UNSERE HERANGEHENSWEISE AN DIE SICHERHEIT ÄNDERN

DIE ANZAHL DER ENDPUNKTE STEIGT DANK BYOD EXPONENTIELL. IT-TEAMS MÜSSEN DAHER AUF ANDERE WEISE AN DAS THEMA SICHERHEIT HERANGEHEN, WENN SICH NICHT POTENTIELLEN ONLINE-BEDROHUNGEN AUSSETZEN WOLLEN

Vor nicht allzu langer Zeit war die Anzahl der Endpunkte, die IT-Experten verwalten und schützen mussten, überschaubar. Und sie waren direkt unter ihrer Kontrolle. IT-Teams konnten ihre Unternehmen vor Online-Bedrohungen schützen, indem sie die „Außengrenze“ sowie die ihnen bekannten lokal installierten Systeme absicherten. In den letzten Jahren haben BYOD (d. h. die Verwendung privater Geräte am Arbeitsplatz) und die Telearbeit unsere Arbeitsweisen jedoch von Grund auf verändert. Dies stellt IT-Teams nun vor die Herausforderung, ihre Strategien für die Verwaltung und den Schutz der Endpunkte und des Firmennetzwerks zu überdenken.

Unternehmen möchten ihren Beschäftigten mit BYOD und anderen Richtlinien für die Telearbeit mehr Flexibilität bieten, während sie zugleich finanziell von der gestiegenen Produktivität und den gesunkenen Kosten profitieren. Dies wird durch eine von MarketsandMarkets durchgeführte Umfrage zum Thema BYOD-Trends belegt, laut der die Akzeptanzrate in Nordamerika Anfang 2017 bei 36 Prozent lag und im Jahresverlauf 2018 auf fast 50 Prozent steigen sollte[1].

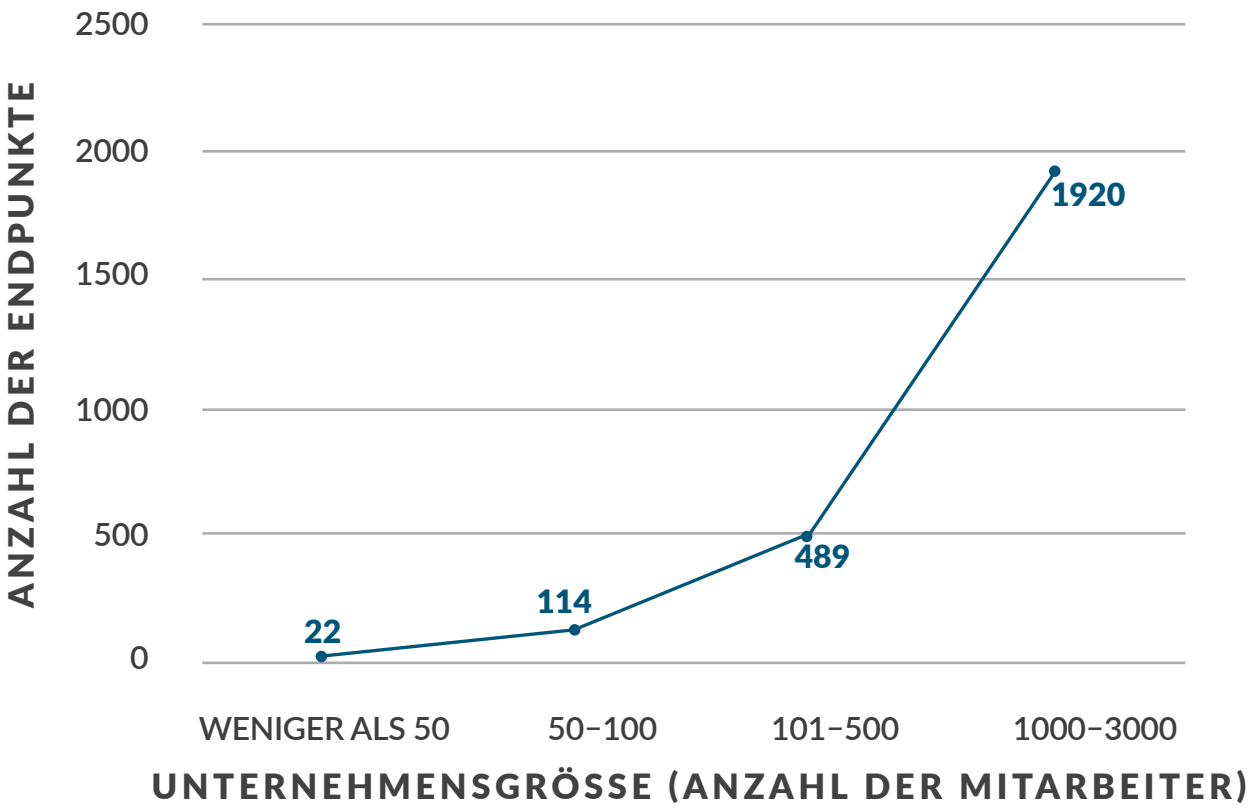
Unsere Untersuchung zeigt, dass 30 Prozent der IT-Experten nicht genau wissen, über wie viele Endgeräte ihr Unternehmen tatsächlich verfügt, sich aber sehr wohl über diesbezügliche Bedrohungen Sorgen machen.

WIE VIELE ENTFERNTE ENDPUNKTE BESITZT IHR UNTERNEHMEN INSGESAMT?

Damit diese Unternehmen Cyberangriffen effektiv vorbeugen können, wird es entscheidend sein, dass sie auf die zunehmende Beliebtheit von BYOD eingehen – und zwar in Form einer umfassenden Lösung für die sichere Verwaltung einer Vielzahl von Geräten.

Jene IT-Experten, die die Anzahl der Endpunkte ihres Unternehmens abschätzen konnten, gaben an, im Durchschnitt über 750 Endpunkte zu verfügen (Server, Mitarbeitercomputer, mobile Endgeräte). Diese beträchtliche Anzahl der Endpunkte macht das ohnehin schon schwierige Unterfangen, sie effektiv zu verwalten und das Unternehmen gleichzeitig vor internen und externen Sicherheitsbedrohungen zu schützen, noch komplexer.

DURCHSCHNITTLICHE ANZAHL DER ENDPUNKTE NACH UNTERNEHMENSGRÖSSE



PROBLEME MIT DER AKTUELLEN HERANGEHENSWEISE: UNTERNEHMEN MÜSSEN SICH DAFÜR RÜSTEN, DEN KRIEG ZU GEWINNEN UND NICHT NUR EINE SCHLACHT

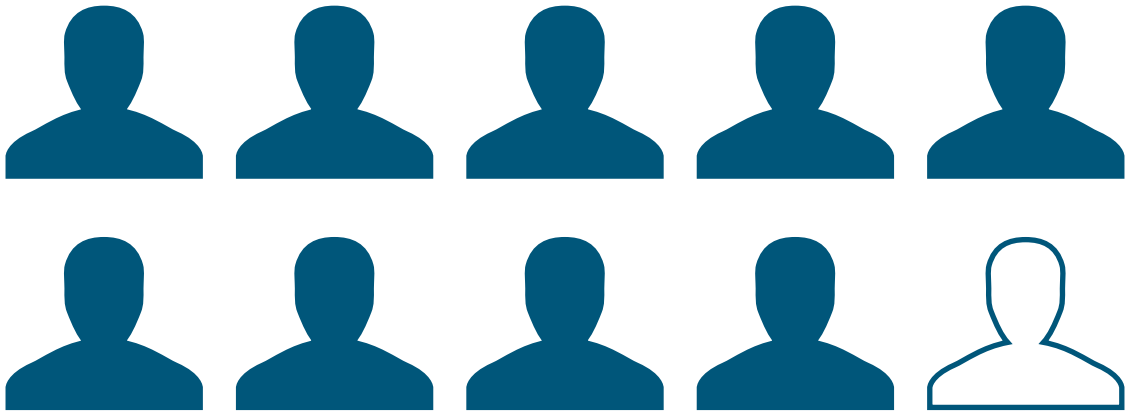
Angesichts der Fülle an Endpunkten und internen und externen Sicherheitsbedrohungen kommt es nicht überraschend, dass nahezu neun von zehn (88 Prozent) der IT-Experten das Endpoint-Management als eine Priorität für ihre Teams sehen.

In der Tat ist der Schutz der Endpunkte vor Malware die zweithäufigste Sicherheitsmaßnahme, die IT-Experten als Reaktion auf diese Bedenken ergreifen.

Andere gängige Sicherheitsmaßnahmen in diesem Zusammenhang sind Firewalls, die Benutzerauthentifizierung und die Verschlüsselung.

Als direkte Konsequenz dieser Sicherheitsmaßnahmen fühlt sich die Mehrheit der IT-Experten (82 Prozent) für den Umgang mit diesen Sicherheitsbedrohungen gerüstet. Nur 26 Prozent sind jedoch der festen Überzeugung, dass diese Sicherheitsmaßnahmen für ihre Endbenutzer effektiv sind.

DAS ENDPOINT-MANAGEMENT IST BEREITS EINE PRIORITÄT, ABER FÜR DEN LANGFRISTIGEN SCHUTZ DES UNTERNEHMENS MUSS MEHR GETAN WERDEN



NAHEZU

9 von 10

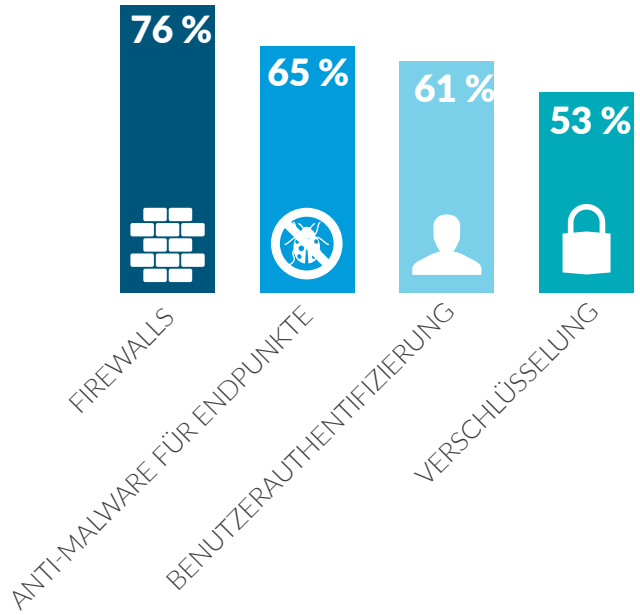
IT-Experten bezeichnen das Endpoint-Management als eine Priorität

DIESE DATEN ZEIGEN, DASS ES NOCH VIEL LUFT NACH OBEN GIBT, WENN UNTERNEHMEN EINE LANGFRISTIGE UND GANZHEITLICHE STRATEGIE FÜR DIE ENDPUNKTSICHERHEIT FINDEN MÖCHTEN:

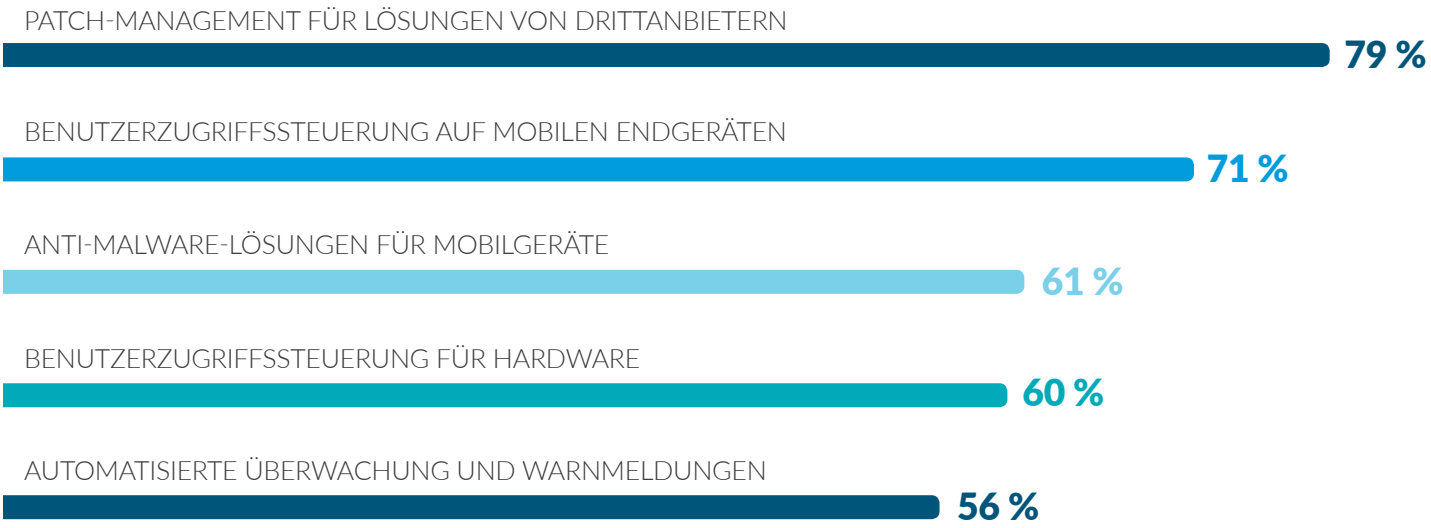
1. Obwohl sich 71 Prozent der IT-Experten eigenen Angaben zufolge aktiv mit der Sicherheit ihrer Hardware befassen, tun dies nur 56 Prozent für ihre Software. Bei Mobilgeräten sind es überhaupt nur 48 Prozent. Diese mangelnde Abdeckung hinterlässt gewaltige Lücken in ihren Sicherheitsstrategien. Immer mehr Mitarbeiter verwenden ihre privaten Smartphones oder Tablets für berufliche Zwecke (z. B. zum Herunterladen oder Bearbeiten von Arbeitsdokumenten oder dem Versenden von E-Mails). Es wird daher immer wichtiger, zu gewährleisten, dass diese Geräte genauso sicher sind wie PCs und andere Endpunkte.

2. Darüber hinaus setzt ein Großteil der IT-Teams viele wichtige Sicherheitsmaßnahmen wie das Patch-Management für Lösungen von Drittanbietern und die Benutzerzugriffssteuerung auf Mobilgeräten derzeit nicht ein, was ihre Unternehmen anfällig für Cyberangriffe macht.

ALS REAKTION AUF SICHERHEITSBEDENKEN ERGRIFFENE MASSNAHMEN



ANTEIL DER IT-EXPERTEN, DIE DIE FOLGENDEN MASSNAHMEN NICHT EINSETZEN



DIE AUSWIRKUNGEN IN ZAHLEN: MANGELNDE VORBEREITUNG BEREITET SIE AUF DAS SCHEITERN VOR

Trotz der unzähligen Hackerangriffe und Sicherheitsbedrohungen, von denen die Medien in letzter Zeit berichteten, beschäftigen sich nur knapp mehr als die Hälfte der IT-Experten (52 Prozent) damit, vor einem Angriff oder Datenleck proaktiv auf Sicherheitsbedenken einzugehen.

Die Gefahren, die Unternehmen durch diese Sicherheitsbedrohungen ausgesetzt sind, betreffen nicht nur ihre Betriebsabläufe, sondern können sich direkt auf das Geschäftsergebnis auswirken, den Ruf des Unternehmens langfristig belasten und sogar zu einer Schließung führen.

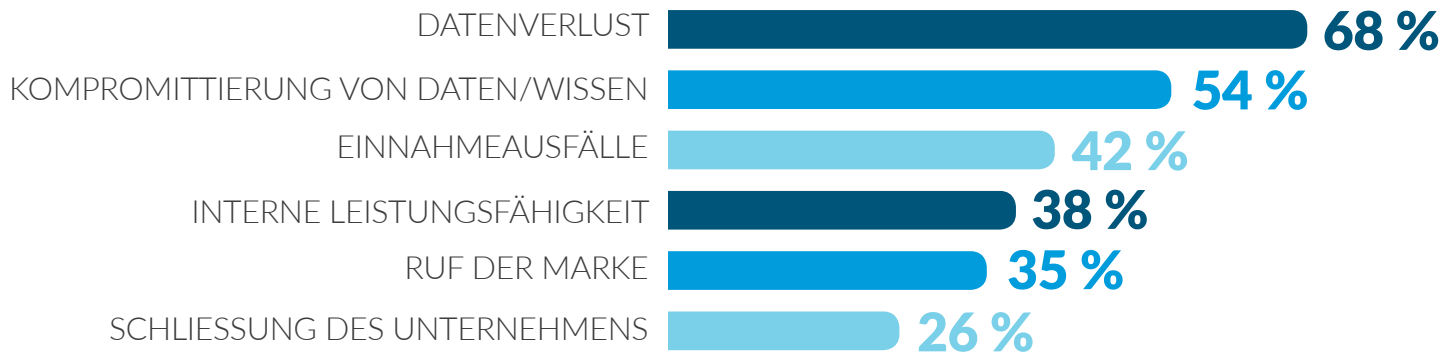
DIE ZAHLEN SIND ERSCHÜTTERND

Manchen Schätzungen zufolge verursachte allein das Schadprogramm WannaCry auf globaler Ebene Schäden zwischen Hunderten Millionen und Milliarden Dollar. Für FedEx/TNT bedeutete der Angriff durch die Ransomware ExPetr entgangene Einnahmen von rund 300 Millionen Dollar[5].

Dazu kommt, dass laut einer von Osterman Research im Auftrag von Malwarebytes durchgeführten globalen Umfrage etwa 16 Prozent der von einem Ransomware-Angriff betroffenen Organisationen Ausfallzeiten von mindestens 25 Stunden erlitten. Bei manchen waren die Systeme sogar mehr als 100 Stunden lang ausgefallen!

Unsere Studie zeigt, dass IT-Experten Datenverluste, die Kompromittierung von Daten sowie Einnahmeausfälle als die größten Risiken sehen, die mit einer Sicherheitsverletzung verbunden sind.

MIT SICHERHEITSBEDENKEN VERBUNDENE RISIKEN



VORTEILE EINER INVESTITION:
INVESTITIONEN SOLLTEN SICH GEMEINSAM MIT DEN RISIKEN WEITERENTWICKELN

DIE IT-SICHERHEIT MUSS ÜBER KONVENTIONELLE SCHUTZMETHODEN HINAUSGEHEN UND NEU AUFTRETENDE SICHERHEITSBEDROHUNGEN UMFASSEND ABDECKEN

Laut unserer Umfrage zählt der Malware-Schutz von Endpunkten derzeit zu den drei wichtigsten Prioritäten in puncto Sicherheit, auf die der größte Anteil der IT-Sicherheitsbudgets entfällt. Die beiden anderen Prioritäten, die einen Großteil der finanziellen Mittel erhalten, sind Firewalls und IT-Schulungen.

In andere Bereiche, die zur Abwehr von Bedrohungen beitragen können, wird jedoch nicht so viel investiert – darunter die automatisierte Überwachung und Warnmeldungen (26 Prozent), Anti-Malware-Lösungen für Mobilgeräte (17 Prozent) und das Patch-Management für Lösungen von Drittanbietern (14 Prozent).

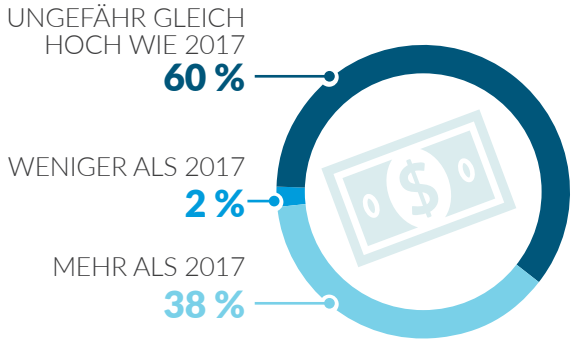
Die Bereiche, in die IT-Experten laut eigener Aussage am wenigsten investieren, sind in der Tat:

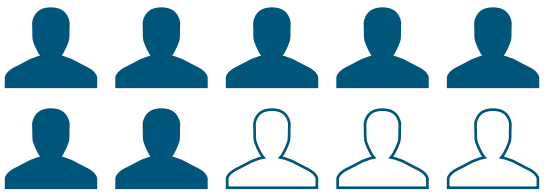
Patch-Management für Lösungen von Drittanbietern sowie die Benutzerzugriffssteuerung für Mobilgeräte und Hardware.

Diese Maßnahmen, denen nur wenige Geldmittel zuteil werden, können allerdings einige wesentliche Vorteile mit sich bringen:

- Wenn Systeme auf Bedrohungen überwacht und echte von falschen Bedrohungen unterschieden werden, kann das Unternehmen Zeit und Geld sparen und seine Produktivität erhöhen.
- Die Sicherheit wird verbessert, da sich IT-Teams auf tatsächliche Vorfälle konzentrieren können.
- Best Practices in puncto Sicherheit werden garantiert eingehalten.
- Das Unternehmen sorgt dafür, dass seine Sicherheitsmaßnahmen in Bezug auf neue Eigenschaften oder Funktionen stets auf dem aktuellsten Stand sind.
- Außerdem wird sichergestellt, dass die Mobilgeräte der Mitarbeiter keinen Eintrittspunkt zu den vertraulichen Daten und Informationen des Unternehmens darstellen können.

IT-BUDGET 2018 IM VERGLEICH ZU 2017





Die **überwiegende Mehrheit (70 Prozent) der IT-Experten** widmet **weniger als 25 Prozent** ihres Budgets der IT-Sicherheit

WAS SIE TUN KÖNNEN

Angriffe auf die Cybersicherheit werden immer häufiger und immer raffinierter und die Anzahl der Endpunkte nimmt bedingt durch neue Trends am Arbeitsplatz rasant zu. IT-Teams gehen auf diese neuen Herausforderungen ein, indem sie eine Reihe von Sicherheitsmaßnahmen ergreifen und das Endpoint-Management zu einer ihrer wichtigsten Prioritäten machen. Wenn Sie nicht möchten, dass Ihr Unternehmen Opfer eines Cyberangriffs wird, sollten Sie allerdings noch mehr tun:

PROAKTIV HANDELN

Warten Sie nicht, bis Sie Opfer eines Hackerangriffs oder eines Datenlecks werden, bevor Sie auf Sicherheitsbedenken eingehen. Vorbeugende Sicherheitsmaßnahmen wie die automatisierte Überwachung und Warnmeldungen und aktualisierte Patches können zur Abwehr zahlreicher Angriffe beitragen.

SYSTEME PATCHEN

Das Patch-Management ist ein wichtiger Faktor für den Schutz Ihrer IT-Infrastruktur. Egal, ob Sie einen Tag pro Woche dem Patchen Ihrer Systeme widmen oder proaktive Warnmeldungen einrichten, die Sie über nötige Patches benachrichtigen – es ist wichtig, dass Sie das Patch-Management jederzeit im Griff haben.

GANZHEITLICHER AN DIE SICHERHEIT HERANGEHEN

Angriffe zielen heutzutage nicht mehr nur auf PCs ab. Mobilgeräte, Server und andere Endpunkte werden immer anfälliger für Cyberangriffe.

MITARBEITER AUFKLÄREN

Die Entwicklung und Förderung korrekter Verhaltensweisen und Gewohnheiten der Mitarbeiter in Sachen Daten- und Cybersicherheit leistet einen wesentlichen Beitrag zu einer sicheren IT-Infrastruktur.

Quellen

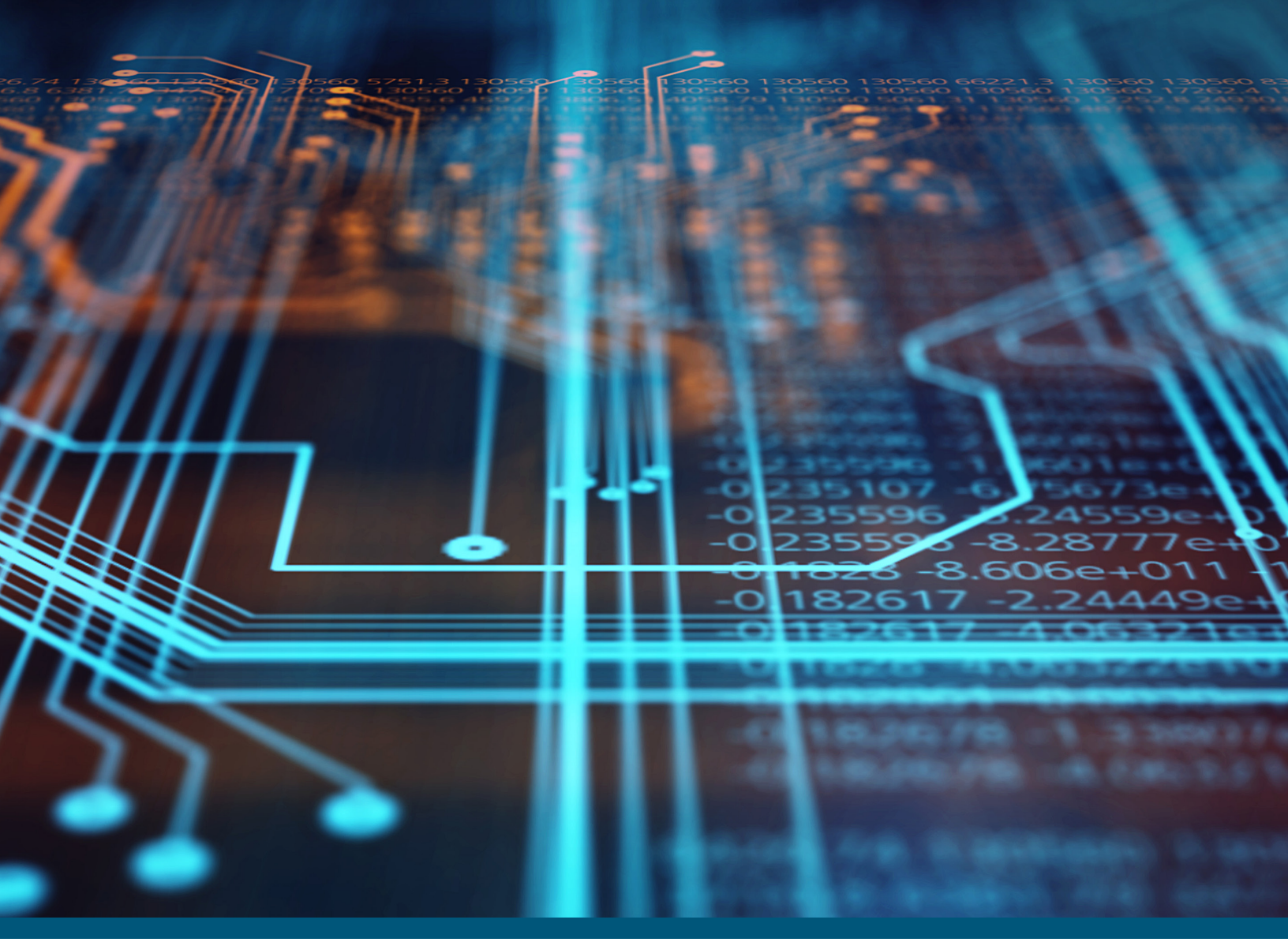
[1] Mobile Business Insights: „The latest BYOD trends and predictions, from mobile focus to endpoint management“, von Jonathan Crowl, 14. August 2017

[2] Entrepreneur: „Business Cyber Attacks Top 4,000 Per Day: Your Guide to Ransomware“, von Jorge Rey, 30. November 2016

[3] ZDNet.com-Infografik: „2018 IT budgets are up slightly; spending focus is on security, hardware, and cloud“, von Amy Talbott, 2. Oktober 2017

[4] Comparitech: „2016-2017 Ransomware statistics and facts“, von Sam Cook, 17. Januar 2018

[5] Verizon 2018 Data Breach Investigations Report, von Maria Korolov (beitragende Verfasserin, CSO), 10. April 2018



Central by LogMeIn

EINFACHE UND SICHERE IT-AUTOMATISIERUNG UND ENDPUNKTVERWALTUNG

LogMeIn Central, Teil des Produktangebots von LogMeIn Inc. im Bereich Identitäts- und Zugriffsverwaltung, ist eine echte Cloud-basierte Endpoint-Management-Lösung, mit der IT-Experten die Endpunktinfrastruktur ihres Unternehmens effektiv überwachen, verwalten und schützen können. Egal, ob Ihre Mitarbeiter remote arbeiten oder Ihre Endpunkte rund um den Globus verteilt sind – LogMeIn Central bietet Ihnen die nötige Geschwindigkeit, Flexibilität und Transparenz, um Ihre Produktivität zu steigern, die IT-Kosten zu senken und die Risiken zu minimieren. Es wurde als das beste Fernzugriffstool für Kleinunternehmen bewertet, die für eine Reihe von Computern verantwortlich sind. Mit seinen leistungsfähigen Fernzugriffsfunktionen macht LogMeIn Central alle Endpunkte in Ihrem Netzwerk zugänglich, sodass Sie Probleme jederzeit und überall beheben können.

https://www.logmein.com/central