WHITE PAPER FÜR UNTERNEHMEN

SICHERHEIT BEGINNT BEIM ENDPUNKT

Gründe für eine Priorisierung der Endpunkt-Sicherheit

Präsentiert von

ZUSAMMENFASSUNG

82 % der Unternehmen hatten in den vergangenen 12 Monaten mit einer Cyber-Sicherheitsbedrohung zu tun.[1] Cyberangriffe treten nicht nur immer häufiger auf, sie werden auch schwerwiegender und kostenintensiver.

Die Präventions- und Schutzmassnahme eines Firewall-geschützten Netzwerk-Perimeters gehört der Vergangenheit an. Erkennen und reagieren ist weit effektiver.

Doch die Schnelllebigkeit von Cybersicherheit sprengt jedes IT-Budget. 77 % der Ausgaben werden nach wie vor in Präventions- und Schutzmassnahmen gesteckt.[2] Nur 36 % der IT-Sicherheitsmanager sehen sich finanziell für eine effektive Endpunktsicherheit gewappnet.[3]

Ein stabiler Datenschutz ist möglich. Mit der richtigen Technologie (von der Erkennung und Reaktion durch Sicherheitslösungen, bis zu einzelnen Geräten), der richtigen Strategie und genügend Ressourcen können sich Unternehmen vor Cyberkriminalität schützen.

Eine fehlende Mehrinvestition in Cybersicherheit und Neuausrichtung der Investitionen für wirklich effektive Abwehrmassnahmen führen zu häufiger auftretenden Sicherheitslücken und schliesslich zu höheren Kosten für das Unternehmen.

Einführung

Cybersicherheit im Zeitalter von unorganisierten Netzwerken
60 % der IT-Leiter sind der Meinung, dass das immer grösser werdende Volumen und die Komplexität von Cyberkriminalität ihre Abwehrmassnahmen sprengen. 80 % der Sicherheitsleiter stellen eine wachsende Bedrohung durch Advanced Persistent Threats (APTs), kriminelle Unternehmungen, staatlich unterstützte Hacker und Hacktivisten fest und sehen dies als vorrangige Herausforderung für die IT-Sicherheit.[4]

Sie liegen hiermit nicht falsch. Die britische Regierung schätzt die wirtschaftlichen Kosten von Cyberkriminalität auf 27 Mrd. GBP, „Tendenz signifikant steigend", während sich der Verlust für Unternehmen auf 21 Mrd. GBP beläuft.[5] Laut dem State of the Endpoint Report 2016 von Ponemon berichteten 78 % der Unternehmen von einem Anstieg von Malware-Angriffen, während es 2011 noch 47 % waren.

Doch der Fokus auf externe Bedrohungen ist etwas fehlgeleitet und kann zu einer Konzentration von Ressourcen zur Prävention und zum Schutz der Perimeter-Abwehr führen.

Obwohl externe Angriffe (Viren, Malware, Phishing) häufiger anfallen, schlagen interne Angriffe mit höheren Kosten zu Buche.[6] Viele jener externen Angriffe stammen von internen Schwachstellen: unachtsame Mitarbeiter ignorieren Sicherheitsprotokolle; ungesicherte Geräte werden an das Netzwerk angeschlossen. Von etwa 81 % der Teilnehmer an der Ponemon-Umfrage wurde dies als grösste Bedrohung für die IT-Sicherheit bestätigt.

Dies wird im Laufe der Zeit nicht besser. Der Endpunkt ist der Schwachpunkt jedes Netzwerks und durch die vermehrte berufliche Nutzung privater Geräte (BYOD; Bring Your Own Device), Telearbeit und das Internet der Dinge kommen noch mehr Endpunkte hinzu. Das bedeutet, dass die Anzahl der Zugänge für Hacker sich ebenfalls vervielfacht.

Im Vergleich zu den damaligen kontrollierten Netzwerken von über Ethernet verbundenen Desktop-PCs sind die heutigen Firmennetzwerke unorganisiert, ein Wirrwarr aus firmeneigenen und privaten Geräten, die über viele WLAN-Netzknoten intern oder extern auf Daten zugreifen.

Die Situation ist jedoch nicht ausweglos. Es ist einfach nur ein neuer Ansatz der Cybersicherheit gefragt. Neue Strategien, die sich dem Wandel von Cyberkriminalität anpassen. Eine neue Technologie, welche die zunehmende Komplexität einer wachsenden Bedrohung abwehren kann.

In diesem White Paper untersuchen wir Art und Ausmass der Bedrohung, um zu wissen, wie unser Feind tickt, bevor wir uns im Zeitalter verschiedener Geräte, ungesicherter Netzwerke und Cloud-Dienste die Frage stellen, wie wir Cybersicherheit umsetzen.

[1] HPI Printer Security Research 2016 (Spiceworks)
[2] PAC Incident Response Management 2015: https://www.pac-online.com/download/19443/155514
[3] Ponemon 2016 State of the Endpoint Report
[4] IBM CISO Assessment 2014
[5] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
[6] https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic

Das Ausmass der Bedrohung

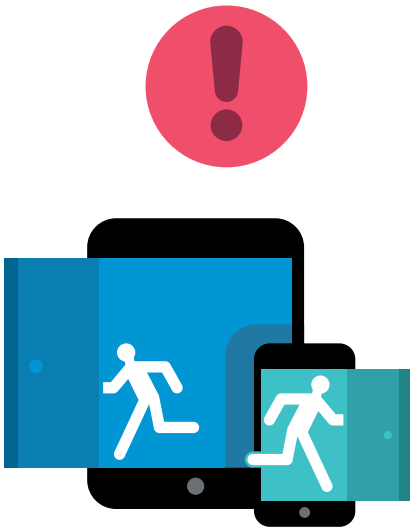
Unternehmen kostet es durchschnittlich 907.053 USD, um Datenschutzverletzungen zu beheben sowie einen Ertragsverlust von 13 %. Im Schnitt benötigt eine Organisation neun Wochen, um den Schaden zu beheben.[7]

Etwa 85 % der befragten Unternehmen im HP Printer Security Report 2015 sagten aus, dass sie in den letzten 12 Monaten mit einer Sicherheitsbedrohung/-lücke zu tun hatten. 80 % der teilnehmenden IT-Fachkräfte gingen von einem Anstieg der Bedrohung in den nächsten drei Jahren aus.[8]

Cyberkriminalität geht richtig ins Geld: Wertverlust durch die gestohlenen oder beschädigten Daten. Ertragsrückgang durch Reputations- und Produktionsverlust. Verlorene Ressourcen zur Schadensbehebung: Arbeitsaufwand durch Supportpersonal, Einführung neuer Sicherheitsrichtlinien, Personalmangel und andere interne Reaktionen. Bussgelder und Strafmassnahmen durch Aufsichtsbehörden. Fall des Aktienkurses.

Die Bedrohung steigt mit der Anzahl der Geräte, die an das Netzwerk angeschlossen sind. Gartner rechnet damit, dass es aufgrund des Internet der Dinge (IoT) bis 2018 11,4 Mrd. vernetzte Geräte geben wird, während es 2016 noch 6,4 Mrd. waren. Bis 2020 werden über 25 % der erkannten Angriffe auf Unternehmen IoT-bezogen sein. Das Internet der Dinge wird laut Prognosen hingegen weniger als 10 % des Sicherheitsbudgets ausmachen.[9]

Die Bedrohung durch Cyberkriminalität wächst weiterhin.



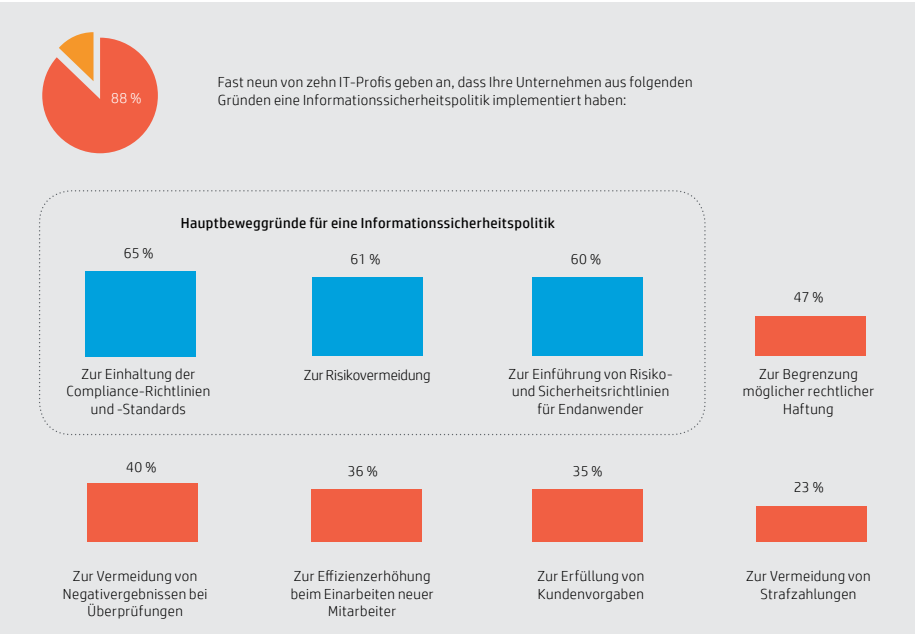
Die Gestalt der Bedrohung

Unternehmen sind tagtäglich von unzähligen Cyberangriffen betroffen. Beim Grossteil handelt es sich um geringfügige Angriffe durch Viren und Malware. 99 % der 2016 durch Ponemon befragten Unternehmen hatten in den vergangenen 12 Monaten mit Malware zu tun. Externe webbasierte Angriffe wie diese sind relativ harmlos und kosten die Organisationen durchschnittlich 4.639 USD.[10]

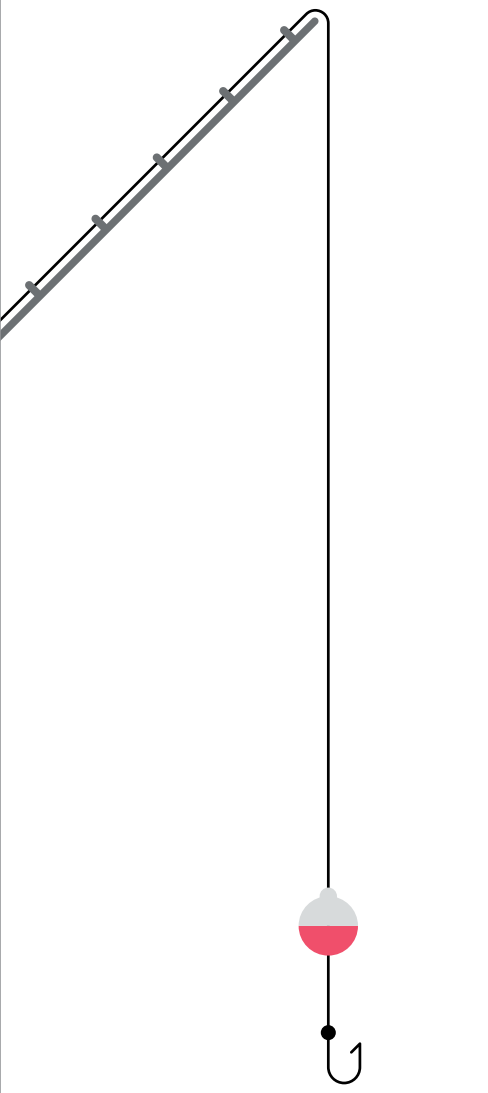
Die nicht so harmlosen Angriffe treten jedoch immer häufiger auf. 51 % der 2015 befragten Unternehmen hatten Erfahrung mit direkten Denial-of-Service (DDoS)-Angriffen, die lähmend sein und im Schnitt 127.000 USD kosten können. Noch alarmierender ist, dass 35 % mit einem bösartigen internen Angriff konfrontiert waren, der durchschnittlich 145.000 USD kostete.[9]

Es entsteht das Bild von unerbittlichen geringfügigen Angriffen von aussen und seltenen, aber erschreckend wahrscheinlichen gewichtigen Angriffen, die vermutlich durch interne Nachlässigkeit oder sogar Arglist entstehen. 62 % der Unternehmen hatten mit Angriffstypen wie Phishing und Social Engineering zu tun, bei denen die Schwachstellen von Mitarbeitern ausgenutzt wurden und durchschnittlich 86.000 USD kosteten.[11]

Eine unabhängige, im Auftrag von HP durchgeführte Umfrage durch Spiceworks untersuchte die Angriffe zwischen 2014 und 2015 auf 90 britische Firmen genauer.[12]



[7] NTT Security Risk:Value Report 2016
[8] HP 2Printer Security Report 2015
[9] http://www.gartner.com/newsroom/id/3291817
[10] https://ssl.www8.hp.com/ww/en/secure/pdf/4aa6-8392enw.pdf
[11] https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic
[12] HPI Printer Security Research, Spiceworks 2016



Wie Lücken entstehen

Die Schlagzeilen stellen unternehmerische Hacker als Bezwinger komplexer sicherer Netzwerke von Regierungen und Firmen dar, die Realität fällt aber gewöhnlich nüchterner aus.

Viren ziehen den Nutzen aus kompromittierten Netzwerken, während Malware meist auf Fehler durch Anwender angewiesen ist. Attacken in Form von Phishing/sozialem Engineering sind davon abhängig. Grosse DDoS- und Datendiebstahlangriffe sind oft auch das Ergebnis fahrlässiger Anwender.

Der mittlerweile berüchtigte Dropbox-Hack war angeblich das Ergebnis eines achtlosen Dropbox-Mitarbeiters, der für interne Systeme dasselbe Passwort verwendete wie für seinen LinkedIn-Account.[13] Der vermeintliche russische Hackangriff auf das DNC war offensichtlich John Podesta, dem ehemaligen Berater von Hillary Clinton, zuzuschreiben, als er einen Link in einer Phishing-E-Mail anklickte, die von einem Berater irrtümlich als „legitim“ eingestuft wurde.[14]

Hacker benötigen keine aktive Hilfe, um erfolgreich zu sein. Genauso gefährlich ist die Ignoranz bzw. die Missachtung von Sicherheitsprotokollen. Eine zunehmende Bedrohung ist die Verwendung von privaten Geräten in der Arbeit und die Nutzung gewerblicher Cloud-Dienste. Beide sind ungesicherte Elemente für ein ansonsten sicheres Netzwerk, entziehen sich der Kontrolle der Unternehmens-IT und lassen die Schwachstelle nicht zurückverfolgen.

Meistens müssen Hacker keine komplexen Algorithmen oder modernste Technik einsetzen, sondern benötigen nur einen etwas unachtsamen Anwender.

Die Firewall ist durchbrochen

Der Eckpfeiler von Cybersicherheit bestand bis vor kurzem aus Antiviren- und Firewall-Programmen. Prävention und Schutz. Realisieren eines sicheren Perimeters. In der aktuellen Arbeitsumgebung stellt dies keine zuverlässige Strategie dar.

81 % der von Ponemon Befragten sagten, dass mobile Geräte im Netzwerk das Ziel von Malware waren. Das Sicherheitsrisiko steigt auch, wenn Mitarbeiter gewerbliche Cloud-Anwendungen (von 72 % der Befragten bestätigt) oder BYOD (69 %) nutzen und vom Heimbüro bzw. an externen Standorten (62 %) arbeiten.[15]

Kurz gesagt, eine Firewall macht nur dann Sinn, wenn der Netzwerkadministrator noch kontrollieren kann, welche Geräte angeschlossen sind. Doch in einer Ära, wo Mitarbeiter ihre eigenen (oft mehrere und ohne Wissen der IT-Abteilung) Geräte beruflich nutzen und immer mehr Angestellte einen Fernzugriff haben, sind die Perimeter einfach nicht mehr zu schützen. Jedes nicht kontrollierte Gerät stellt einen für Hacker anfälligen Endpunkt dar.

[13] https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach

[14] https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0

[15] Ponemon 2016 State of the Endpoint Report

Die Lösung von HP: Gehen Sie über die Netzwerksicherheit hinaus!

Michael Howard, weltweiter Sicherheitsleiter von HP, zur Realisierung der Endpunkt-Sicherheit

Die aktuelle Hauptsorge besteht darin, dass Unternehmen aufgrund mangelndem Bewusstseins und Unkenntnis bestimmter Geräte und den damit verbundenen Risiken unbedingt jeden Endpunkt sichern wollen. Sie fühlen sich hinter einer Firewall sicher, auch wenn diese alleine vor Angriffen längst nicht mehr schützt. Sicherheitsbeauftragte müssen jeden Endpunkt innerhalb der Infrastruktur kennen und sicherstellen, dass jeder Endpunkt vielschichtig geschützt ist, um die immer komplexeren Angriffe abzuwehren.

Für Sicherheitsmitarbeiter ist es unabdingbar, jede Ecke ihrer betrieblichen IT-Infrastruktur zu untersuchen und zusätzlich zu den Standard-Netzwerkperimetern eine zusätzliche Schutzebene zu entwickeln. Firewalls alleine können komplexen Angriffen nicht standhalten. Zwingend erforderlich ist eine Abwehrmethode mit mehreren Schutzebenen je Endpunkt, um zu garantieren, dass Ihr Unternehmen die regulatorischen Anforderungen erfüllt und empfindliche Strafen vermeidet.

Die Richtlinien von HP besagen, dass bei jeder neuen Entwicklung in Form von Lösungen, Diensten oder Produkten Sicherheit an erster Stelle steht. Die Entwickler wissen, dass sie die Sicherheitsanforderungen erfüllen und wissen müssen, wie sie diese sicher in das Netzwerk integrieren.

Sicherheit sollte mehr denn je an erster Stelle stehen und nicht nur ein Zusatz sein. Seit Jahren wird diese Strategie von HP vertreten.

Sicherheitsebenen

Ein neuer Ansatz der Cybersicherheit muss vielschichtig sein.
Die Netzwerksicherheit ist nach wie vor wichtig, doch diese muss selbst aus separaten Netzwerken bestehen. Viele Sicherheitslücken liegen bei der ersten Eintrittsstelle, die Zugriff auf das gesamte System gewährt. Denken Sie nur an John Podestas Phishing-Fauxpas. Die Eingrenzung sensibler Daten in mehrere Datenzugriffsschichten ist erforderlich, so dass man mit einem gestohlenen Schlüssel nicht gleich die ganze Burg erobern kann.

Die Geräte müssen aufrüsten. IT-Leiter müssen unbedingt sicherstellen, dass jedes an das Netzwerk angeschlossene Gerät durch regelmässig aktualisierte Sicherheitsprogramme (gegen Viren, Malware und Spyware) geschützt und regelmässig nach Abweichungen durchsucht wird. Besser ist es, die Geräte selbst als Sensoren zu nutzen und Informationen in Echtzeit zu erfassen, um jede Lücke in ihrem Netzwerkparameter zu melden.

Jeder Mitarbeiter muss auf Cyber-Sicherheitsprotokolle geschult werden und es müssen umfassende Sicherheitskontrollen vorliegen. Menschliches Versagen, von Klicks auf den falschen Link bis hin zu Verbindungen zu einem Endgerät, stellt für das Netzwerk die höchste Bedrohung dar. Menschliches Versagen lässt sich anhand von Schulungen reduzieren.

Gerätesicherheit

Die vielleicht grösste Antwort auf moderne Cybersicherheit ist die Kontrolle darüber, welche Geräte Zugriff auf das Netzwerk haben.
Die naheliegendste und einfachste Lösung ist häufig der Einsatz von getrennten WLAN-Netzwerken für Gäste und Mitarbeiter, sodass ungesicherte externe Geräte keinen Zugriff auf das Hauptnetz haben. Dies geht Hand in Hand mit der Schulung von Mitarbeitern zur Nutzung dieses Netzwerks mit ihren privaten Geräten.

Als nächstes ist sicherzustellen, dass Sie Kontrolle über die Geräte der Mitarbeiter haben. Dies ist in den Unternehmensrichtlinien für BYOD bzw. CYOD (Choose Your Own Device) zu berücksichtigen. Es ist ein starkes Argument zugunsten von CYOD, das eine höhere Kontrolle darüber zulässt, welche Geräte verwendet (eine Wahl derjenigen mit besseren Sicherheitsfunktionen) und wie diese konfiguriert werden sowie die Verwaltung und Kontrolle dieser Geräte ermöglicht.

Die Verwendung eines unserer PCs aus der HP Elite-Reihe ist einem günstigen Laptop vorzuziehen. HP Elite-PCs verfügen über die HP SureStart-Technologie, die das BIOS alle 15 Minuten überprüft und das Gerät auf seinen Originalzustand zurücksetzt, sobald Abweichungen erkannt werden, und unerwünschte Eindringlinge abblockt. Diese und zahlreiche weitere Funktionen sorgten dafür, dass unser HP EliteBook x360 kürzlich als das „sicherste Business-Convertible der Welt“ ausgezeichnet wurde.[16] Doch Sie können nicht davon ausgehen, dass Mitarbeiter privat einen HP Elite PC besitzen.

Mitarbeiter möchten aus den folgenden zwei Gründen oft lieber ihr eigenes Gerät benutzen:
1. Die Verbrauchertechnologie ist häufig besser als die in der Arbeit
2. Mitarbeiter wollen die Technik benutzen, mit der sie vertraut sind

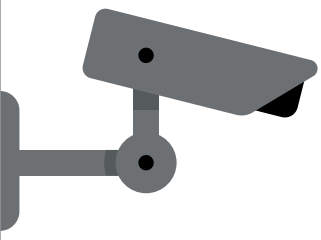
Durch eine gut ausgestattete CYOD-Politik, bei der regelmässig Aktualisierungen angeboten werden, können Unternehmen ihren Mitarbeitern bessere Geräte zur Verfügung stellen als ihre eigenen und zudem ein grösseres Mass an Kontrolle über die Sicherheit dieser Geräte haben. Genau dies sind die Alleinstellungsmerkmale unseres HP Device as a Service (DaaS).

Deshalb ist es wichtig, alle Geräte in die Sicherheitsstrategie einzubeziehen, sogar die oftmals vergessenen. Bei einer IDC-Umfrage meinten 80 % der Teilnehmer, dass die IT-Sicherheit für ihr Unternehmen wichtig sei, aber nur 59 % konnten dies von der Druckersicherheit behaupten, obwohl über die Hälfte in den vergangenen 12 Monaten mit einer druckerbezogenen Sicherheitslücke zu tun hatte. Dies ist offensichtlich ein Schwachpunkt.

Die durchschnittliche Anzahl von Sicherheitslücken vor der Implementierung einer Druckersicherheit war 9,9 pro Jahr bei Durchschnittskosten von 521.400 USD (inkl. Bussgelder). Nach der Einführung einer Druckersicherheit sank die Anzahl der Lücken im Schnitt auf 1,5; man sparte 200 Arbeitsstunden pro Jahr und 250.000 USD für damit verbundene Kosten, inkl. Audit und Compliance.[17]

[16] Sicherstes Gerät auf Grundlage der einzigartigen, umfassenden Sicherheitsfunktionen von HP, ohne zusätzliche Kosten; >1 Million Stück Jahresabsatz Stand 1. Dezember 2016 von HP Elite PCs mit Intel 7th Gen Intel® Core™-Prozessoren, Intel® Integrated Graphics und Intel® WLAN. Dünnstes Gerät auf Grundlage von Mitbewerbern mit >1 Million Stück Jahresabsatz, Convertibles ohne ablösbaren Bildschirm mit Windows Pro OS und Intel® Core™ vPro™-Prozessoren der 6. oder 7. Generation ab 1. Dezember 2016.

[17] IDC The Business Value of Printer Security 2015



Aktives Erkennen und Reagieren

Einer Umfrage durch PAC zufolge werden 77 % der IT-Sicherheitsaufwendungen für Präventions- und Schutztechnologien wie Antivirenprogramme und Firewalls ausgegeben. Doch dieser Ansatz ist wirkungslos. Die Untersuchung kam auch zu dem Ergebnis, dass 67 % der befragten Firmen in den letzten 12 Monaten, und 100 % irgendwann einmal, eine Cyberlücke hatten.[18]

Antivirenprogramme sind dabei erschreckend ineffektiv. Damballa führte Tests durch, bei denen sie absichtlich ein Netzwerk angriffen, um die Reaktion des Antivirenprogramms zu testen. Es dauerte sechs Monate, bis 100 % der bösartigen Dateien identifiziert wurden.[19] Dies steht im Einklang mit anderen PAC-Ergebnissen, nach denen es zwischen einem und sechs Monaten dauerte, bis Firmen Attacken bemerkten.

Die Sicherung von Endpunkten kann nicht länger der Prävention zugeschrieben werden. Die wachsende Anzahl der Viren-/Malwarevorfälle sowie die Unsicherheit von BYOD/mobilem Arbeiten bedeutet, dass Sicherheitslücken unvermeidlich sind. Niemand behauptet, dass Prävention und Schutz komplett abgeschafft werden sollen, doch müssen Erkennen und Reagieren eindeutig mehr im Fokus stehen.

Eine kontinuierliche Kontrolle in Echtzeit ist notwendig, idealerweise mit Endpunkten, die selbst als Sensoren fungieren und das restliche Netzwerk alarmieren, falls diese attackiert wurden. Somit kann die IT-Sicherheit per Fernwartung eingreifen, dazu gehören Prozesse wie:

- Abschalten eines Geräts per Fernwartung
- Abstellen eines infizierten Prozesses bzw. eines Prozesses, der Malware verbreitet
- Unter Quarantäne stellen einer bestimmten Datei oder einer Dateigruppe
- Unterbrechung von Netzwerkübertragungen, um infizierte Geräte zu isolieren[20]

Die Akzeptanz, dass diese Sicherheitslücken unvermeidbar sind, und die Einführung von angemessenen Response-Protokollen (sowie die Implementierung einer Technologie, um diese auszuführen) ist die einzige Lösung, um Cybersicherheit zu garantieren, wenn auf Prävention kein Verlass mehr ist.

„Keine Technologie garantiert Sicherheit, wenn sie von Menschen untergraben wird."

– Joseph Steinberg [21]

Sicherheit durch Mitarbeiter

Genauso wichtig, wenn nicht sogar wichtiger als die Absicherung des Gerätes selbst, ist die sichere Anwendung.
Jeder Mitarbeiter muss in Bezug auf Cybersicherheit geschult werden. Sie müssen sich der Risiken von Phishing bewusst sein. Der Risiken beim Besuch verdächtiger Websites. Der Risiken beim Herunterladen verdächtiger Anhänge. Sie müssen sich der sicheren Passwortanwendung bewusst sein, indem starke, einzigartige Passwörter für jede sensible Anmeldung sowie der korrekte Passwort-Manager zur Speicherung verwendet werden.

Sie müssen auf die Bedeutung dessen hingewiesen werden, das Sicherheitsprogramm auf ihrem Gerät regelmässig zu aktualisieren, um die IT-Abteilung von der Kontrolle zu entlasten. Sie müssen darauf achten, lediglich sichere Geräte zu verwenden, um auf Firmennetzwerke zuzugreifen, und vermeiden, mit privaten Geräten über externe, ungesicherte Netzwerke auf sensible Daten zuzugreifen.

Viele hochrangige Experten für Cybersicherheit empfehlen eine Durchführung simulierter Phishing-Angriffe, was so weit geht, dass Mitarbeiter durch fingierte Phishing-Websites getestet werden und somit die Schulung auf Cybersicherheit praxisbezogen wird. Da die meisten Angriffe menschliches Versagen ausnutzen, egal ob durch fahrlässiges oder bösartiges Handeln.

[18] PAC Incident Response Management 2015
[19] https://www.damballa.com/time-to-fix-malware-strategies-2/
[20] The Essential Endpoint Detection Checklist – HP Now
[21] https://digitalguardian.com/blog/data-security-experts-answer-what-biggest-misconception-companies-have-about-endpoint-security

Fazit

Anstatt in die IT-Sicherheit in Form von Prävention und Schutz zu investieren, sollte man sich auf Erkennungs- und Reaktionsmassnahmen am Endpunkt konzentrieren
Der Schutz von Firmendaten in der derzeitigen IT-Umgebung, die mit einer zunehmenden Bedrohung durch Cyberkriminalität und einem Kontrollverlust über die Netzwerkperimeter konfrontiert ist, benötigt zwei Dinge: eine Änderung des Konzepts und mehr Ressourcen.

Das Konzept eines Netzwerks muss geändert werden. Die Idee des Netzwerks als Absperrung um eine Auswahl an Geräten ist nicht mehr gültig. Es ist an der Zeit, der Wahrheit ins Auge zu sehen. „Das Netzwerk" ist ein Trugbild. Sie ergibt sich aus den angeschlossenen Geräten, jedes ein Endpunkt. Die Sicherung des Netzwerks ist gleichzusetzen mit der Sicherung des Endpunkts. Und jeder Endpunkt besteht aus zwei Elementen: dem Gerät und seinem Nutzer. Beides muss berücksichtigt werden.

Die Durchsetzung der Sicherheit bei diesem Paradigmenwechsel ist viel komplizierter als die primitive Umgebung vergangener Tage, bei der Desktop-PCs über Ethernet verbunden waren. Sie benötigt mehr Ressourcen und diese müssen durchgesetzt werden. Das haben 61 % der Ponemon-Teilnehmer erkannt.

Der Trick ist, den Rest des Unternehmens zu überzeugen. Lediglich 36 % der Teilnehmer meinten, dass ihnen genügend Gelder und Mitarbeiter für die Endpunkt-Sicherheit zur Verfügung ständen. 69 % sagen, dass der IT-Abteilung nicht genügend Mitarbeiter für mehr Support zur Verfügung ständen. 71 % meinten, dass Endpunkt-Sicherheitsrichtlinien schwer durchzusetzen wären.[22]

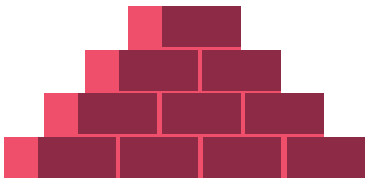
80 % der IT-Sicherheitsleiter finden, dass die Erfüllung gesetzlicher Auflagen die beste Methode sei, um die Förderung ihrer Sicherheitsprogramme zu rechtfertigen. Gleichzeitig bezeichnen sie die Konformität als den unwichtigsten Finanzierungsgrund. Konformität ist gleichzusetzen mit der Erfüllung des absoluten Minimums.[23]

IT-Entscheidungsträger müssen sich mit Mitgliedern der Vorstandsebene austauschen, um der Bedeutung der Sicherheit gerecht zu werden. Verdeutlichen Sie die Kosten einer laxen Sicherheit (Aufwendungen für eine Wiederherstellung, Ertragsverlust, Kursverlust von Aktien) und bringen Sie die langfristigen Einsparungen zum Ausdruck. Viele Sicherheitslösungen schaffen auch anderswo Verbesserungen. Denken Sie an die Produktivitätsverbesserung durch die Einführung einer Druckersicherheit und die Rentabilitätsvorteile durch regelmässig aktualisierte Technologien in einem flexiblem CYOD-Programm, das von einer Drittpartei bezogen werden kann (wie HP DaaS). Es kann ein eindeutiger wirtschaftlicher Nutzen entstehen.

Die Herausforderung ist gewaltig. Mit der explosionsartigen Verbreitung von Geräten im Bereich IoT sowie der zunehmenden Komplexität von Cyberkriminalität wird sie langfristig gesehen noch gewaltiger werden. Sie ist aber nicht unüberwindbar. Mit der richtigen Technik, der richtigen Strategie und den richtigen Ressourcen können wir unsere Endpunkte schützen. Wir können unsere Daten schützen.

Mehr über HP Device as a Service und wie Sie dadurch ein umfassendes, flexibles und sicheres CYOD-Programm ausführen, erfahren Sie **hier**.

Entdecken Sie ausserdem mehr über unsere bisher sicherste Gerätereihe, die **HP Elite-Reihe**, sowie über HPs Sicherheitslösungen **hier**.



Registrieren Sie sich, um Updates zu erhalten hp.com/go/getupdated

---

[22] Ponemon 2016 State of the Endpoint Report

[23] https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697