WAS SIE TUN KÖNNEN, UM IHRE ENDGERÄTE GEGEN NEUE CYBERBEDROHUNGEN ABZUSICHERN

Schützen Sie Ihre Geräte, Ihre Daten und Ihre Reputation – mit intelligenten Entscheidungen rund um die IT-Sicherheit: Wie robuste Hardware und Services Ihrem Unternehmen helfen, den entscheidenden Schritt voraus zu sein.

INHALT

01 SO SCHÜTZEN SIE SICH GEGEN CYBERKRIMINALITÄT

Die digitale Landschaft befindet sich im stetigen Wandel, und Cyberkriminelle werden immer raffinierter. Unternehmen sehen sich dadurch neuen Risiken ausgesetzt. Von modernen Arbeitsmodellen bis hin zur steigenden Anzahl ernstzunehmender Angriffe auf Endgeräte: Es gibt heute zahlreiche Bereiche, die für die unternehmensweite IT–Sicherheit potenzielle Lücken bergen können.

Es steht viel auf dem Spiel. Doch es gibt Mittel und Wege, Ihre Abwehr zu stärken.

Kein Unternehmen wünscht sich Schlagzeilen im Zusammenhang mit fahrlässig verursachten Cyberangriffen. Um Imageverluste dieser Art zu vermeiden, sollten sich Organisationen daher rechtzeitig mit der IT–Sicherheit auf Geräteebene befassen und Services implementieren, die dazu beitragen, Risiken von heute zu minimieren – und sich für die Risiken von morgen zu rüsten.

SIND DIESE DREI PUNKTE IN IHREM UNTERNEHMEN GANZ OBEN AUF DER AGENDA?

Auf den folgenden Seiten zeigen wir Ihnen einige der wichtigsten Trends zu den Themen Cybersicherheit und potenzielle Bedrohungen für moderne Endgeräte auf. Fragen Sie sich zunächst: Was unternimmt mein Unternehmen, um sich zu schützen? Fließen die folgenden drei zentralen Punkte in unsere PC-Kaufentscheidungen ein? Später widmen wir uns dann der Frage, wie Sie sicherstellen können, dass diese Aspekte durchgängig in Ihre IT-Infrastruktur integriert sind.

1

Widerstandsfähige Hardware,

die Firmware und Anwendungen schützt, sowie bei Angriffen das BIOS sofort sichert und schnell wiederherstellt, damit Sie ohne große Verzögerungen weiterarbeiten können.

2

Mehrere Schutzebenen,

die Ihre IT proaktiv vor Bedrohungen bis hinein in die Betriebssystem-Ebene und darüber hinaus schützen und verhindern, dass das Netzwerk in Mitleidenschaft gezogen wird – von hardwaregestützter Sicherheit bis hin zu Technologien für die Gefahrenprävention.

3

Proaktives IT-Management,

das dafür sorgt, Sicherheitsrichtlinien durchzusetzen, Gefahren automatisch zu überwachen und aktiv gegen diese vorzugehen.

02 NEUE ARBEITSMODELLE BEDEUTEN AUCH NEUE SICHERHEITSRISIKEN

Dank der leistungsfähigen digitalen Umgebung von heute sind Unternehmen besser vernetzt denn je. Die Digitalisierung hat flexible Arbeitsmodelle nicht nur möglich gemacht, sondern auch dafür gesorgt, dass Teams rund um den Globus diese Art der Zusammenarbeit bevorzugen. Der Wunsch nach mehr Flexibilität am Arbeitsplatz wächst stetig – doch während die Produktivität und die Zufriedenheit der Mitarbeiter davon profitieren, steigt gleichzeitig die Zahl neuer Standorte, Geräte und Netzwerke im System. Die Folge: Unsichere Netzwerke oder nicht gesicherte Endgeräte machen Unternehmen anfällig für Angriffe.

aller Unternehmen geben an, dass flexibles Arbeiten die Produktivität verbessere,[1] doch mit den mobilen Mitarbeitern verlassen auch sensible Daten die Büroumgebung.

AKTUELLER AUSBLICK:	MÖGLICHE LÖSUNG:
Arbeitsaufgaben werden an neuen Standorten und auf neuen Geräten erledigt	Überlegungen zum Schutz vor den Risiken flexibler Arbeitsmodelle
Mehr als die Hälfte der Mitarbeiter weltweit arbeitet mindestens 2,5 Tage pro Woche außerhalb des Büros.[1]	Management-Services bieten Support außerhalb des Büros, statten Nutzer mit sicheren, topaktuellen Geräten aus und können bei Bedarf Daten aus der Ferne löschen.
Coffee Shops und Cafés sind der zweitbeliebteste Ort zum Arbeiten.[2]	Selbstheilende Hardware erkennt und schützt vor Gefahren in unsicheren Netzwerken, um die Bedrohung in Echtzeit einzudämmen. Bildschirme mit integriertem Blickschutz halten darüber hinaus visuelle Hacker fern.
Nur 40 % der persönlichen Geräte, die zum Arbeiten verwendet werden, unterliegen den Sicherheits-vorschriften.[3]	Sicherheits- und Bedrohungsanalysen bieten Transparenz und Einblicke zur Vorhersage von Problemen; Managed Services überwachen den Status und analysieren Bedrohungen.

„Mitarbeiter können unterwegs arbeiten – in Cafés, im Hotel, im Flugzeug. Viele verbinden sich dabei mit beliebigen drahtlosen Netzwerken, ohne die entsprechenden Berechtigungen zu kennen. Und dann gehen sie zurück ins Büro, loggen sich wieder ins Unternehmens-netzwerk ein, können dadurch das System infizieren– und somit das gesamte Unternehmen in Gefahr bringen."

Michael Calce, genannt „MafiaBoy", Vorsitzender des HP Security Advisory Board

VIER DINGE, DIE SIE BEACHTEN SOLLTEN

Die folgenden Fragen können Sie dabei unterstützen, den aktuellen Status Ihrer Hardware und Services zu beurteilen und zu bewerten, ob Ihr Unternehmen gegen potenzielle Angriffe ausreichend geschützt ist.

- Hat Ihr Unternehmen einen Patch-Management-Prozess zur systematischen Behebung von Software-Schwachstellen im Einsatz?
- Würde Ihr Unternehmen von regelmäßigen Einblicken in den Status und die Effizienz seiner Sicherheitssysteme profitieren?
- In welche Technologien investiert Ihr Unternehmen derzeit, um die Sicherheit von Endgeräten zu gewährleisten?
- Bieten Sie Sicherheitstrainings für Endbenutzer an und falls ja, wie effektiv sind diese?

EIN BLICK AUF DIE DERZEITIGE IT-LANDSCHAFT ZUR CYBERSICHERHEIT

Ohne Internet ist Business heute undenkbar. Doch mit der zunehmenden Komplexität der digitalen Welt steigt auch die Cyberkriminalität – und das Maß der Gefahr, das sie für unsere Sicherheit darstellt. Die Bedrohungen werden immer zahlreicher und komplexer, und sie breiten sich immer schneller im gesamten Unternehmen aus, wenn sie erst einmal ins System eingedrungen sind.

Um sich gegen das wachsende Risikopotenzial zu wappnen, müssen Unternehmen bei der Auswahl neuer Services und Geräte gezielt nach bestimmten Funktionen Ausschau halten. Durch die Entscheidung für Hardware und Services, die sofort auf Bedrohungen reagieren können, lässt sich sicherstellen, dass die Mitarbeiter den Betrieb schnell wieder aufnehmen können, um die Produktivität aufrechtzuerhalten. So kann das Unternehmen langfristige finanzielle Folgen, die durch Cyberkriminalität entstehen, vermeiden.

68 % der führenden Unternehmen geben an, dass Cyberrisiken zunehmen.[4]

Die Folgekosten von Cyberangriffen sind in einem Jahr um 12 % gestiegen und liegen im Durchschnitt bei **13 Mio. US-Dollar**.[4]

Cyberangriffe und Datenmissbrauch sind **zwei der Top-5-Risiken**, denen sich CEOs gegenübersehen.[4]

EIN BLICK AUF DATENVERLETZUNGEN IN VERSCHIEDENEN BRANCHEN

Medienberichte über Datenverletzungen und Computerbetrug haben in den letzten Jahren stark zugenommen. Cyberkriminelle machen vor keiner Branche Halt. Von Hotel- und Gastronomiebetrieben über Social-Media-Riesen und Stadtverwaltungen bis hin zu Gesundheitsdienstleistern: Selbst die größten Unternehmen der Welt sehen sich mit Negativschlagzeilen zum Verlust von Kunden, Mitarbeiter- und Firmendaten konfrontiert.

FACEBOOK

Im April 2019 stand Facebook erneut unter Beschuss, da Millionen von Nutzerdaten offengelegt wurden. Das beliebte soziale Netzwerk erlaubte zwei Apps den Zugriff auf die persönlichen Daten seiner Nutzer – und diese Informationen lagen auf unsicheren Servern. Insgesamt konnte auf 540 Millionen Datensätze zugegriffen werden, einschließlich Facebook–IDs, Kommentare und Likes.[5]

Dieser Vorfall geschah weniger als ein Jahr nachdem Facebook die größte Datenverletzung der Unternehmensgeschichte bekannt gegeben hatte, bei der persönliche Informationen von bis zu 50 Mio. Nutzern offengelegt wurden, woraufhin die Facebook–Aktie um mehr als 3 % sank.[6]

„Die Wahrheit ist, dass wir einen Punkt erreicht haben, an dem die meisten Städte jede Woche mit einer Million solcher Angriffe konfrontiert sind – damit haben lokale Behörden heute zu kämpfen.“[9]

Nicole Perlroth, Reporterin für Cybersicherheit, New York Times (aus einem Interview von Dave Davies im Rahmen des Radioprogramms „Fresh Air with Terry Gross“, produziert von WHYY, Inc. und ausgestrahlt von NPR)

DIE STÄDTE BALTIMORE UND GREENVILLE IN DEN USA

Laut des „2019 Data Breach Investigations Report“ von Verizon richteten sich 16 % aller Verstöße gegen öffentliche Einrichtungen – der höchste Prozentsatz aller untersuchten Sektoren.[7] Im Mai 2019 wurde auf die Stadt Baltimore im US–Staat Maryland ein Ransomware–Angriff verübt, bei dem rund 10.000 behördlich genutzte IT–Geräte mit einer neuen Ransomware namens RobbinHood[8] infiziert wurden, die kritische städtische Services wie das Zahlungssystem für Wasser und Grundsteuer lahmlegte. Die Hacker forderten 13 Bitcoins (etwa 100.000 US–Dollar) Lösegeld, um die Systeme wieder freizuschalten. Da die Stadt der Forderung nicht nachkam, stiegen die Kosten in der Folge auf mehrere Millionen US–Dollar an.

Baltimore war die zweite Stadt in den USA, die der böswilligen RobbinHood–Attacke zum Opfer fiel. Im Vormonat war bereits Greenville im Bundesstaat North Carolina angegriffen worden. Doch damit nicht genug. Zahlreiche weitere Städte auf der ganzen Welt waren von den Angriffen betroffen, auch wenn die Öffentlichkeit nicht informiert wurde.

AUSTRALIAN NATIONAL UNIVERSITY

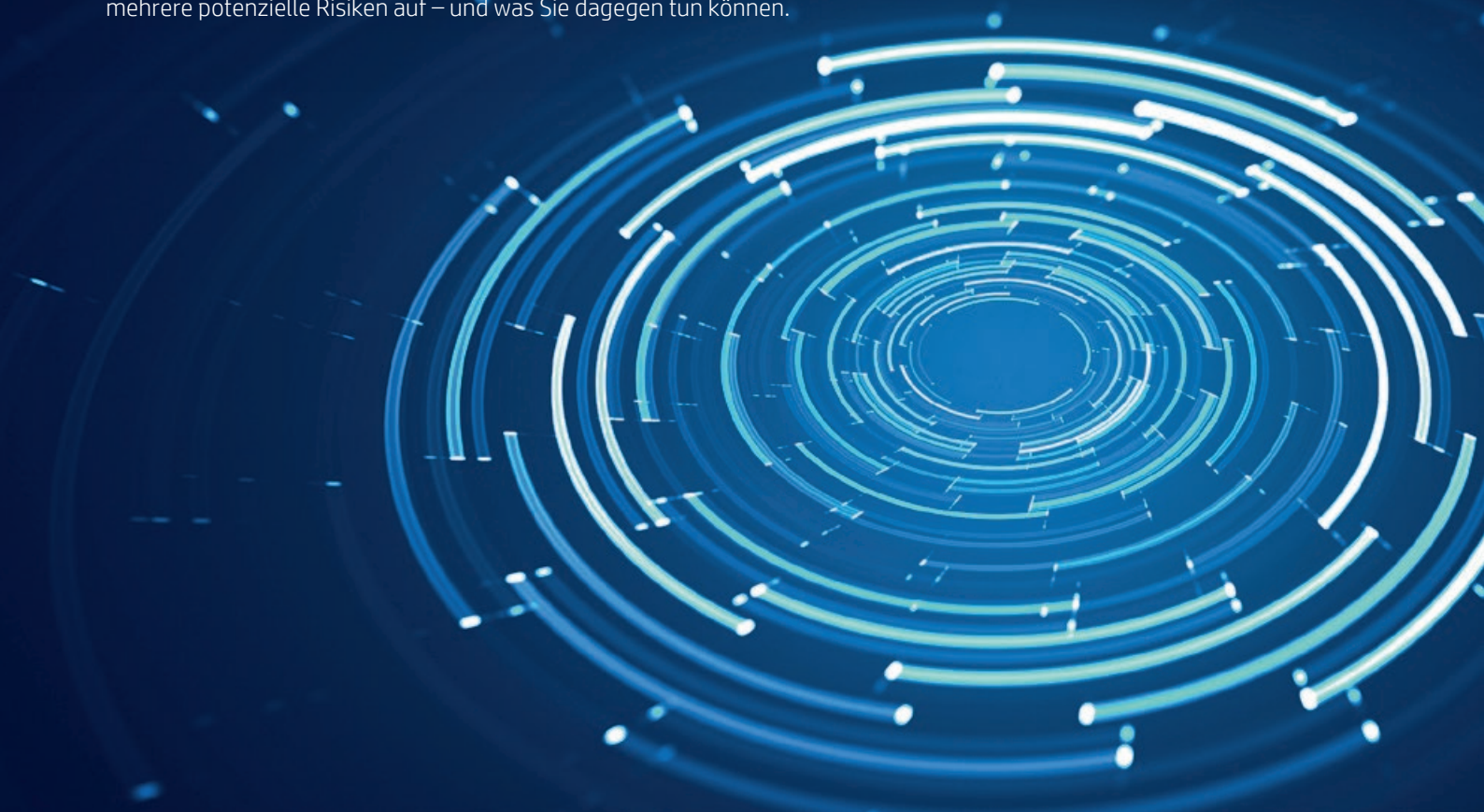
Wie die Universität bestätigt hat, wurden geschätzte 200.000 Personen, einschließlich Mitarbeitern und Studierenden, von einer schweren Datenpanne betroffen, die im Mai 2019 entdeckt wurde. In einer Mitteilung an die Leitung der Hochschule erklärte der Vizekanzler, dass ein Unbefugter Zugriff auf persönliche Informationen aus 19 Jahren hatte, darunter Namen, Adressen, Gehaltsabrechnungen und Bankkonten.[10]

04 WELCHE GEFAHREN SOLLTEN SIE AUF DEM SCHIRM HABEN?

„Wir haben einen Anstieg bei Firmware-Angriffen beobachtet, d. h. Angriffe auf die in der Hardware eingebettete Software, über die der Angreifer das gesamte System unter seine Kontrolle bringen kann. Um diesem Bedrohungsszenario entgegenzuwirken, hat HP branchenführende Systeme und Geräte entwickelt, deren Sicherheitslevel bereits auf Hardwareebene beginnt, um dazu beizutragen, vor Angriffen zu schützen, sie zu erkennen und die Folgen zu beheben – mit minimaler Unterbrechung für die Nutzer."

Boris Balacheff, Chief Technologist im Bereich System Security Research und Innovation bei HP, für die Sonderausgabe zum Thema „Cybersicherheit" des HP Innovation Journal.

Bedrohungen lauern überall. Und sie haben die unterschiedlichsten Formen. Doch für jede Bedrohung gibt es die passende Gegenwehr. Wir zeigen Ihnen mehrere potenzielle Risiken auf – und was Sie dagegen tun können.



AKTUELLER AUSBLICK:	MÖGLICHE LÖSUNG:
Die Anzahl der Bedrohungen nimmt zu	Funktionen, auf die Sie achten sollten, um Ihr Unternehmen zu schützen
Unsichere Geräte mobiler Mitarbeiter Immer mehr Mitarbeiter arbeiten über verschiedene Geräte, Standorte und Verbindungen hinweg – und nicht alle davon sind sicher.	Überwachung und Analysen in Echtzeit geben Einblick in den Status der Geräte und können erkennen, woher ein Angriff auf die Sicherheit kommt, um eine schnelle Reaktion zu gewährleisten.
Raffinierte Malware-Angriffe Malware, die gezielt modifiziert wurde, um ein System zu infiltrieren, ist für herkömmliche Sicherheitskontrollen und Antivirusprogramme oft nicht auffindbar.	Künstliche Intelligenz (KI) mit Deep-Learning-Technologie kann neue, noch nie dagewesene Malware identifizieren und vor ihr schützen.
Angriffe auf die Firmware Sicherheit auf Firmwareebene – insbesondere im BIOS – kann für Malware anfällig sein und von Hackern ausgenutzt werden.	Ein selbstheilendes BIOS erkennt Bedrohungen und stellt sich nach Angriffen oder Beschädigungen automatisch wieder her, ohne dass das IT-Team eingreifen muss.

AKTUELLER AUSBLICK:	WICHTIGE ENTSCHEIDUNGEN:
Die Anzahl der Bedrohungen nimmt zu	Funktionen, auf die Sie achten sollten, um Ihr Unternehmen zu schützen
Ransomware Als zweithäufigste Malware-Bedrohung[7] verzeichneten Ransomware-Angriffe in der ersten Jahreshälfte 2019 einen Anstieg um 15 %.[3] Ransomware wird entwickelt, um Daten zu sperren, zu verschlüsseln und den Zugriff darauf zu blockieren, bis ein Lösegeld bezahlt wird.	Hardwaregestützte Sicherheit kann dazu beitragen, PCs vor Ransomware zu schützen und die Wiederherstellung zu beschleunigen, um Auswirkungen und Ausfallzeiten zu minimieren.
Cryptojacking Eine Form des Cyberangriffs, bei dem Hacker die Verarbeitungsleistung ihres Ziels „abgraben“, um Kryptowährung zu stehlen. McAfee hat herausgefunden,[11] dass das Aufkommen von Cryptomining-Malware im Jahr 2018 um 4.000 % gestiegen ist und teure Folgen in Bezug auf Energiekosten, Netzwerkleistung und Anfälligkeit für andere Angriffe nach sich ziehen kann.	Managed Services stellen sicher, dass Sie jederzeit mit den neuesten Geräten, aktueller Software und hoch entwickelten Schutzmechanismen ausgestattet sind. Sie wollen mehr zum Thema Cryptojacking erfahren? Lesen Sie unseren Leitfaden über Cryptojacking und erfahren Sie, wie Sie den Cyberdieben einen Riegel vorschieben.
Menschliches Versagen und Endgeräte Endgeräte sind ein gerne genutzter Angriffsvektor. Auch Mitarbeiter sind anfällig für Attacken, sodass sich die Erfolgsaussichten erhöhen, wenn beide Risikofaktoren zusammenkommen. E-Mail ist mit 94 % der häufigste Kanal, über den Malware ins System gelangt.[7]	Zukunftsweisender Malware-Schutz isoliert betroffene E-Mails, Browser und Dateien, um die Verbreitung im System unmittelbar zu unterbinden.

Sicherheitsrichtlinien und Antivirussoftware alleine reichen nicht aus. Unternehmen sollten rechtzeitig zusätzliche Schutzebenen und Services in Betracht ziehen, um ihre Abwehr aktiv zu stärken.

05 SICHERHEIT BEGINNT BEI DEN ENDGERÄTEN

Endgeräte sind ein beliebtes Ziel für Cyberangriffe. Immer häufiger werden Sicherheitsverletzungen im Unternehmen auf ein infiziertes Endgerät zurückgeführt.[12] Von der Dezentralisierung des Arbeitsplatzes, die eine durchgängige Überwachung der Geräte schwierig macht, bis hin zu dem Druck, Angriffe auffangen zu müssen, die Antivirenprogramme übersehen: Ein Mangel an Sicherheit auf Endgerätelevel kann das gesamte Unternehmen, dessen Produktivität und nicht zuletzt dessen Geschäftsergebnis stark beeinträchtigen.

aller Unternehmen berichteten von schweren Datenverstößen, die auf ein unsicheres Endgerät zurückzuführen sind.[12]

AKTUELLER AUSBLICK:	MÖGLICHE LÖSUNG:
Endgeräte stellen in der Unternehmenssicherheit ein schwaches Glied dar.	Überlegungen, um Endgeräte gegen Bedrohungen zu schützen.
Bei Zero-Day-Angriffen ist die Wahrscheinlichkeit, dass Unternehmen gefährdet werden, viermal höher.[12]	Managed Services können durch Bedrohungsschutz und Analysen in Echtzeit vor Zero-Day-Angriffen schützen.
57 % aller erfolgreichen Angriffe wurden von traditioneller Antivirensoftware nicht erkannt.[12]	Künstliche Intelligenz (KI) mit Deep-Learning-Technologie, die über die traditionelle Antivirusebene hinausgeht, kann den Geräteschutz weiter erhöhen.
Bei über der Hälfte der Verstöße dauert es Monate oder länger, bis sie entdeckt werden.[7]	Services, die einen vollständigen Überblick über den Gerätezustand inklusive Reporting bereitstellen, können Unternehmen dabei helfen, Probleme aufzudecken und Geräte zu schützen.
Die Häufigkeit neuer oder unbekannter Zero-Day-Angriffe ist im Jahr 2018 von 24 % auf 37 % gestiegen.[12]	Angesichts täglich neuer Malware kann Künstliche Intelligenz (KI) mit Deep-Learning-Technologie vor nie dagewesenen Angriffen schützen, noch bevor diese entstehen.
48 % aller bösartigen E-Mail-Anhänge sind Office-Dateien.[13]	Technologie zur Isolierung von Bedrohungen in Echtzeit fängt Malware aus E-Mail-Anhängen oder Dateidownloads ab und verhindert so, dass sie sich auf das Gerät und das Netzwerk ausbreitet.

Mehr Infos?

Entdecken Sie Fünf Gründe, warum die Sicherheit Ihrer Endgeräte ein Risiko sein könnte.

DER MENSCHLICHE FAKTOR

Wo Endgeräte sind, sind auch Mitarbeiter. Und wo es Menschen gibt, gibt es auch unweigerlich menschliches Versagen. Und Betrüger, die bereit sind, das auszunutzen. Der „2019 Data Breach Investigations Report" von Verizon ergab, dass 21 % der Verstöße durch menschliches Versagen verursacht wurden – ein Anstieg um 5 % in fünf Jahren.[7] Könnte unzureichendes Sicherheitsbewusstsein der Grund sein? Untersuchungen von Proofpoint ergaben, dass Mitarbeiter fast ein Viertel der sicherheitsrelevanten Fragen falsch beantworten,[14] darunter Fragen zur Verschlüsselung auf Mobilgeräten, zu den Maßnahmen, die nach einem potenziellen Verstoß zu ergreifen sind, und zur Identifizierung von Phishing-Angriffen.

Social Engineering, vom Spear-Phishing (Phishing, das auf ein bestimmtes Unternehmen abzielt) bis hin zum Pretexting (Abgreifen vertraulicher Informationen durch einen fingierten Vorwand), kann Mitarbeiter dazu verleiten, betrügerische Websites zu besuchen und sensible Informationen einzugeben oder Malware auf ihre Geräte herunterzuladen und zu installieren. Obwohl die Häufigkeit der durch Phishing verursachten Verstöße zurückgeht,[7] wird Social Engineering in neuen Ausprägungen für Unternehmen weiterhin ein Problem bleiben.

- Bei 32 % aller Verstöße war Phishing im Spiel[12]
- 65 % der kriminellen Gruppen nutzen Spear-Phishing als primären Infektionsvektor[13]
- Rund 25 % aller Personen klicken einmal pro Jahr auf eine Phishing-Datei[15]
- Je mehr Phishing-E-Mails eine Person anklickt, desto größer ist die Wahrscheinlichkeit, dass sie erneut welche anklicken wird.[15]

„Statistisch gesehen sind die Mitarbeiter oft das schwächste Glied. Aber sie haben nicht unbedingt Schuld. Mitarbeiter müssen mit der richtigen Technologie ausgestattet sein. Sie brauchen Systeme mit integrierter Sicherheit, die ihnen hilft, sich in diesem endlosen Raum potenzieller Sicherheitsverletzungen und Angriffsvektoren zurechtzufinden."

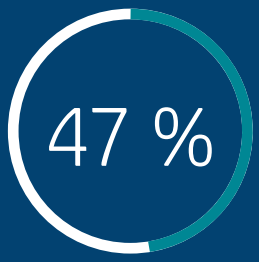
Michael Calce, genannt „MafiaBoy", Vorsitzender des HP Security Advisory Board

Wo menschliches Versagen Schwachstellen mit sich bringt, müssen Entscheider neue Wege finden, um den Rest des Netzwerks zu schützen. Interne Schulungen und Richtlinien können dazu beitragen, die Anfälligkeit zu verringern. Doch die Einführung von sicherer Hardware, Lösungen zum Schutz vor Bedrohungen und Managed Services kann die Verteidigungslinie stärken und Sicherheitslücken schließen.

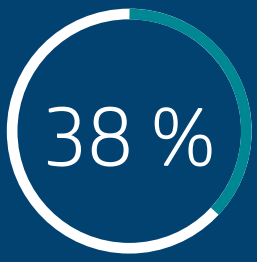
FINANZIELLE FOLGEN SIND NICHT DAS EINZIGE

Datenverletzungen kosten Unternehmen oft mehr als „nur" Geld: Das Vertrauen der Partner, die Loyalität der Kunden und der gesamte Ruf der Firma stehen auf dem Spiel. Tatsächlich sind es insbesondere die Arbeitsmoral der Mitarbeiter und die Geschäftsbeziehungen, die durch Cyberkriminalität in Mitleidenschaft gezogen werden.

Ausmaß der Beeinträchtigung[16]



Arbeitsmoral der Mitarbeiter



Geschäftsbeziehungen

Ruf/Markenwert

06 SICHERHEITSANFORDERUNGEN FÜR IHRE NÄCHSTE AUSSCHREIBUNG

„Die signaturbasierte Erkennung macht heute einen großen Teil der traditionellen Sicherheitstechnologien aus, und das genügt einfach nicht mehr. Ich bin wirklich begeistert davon, was HP mit HP Sure Sense entwickelt hat. Es handelt sich dabei im Wesentlichen um verhaltensbasierte Erkennung im Gegensatz zur signaturbasierten Erkennung. Es werden also zahlreiche Abwehrmaßnahmen ergriffen, um auf Angreifer zu reagieren."

Michael Calce, genannt „MafiaBoy", Vorsitzender des HP Security Advisory Board

Auch wenn die aktuellen Vorhersagen für Bedrohungsszenarien, Schwachstellen und Risiken nicht allzu sonnig erscheinen: Die richtigen Fragen zu stellen, kann dazu beitragen, Ihr Unternehmen mit dem richtigen Schutz auszustatten. Ihre Hardware– und Serviceanforderungen sollten das wandelbare Gesicht der Cybersicherheit widerspiegeln und Ihre IT–Abteilung bei der Bewältigung aktueller und zukünftiger Risiken unterstützen. Es ist daher ein Muss, bei der Anschaffung neuer Ressourcen den Sicherheitsaspekt zu priorisieren. Denken Sie über robuste Hardware, Schutzebenen und proaktives Management nach.

WELCHE ANFORDERUNGEN HEUTE IN KEINER AUSSCHREIBUNG FEHLEN DÜRFEN

Sie sind auf der Suche nach einem neuen IT-Anbieter? Die folgenden fünf Kernbereiche sollten Sie auf jeden Fall in Ihre Ausschreibung aufnehmen, wenn Sie in der Lage sein wollen, der steigenden Flut von Sicherheitsbedrohungen gut gewappnet begegnen zu können.

1 HARDWARE

Lassen Sie nicht zu, dass Malware oder Ransomware Ihre Geräteflotte und wichtige Projekte zum Erliegen bringen. Entscheiden Sie sich für Hardware, die darauf ausgelegt ist, Angriffe zu erkennen und sich anschließend selbst wiederherzustellen. Hardware, die Sie über Veränderungen informiert und die Verbreitung von Sicherheitsrisiken einschränkt, sodass Ihre Nutzer im Falle eines Angriffs schnell wieder den herkömmlichen Betrieb aufnehmen können.

Lösung: HP Sure Start,[17] HP Sure Run[18] und HP Sure Recover[19] sorgen für widerstandsfähige Hardware, die sich selbst überwacht und selbst heilt.

- HP Sure Start sichert Ihre PCs mit einem hardwaregestützten selbstheilenden Schutz, der das BIOS automatisch wiederherstellt, noch bevor der PC in sein Betriebssystem hochfährt.
- HP Sure Run hält kritische Sicherheitsmaßnahmen aufrecht, um unerwünschte Einstellungsänderungen zu verhindern.
- HP Sure Recover gewährleistet eine schnelle, sichere und automatisierte Wiederherstellung Ihres Betriebssystems über eine integrierte Reimaging-Funktion, wobei lediglich eine Netzwerkverbindung erforderlich ist.

2 SCHUTZ GEGEN BEDROHUNGEN

Eine von zehn URLs führt zu Malware,[13] also muss Ihr Unternehmen Endgeräte vor böswilligen Websites und Anhängen schützen. Halten Sie Ausschau nach robusten Hardware-Funktionen, die neue Risiken erkennen und Ihre Systeme in Echtzeit gegen die ausgeklügelte Malware schützen, die Mitarbeiter und herkömmliche Virenschutzprogramme mitunter übersehen.

Lösung: HP Sure Click[20] isoliert automatisch infizierte Dateien und böswillige Websites, damit Ihre Nutzer und Systeme beim Klicken geschützt sind. Dank der Künstlichen Intelligenz (KI) mit Deep–Learning–Technologie von HP Sure Sense[21] sind Sie auch vor Angriffen gewappnet, die nie zuvor aufgetreten sind.

3 ANALYSEN UND EINBLICKE

Wenn Sie jederzeit über den Gesundheits– und Schutzstatus Ihrer Geräte informiert sind, kann Ihr IT–Team Probleme lösen, bevor sie sich auf die Nutzer auswirken. Sie erhalten Zugriff auf Analysen und Berichte zu Sicherheitsvorfällen, um Bedrohungen zu identifizieren, Sicherheitsrichtlinien durchzusetzen und dank der erforderlichen Informationen und Einblicke Ihre Geräte und Daten zu schützen.

Lösung: HP Proactive Management mit HP TechPulse setzt einzigartige vorausschauende Analysen ein, um einen ganzheitlichen Blick auf den Geräteschutz zu liefern. Außerdem stellt die Technologie Berichte und Warnmeldungen über ungeschützte Geräte und versuchte Bedrohungen bereit, um Sie bei der Überwachung und Eindämmung von Sicherheitsproblemen zu unterstützen.

MANAGED SERVICES

IT–Sicherheitsteams sehen sich mit vielen komplexen, aufwendigen Routinearbeiten konfrontiert, die wenig Zeit für andere Prioritäten lassen. Arbeiten Sie mit einem Anbieter zusammen, der Managed Services anbietet, um den Zustand der Geräte im Blick zu behalten.

In der IT herrscht ein weltweiter Fachkräftemangel. Weltweit sind derzeit rund 2,93 Millionen Stellen im Bereich Cybersicherheit unbesetzt,[22] und voraussichtlich wird diese Zahl bis 2030 auf 85 Millionen ansteigen – das entspricht der Bevölkerung Deutschlands.[23] Könnte Ihr IT–Team da nicht ein wenig Unterstützung gebrauchen?

Lösung: HP Proactive Security[24] ist die weltweit fortschrittlichste isolationsbasierte Sicherheitslösung für Malware–Schutz in Echtzeit auf PCs unter Windows 10.[25] Ergänzend können unsere HP Service–Experten[26] Ihr IT–Team entlasten, indem sie Sicherheitsrichtlinien durchsetzen und tägliche Managementaufgaben durchführen, um den Zustand Ihrer Multi–OS–Umgebung zu überwachen.

5 GERÄTEAKTUALISIERUNG

Die heutige IT–Landschaft ändert sich ständig, und mit ihr die Sicherheitsziele. Unternehmen müssen sicherstellen, dass ihre Geräte in regelmäßigen Intervallen aktualisiert werden. Denn nur, wenn sie mit den neuesten Technologien und aktuellen Sicherheitsfunktionen ausgestattet sind, können sie mit den sich entwickelnden Cyberbedrohungen Schritt halten.

Lösung: HP Services für jede Phase des Gerätelebenszyklus helfen Ihnen, Ihre IT–Ressourcen zu optimieren, Nutzer mit der neuesten Technologie auszustatten und die sichere Außerbetriebnahme von Geräten zu gewährleisten, um wertvolle Daten zu schützen.

07 DIE RICHTIGEN FRAGEN, UM IHR SICHERHEITSLEVEL ZU ERHÖHEN

Welche Erwartungen hat Ihr Unternehmen an die Sicherheit seiner Geräte und Netzwerke? Um Ihre Anforderungen präzise zu umreißen, sollten Sie im Gespräch mit potenziellen Anbietern die zentralen Hardware- und Servicebereiche vertiefen und gezielte Fragen stellen. So können Sie sicherstellen, dass Sie sich für einen Partner entscheiden, mit dem Sie zusammenarbeiten möchten und der Sie dabei unterstützt, Ihr Unternehmen umfassend zu schützen. Stellen Sie die folgenden zehn Fragen, um Ihre Anforderungen zu ermitteln und Ihre Überlegungen auszuweiten.

1

Kann sich Ihre Hardware selbst schützen und nach modernen Malware-Attacken selbsttätig wiederherstellen?

Fragen Sie nach hardwaregestütztem Schutz und danach, was im Falle eines Angriffs wiederhergestellt werden kann und wie lange dies dauert.

2

Werden wir in der Lage sein, böswillige Aktivitäten aktiv zu überwachen?

Finden Sie heraus, ob Sie Zugang zu Einblicken, Berichten und Analysen haben, die Ihnen helfen, Bedrohungen zu erkennen und darauf zu reagieren.

3

Welche Einzelheiten erfahren wir, wenn ein versuchter Angriff stattgefunden hat?

Informieren Sie sich darüber, welche Inhalte und Analysen Sie erhalten und inwiefern diese hilfreich sind, um Angriffe auf Ihr Unternehmen besser verstehen zu können.

4

Welche Funktionen bieten Sie im Bereich vorausschauende Analyse?

Stellen Sie fest, ob Sie Zugang zu einer Analysetechnologie haben, die Probleme frühzeitig erkennen kann, um Sie vor Angriffen zu schützen.

5

Welche Technologien bieten Sie an, die es ermöglichen, nie da gewesene Bedrohungen zu erkennen und aufzuhalten?

Finden Sie heraus, ob Sie von Künstlicher Intelligenz (KI) mit Deep–Learning–Technologie profitieren können, die Malware instinktiv erkennt und in Echtzeit reagiert.

6

Welche zusätzlichen Datenschutzoptionen können Sie anbieten?

Fragen Sie nach Funktionen wie Datenlöschung, Bildschirm mit integriertem Blickschutz oder Fernsperre zum Schutz sensibler Daten.

7

Wie sind Sie in der Lage, die Verbreitung von Viren zu verhindern?

Isolationstechnologie kann Malware, die über URLs, Anhänge oder Dateien ins System eindringt, eindämmen und vor ihr schützen. Finden Sie heraus, ob Sie davon profitieren können.

8

Können Sie uns bei der Durchsetzung unserer Richtlinien helfen, und werden uns Support–Experten zur Verfügung stehen?

Stellen Sie sicher, dass Sie auf Fachwissen zugreifen können, um Ihren Sicherheitsschirm zu optimieren und Ihre internen IT–Teams zu entlasten.

9

Wie lauten Ihre Bedingungen bezüglich der Aktualisierung von Geräteflotten?

Finden Sie heraus, wie häufig Sie Ihre Geräte aktualisieren können, um ein Höchstmaß an Sicherheit zu gewährleisten.

10

Wie entsorgen Sie ausgemusterte Geräte?

Stellen Sie sicher, dass Prozesse zum Schutz von Daten angewendet werden, wenn Geräte das Ende ihres Lebenszyklus erreicht haben.

Cyberangriffe werden immer häufiger und immer raffinierter, doch Unternehmen können sich dagegen wehren – mit starken Sicherheitslösungen und einer lückenlosen Sicherheitsstrategie. HP stellt Ihnen ein umfassendes Portfolio an Hardwarefunktionen und Services bereit, die Sie aktiv dabei unterstützen, den Schutz Ihres Unternehmens zu gewährleisten. Mit unserer HP Elite Serie nutzen Sie die sichersten PCs der Welt.[27] Und mit HP Services profitieren Sie von proaktivem Schutz – für Ihren guten Ruf und die Zukunft Ihres Unternehmens.

HP Sicherheitslösungen können Ihre Geräte, Ihre Daten und Ihre Identität absichern und Ihr Unternehmen vor neuen Cyberbedrohungen schützen.

Jetzt mehr erfahren

QUELLENANGABEN UND HAFTUNGSAUSSCHLUSS

1 IWG, „The IWG Global Workplace Survey", März 2019. http://assets.regus.com/pdfs/iwg-workplace-survey/iwg-workplace-survey-2019.pdf
2 Buffer, „Zum Stand der mobilen Arbeit", 2019. https://buffer.com/state-of-remote-work-2019.
3 HR Dive, „Mitarbeiter nutzen persönliche Geräte zum Arbeiten ohne umfassende Aufsicht", Mai 2019. https://www.hrdive.com/news/employees-use-personal-devices-for-work-without-much-oversight/523913/.
4 Ponemon in Zusammenarbeit mit Accenture, „Die Kosten der Cyberkriminalität", März 2019. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study.
5 Telegraph, „Millionen Nutzerdaten von Facebook bei Datenverstoß offengelegt", April 2019. https://www.telegraph.co.uk/technology/2019/04/03/millions-facebook-user-records-exposed-data-breach/.
6 Fortune, „Facebook verliert rund 13 Mrd. US-Dollar an Wert nach einem Datenverstoß, der 50 Millionen Nutzer betrifft", September 2018,
7 Verizon, „2019 Data Breach Investigations Report", 2019. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf.
8 Ciso Mag, „Baltimore-Hacker veröffentlichen Daten auf Twitter, nachdem kein Lösegeld bezahlt wurde". https://www.cisomag.com/baltimore-hackers-leak-data-on-twitter-after-no-ransom-was-paid/.
9 aus einem Interview von Dave Davies im Rahmen des Radioprogramms „Fresh Air with Terry Gross", produziert von WHYY, Inc. und ausgestrahlt von NPR, Juni 2019, „Hacker fordern Lösegeld und legen Computersysteme in US-Städten lahm" https://www.npr.org/2019/06/13/732320853/hackers-demanding-ransoms-paralyze-city-computer-systems-in-the-u-s?t=1566209375528.
10 Guardian, „Australian National University von schwerem Datenverstoß betroffen", Juni 2019. https://www.theguardian.com/australia-news/2019/jun/04/australian-national-university-hit-by-huge-data-breach.
11 McAfee, „McAfee Labs Threats Report", Dezember 2018. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf?zanpid=2566983967299851264.
12 Ponemon, „Zum Stand der Endgerätesicherheit" https://cdn2.hubspot.net/hubfs/468115/whitepapers/state-of-endpoint-security-2018.pdf.
13 Symantec, „2019 Internet Security Threat Report". https://www.symantec.com/en/uk/security-center/threat-report.
14 Proofpoint, Report „Beyond the Phish", 2019. https://www.proofpoint.com/uk/resources/threat-reports/beyond-phish.
15 Verizon, „2018 Data Breach Investigations Report", 2018.
16 PwC, „Global Economic Crime and Fraud Survey", 2018. https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018.pdf.
17 HP Sure Start Gen5 ist auf ausgewählten HP PCs mit Intel Prozessoren® verfügbar. Hinweise zur Verfügbarkeit finden Sie in den Produktspezifikationen.
18 HP Sure Run Gen2: Hinweise zur Verfügbarkeit finden Sie in den Produktspezifikationen.
19 HP Sure Recover Gen2: Hinweise zur Verfügbarkeit finden Sie in den Produktspezifikationen. Erfordert eine offene, kabelgebundene Netzwerkverbindung. Nicht auf Plattformen mit mehreren internen Speicherlaufwerken verfügbar. Sie müssen wichtige Dateien wie Daten, Fotos, Videos sichern, bevor Sie HP Sure Recover nutzen, um Datenverluste zu vermeiden. Plattformen mit Intel® Optane™ werden von HP Sure Recover (Gen1) nicht unterstützt.
20 HP Sure Click ist auf ausgewählten HP Plattformen verfügbar und unterstützt Microsoft Internet Explorer, Google Chrome™ sowie Chromium™. Unterstützt werden u. a. Anhänge in Form von Microsoft Office (Word, Excel, PowerPoint) und PDF-Dateien im schreibgeschützten Modus, wenn Microsoft Office bzw. Adobe Acrobat installiert sind.
21 HP Sure Sense erfordert Windows 10. Hinweise zur Verfügbarkeit finden Sie in den Produktspezifikationen.
22 ISC2, „Experten für Cybersicherheit konzentrieren sich auf die Entwicklung neuer Fähigkeiten, da immer weniger Fachkräfte zur Verfügung stehen", 2018.
https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx.
23 Korn Ferry, „Der 8,5-Billionen-US-Dollar-Fachkräftemangel", Mai 2018. https://www.kornferry.com/institute/talent-crunch-future-of-work.
24 HP Proactive Security separat für Windows 10 Geräte erhältlich, unabhängig vom Hersteller.
Weitere Systemanforderungen finden Sie unter www.hpdaas.com/requirements. Erfordert HP TechPulse, das in jedem HP DaaS oder HP DaaS Proactive Management Plan enthalten ist. HP Service-Experten sind nur im Rahmen des Proactive Security Enhanced Serviceplans verfügbar.
25 Basierend auf einer internen Analyse von HP zu Sicherheitsservices mit Isolationstechnologie, die SaaS und Managed Services anbieten, welche eine integrierte und konfigurierte Analyse zur Durchsetzung der Compliance und zur Analyse von Malware-Bedrohungen umfassen. „Die weltweit fortschrittlichste" basierend auf hardwaregestütztem Virtual-Machine-Isolationsschutz (VM) mit der Isolierung individueller Browser-Tabs und Anwendungen (Stand: März 2019).
26 HP Service-Experten, die Bedrohungsanalysen durchführen und Isolationsaktivitäten für HP Proactive Security überwachen, sind nur im Rahmen des erweiterten Serviceplans verfügbar.
27 Basierend auf den einzigartigen und umfassenden Sicherheitsfunktionen von HP, ohne zusätzliche Kosten, und der Verwaltung durch das HP Manageability Kit eines jeden Bereichs eines PCs, einschließlich Hardware, BIOS und Softwareverwaltung mithilfe des Microsoft System Center Configuration Manager unter Anbietern mit > 1 Million verkauften Einheiten pro Jahr (Stand: November 2016) von HP Elite PCs mit Intel® Core® Prozessoren der 7. Generation oder höher, Intel® integrierten Grafikkarten und Intel® WLAN.

4AA7-6415DEE, November 2019

VIELEN DANK!

Ihren persönlichen Ansprechpartner
Jennifer Regh
erreichen Sie telefonisch unter:
+49 6571/9114-622

E-Mail:
jregh@softexpress.de

SoftExpress

SoftExpress GmbH
Zur Hohlwies 11
54533 Greimerath
www.softexpress.de