White paper

Sicherheit beginnt beim Endpunkt

Wenn es um IT-Sicherheit geht, sprechen viele Gründe dafür, am Endpunkt anzusetzen. Welche das sind, lesen Sie hier.

Brought to you by

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 Sicherheitsverantwortlichen stellen eine wachsende Bedrohung durch Advanced Persistent Threats (APTs) - kriminelle Unternehmungen durch staatlich unterstützte Hacker und Hacktivisten - fest und sehen dies als vorrangige Herausforderung für die IT-Sicherheit.

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 24,3 Mrd. EUR beläuft. Laut dem State of the Endpoint Bericht 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. Viele jener externen Angriffe stammen von internen Schwachstellen wie zum Beispiel unachtsame Mitarbeiter, die Sicherheitsprotokolle ignorieren oder ungesicherte, an das Netzwerk angeschlossene Geräte. 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 dem Internet der Dinge kommen noch mehr Endpunkte hinzu. Das bedeutet, dass sich die Anzahl der Zugänge für Hacker 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 Wi-Fi-Netzknoten intern oder extern auf Daten zugreifen.

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

Untersuchen wir also zunächst Art und Ausmaß der Bedrohung, um zu wissen, wie unser Feind tickt, bevor wir uns in einer Zeit verschiedenster Geräte, ungesicherter Netzwerke und Cloud-Dienste die Frage stellen, wie wir Cybersicherheit gewährleisten.

[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

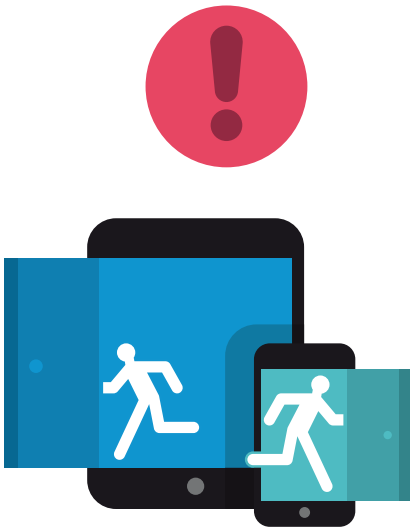
Unternehmen kostet es durchschnittlich rund 806.000 EUR, um Datenschutzverletzungen zu beheben sowie einen Ertragsverlust von 13 %. Im Schnitt benötigt eine Organisation neun Wochen, um den Schaden zu beheben.[7]

Etwa 85 % der befragten Unternehmen im HP Printer Security Report 2015 sagten aus, dass sie in den letzten 12 Monaten mit einer Sicherheitsbedrohung zu tun hatten. 80 % der teilnehmenden IT-Fachkräfte gehen 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, erhöhter 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 durch das Internet der Dinge (IoT) bis 2018 11,4 Mrd. vernetzte Geräte geben wird. 2016 waren es noch 6,4 Mrd. 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 und wächst.



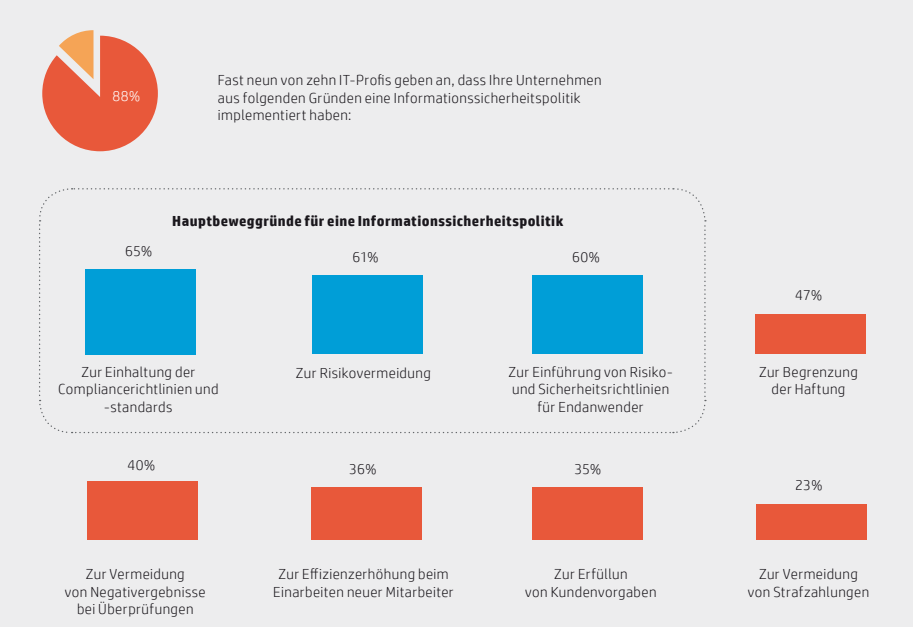
Die Gestalt der Bedrohung

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 etwa 4.100 EUR.[10]

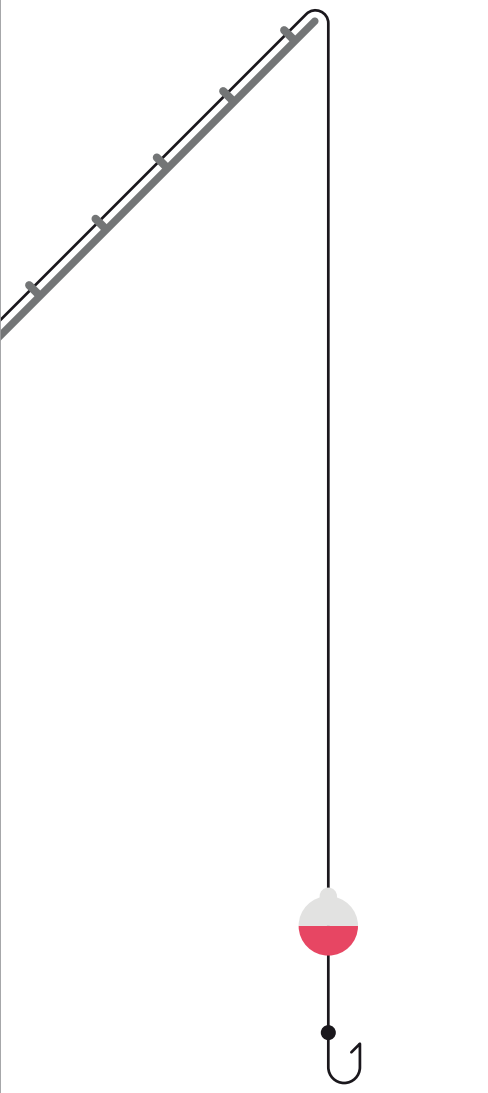
Jedoch treten die nicht so harmlosen Angriffe immer häufiger auf. 51 % der 2015 befragten Unternehmen hatten Erfahrung mit direkten Denial-of-Service (DDoS)-Angriffen, die lähmend sein können und im Schnitt bis zu 113.000 EUR kosten. Noch alarmierender ist, dass 35 % mit einem bösartigen internen Angriff konfrontiert waren, der durchschnittlich 129.000 EUR kostete.[9]

Es entsteht das Bild von unerbittlichen, aber geringfügigen Angriffen von außen auf der einen und seltenen, aber extrem gefährlichen Angriffen, die vermutlich durch interne Nachlässigkeit oder sogar Arglist entstehen, auf der anderen Seite. 62 % der Unternehmen hatten mit Angriffstypen wie Phishing und Social Engineering zu tun, bei denen die Schwachstellen von Mitarbeitern ausgenutzt wurden und durchschnittlich 76.500 USD kosteten.[11]

Eine unabhängige, im Auftrag von HP durchgeführte Umfrage durch Spiceworks teilte die Angriffe zwischen 2014 und 2015 auf 90 britische Firmen auf.[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] https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach



Wie Lücken entstehen

Die Schlagzeilen stellen Unternehmens-Hacker als Bezwinger komplexer und als sicher geltender Netzwerke. 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 oder sozialem Engineering sind ebenfalls von Anwendern abhängig. Und auch große DDoS- und Datendiebstahlangriffe sind häufig das Ergebnis fahrlässiger Mitarbeiter.

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 den 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. 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. Sie entziehen sich der Kontrolle der Unternehmens-IT und lassen die Schwachstelle nicht zurückverfolgen.

Meistens müssen Hacker daher gar keine komplexen Algorithmen oder modernste Technik einsetzen. Ihnen genügt ein etwas unachtsamer Anwender.

Die Firewall ist durchbrochen

Die Eckpfeiler von Cybersicherheit bestand bis vor kurzem aus Antiviren- und Firewall-Programmen, Prävention und Schutz sowie der Realisierung eines sicheren Perimeters. In der aktuellen Arbeitsumgebung stellt all dies keine ausreichend zuverlässige Strategie mehr dar.

81 % der von Ponemon Befragten gaben an, dass mobile Geräte im Netzwerk das Ziel von Malware waren. Das Sicherheitsrisiko steigt auch, wenn Mitarbeiter gewerbliche Cloud-Anwendungen (von 72 % der Befragten bestätigt), 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, in der Mitarbeiter ihre eigenen (oft mehrere und ohne die IT-Abteilung zu informieren) 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.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0
[14] Ponemon 2016 State of the Endpoint Report
[15] http://www8.hp.com/us/en/campaign/computersecurity/

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

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

Die aktuelle Hauptproblem besteht darin, dass Unternehmen aufgrund von mangelndem Bewusstsein und Unkenntnis bestimmter Geräte und den damit verbundenen Risiken nicht alle Endpunkte sichern können. Stattdessen fühlen sie sich hinter einer Firewall sicher – auch wenn diese alleine vor Angriffen längst nicht mehr schützt. Sicherheitsbeauftragte müssen jedoch jeden Endpunkt innerhalb der Infrastruktur kennen und sicherstellen, dass jeder dieser Endpunkte vielschichtig geschützt ist. Nur so können die immer komplexeren Angriffe abgewehrt werden.

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 daher eine Abwehrmethode mit mehreren Schutzebenen je Endpunkt. Dies garantiert, dass Ihr Unternehmen die regulatorischen Anforderungen erfüllt. Und auch empfindliche Strafen können so vermieden werden.

Für HP hat es oberste Priorität, dass bei jeder neuen Entwicklung – seien es Lösungen, Dienstleistungen oder Hardware-Produkte – Sicherheit an erster Stelle steht. Die Entwickler wissen, dass sie die Sicherheitsanforderungen erfüllen und diese in das Netzwerk integrieren müssen.

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

[16] http://www8.hp.com/us/en/campaign/computersecurity/

[17] IDC The Business Value of Printer Security 2015

Sicherheitsebenen

Ein neuer Ansatz der Cybersicherheit muss vielschichtig sein.
Die Netzwerksicherheit ist nach wie vor wichtig, doch diese muss selbst in fremden 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.

Auch bei den Geräten muss damit aufgerüstet werden. 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 zudem auf Cyber-Sicherheitsprotokolle geschult werden und umfassende Sicherheitskontrollen müssen ebenso vorliegen. Menschliches Versagen, vom Klick auf den falschen Link bis hin zum unsicheren Endgerät, stellen zwar für das Netzwerk die höchste Bedrohung dar, doch dies 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 Wi-Fi-Netzwerken für Gäste und Mitarbeiter, so dass ungesicherte externe Geräte keinen Zugriff auf das Hauptnetz haben. Dies geht Hand in Hand mit der Mitarbeiter-Schulung zur Netzwerk-Nutzung über private Geräte.

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. Für CYOD spricht, dass diese Regelung eine höhere Kontrolle darüber zulässt und welche Geräte verwendet werden. Auch Konfiguration, Verwaltung und Kontrolle dieser Geräte ist erleichtert.

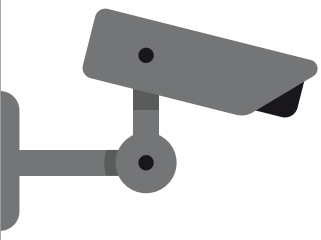
Warum Produkte aus der HP Elite-Reihe daher einem günstigen Laptop vorzuziehen sind? Jeder HP Elite PC verfügt über die HP SureStart-Technologie, die das BIOS alle 15 Minuten überprüft und das Gerät auf seinen Originalzustand zurücksetzt, sobald Unregelmäßigkeiten erkannt werden. Unerwünschte Eindringlinge werden zudem sofort abgeblockt. Diese und zahlreiche weitere Funktionen sorgten dafür, dass Computer aus der HP Elite 800-Serie kürzlich als die „sichersten Computer der Welt“ ausgezeichnet wurden. Doch Sie können nicht davon ausgehen, dass Mitarbeiter privat einen HP Elite PC besitzen und für berufliche Zwecke nutzen.

Und dennoch möchten Mitarbeiter aus zwei Gründen zumeist 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 haben zugleich mehr Kontrolle über die Sicherheit eben jener Geräte.

Es ist eminent wichtig, alle Geräte in die Sicherheitsstrategie einzubeziehen. 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 etwa 460.000 EUR (inkl. Bußgelder). Nach der Einführung einer Druckersicherheit sank die Anzahl der Lücken im Schnitt auf 1,5, man sparte 200 Arbeitsstunden pro Jahr und 222.000 EUR an damit verbundenen Kosten ein, inkl. Audit und Compliance.[17]



Aktives Erkennen und Reagieren

Einer Umfrage durch PAC zufolge werden 77 % der IT-Sicherheitsaufwendungen für Präventions- und Schutztechnologie 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 aufwiesen.[18]

Antivirenprogramme sind dabei erschreckend ineffektiv. Die US-amerikanische IT-Sicherheitsfirma 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. Dies steht im Einklang mit anderen PAC-Ergebnissen, nach denen es bis zu sechs Monate dauerte, bis Firmen Attacken bemerkten.

Die Sicherung von Endpunkten kann nicht länger der Prävention zugeschrieben werden. Die wachsende Anzahl der Viren- und Malwarevorfälle sowie die Unsicherheit durch BYOD bzw. mobile Arbeit bedeutet, dass Sicherheitslücken unvermeidlich sind. Niemand behauptet, dass Prävention und Schutz komplett abgeschafft werden sollen, doch Erkennen und Reagieren müssen 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 dieses attackiert wurde. Somit kann die IT-Sicherheit per Fernwartung eingreifen. Hierzu gehört:

- 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 zur Ausführung) sind die einzige Lösungen, 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. Dazu zählen Risiken beim Besuch verdächtiger Websites, Risiken beim Herunterladen verdächtiger Anhänge oder unsichere Passworte.

Mitarbeiter müssen mit Nachdruck darauf hingewiesen werden, das Sicherheitsprogramm auf ihren Geräten regelmäßig zu aktualisieren. Zudem müssen Mitarbeiter darauf achten, ausschließlich sichere Geräte zu verwenden, um auf Firmennetzwerke zuzugreifen, und sie müssen es vermeiden, mit privaten Geräten über externe, ungesicherte Netzwerke auf sensible Daten zuzugreifen.

Viele hochrangige Experten für Cybersicherheit empfehlen simulierte Phishing-Angriffe. Mitarbeiter werden dabei durch fingierte Phishing-Websites getestet , da die meisten Angriffe menschliches Versagen ausnutzen.

[18] https://www.damballa.com/time-to-fix-malware-strategies-2/
[19] The Essential Endpoint Detection Checklist – HP Now (wird verlinkt nach Veröffentlichung)
[20] https://digitalguardian.com/blog/data-security-experts-answer-what-biggest-misconception-companies-have-about-endpoint-security
[21] Ponemon 2016 State of the Endpoint Report

Fazit

Anstatt bei der IT-Sicherheit in Prävention und Schutz zu investieren, sollte man sich auf Erkennungs- und Reaktionsmaßnahmen am Endpunkt konzentrieren.
Der Schutz von Firmendaten, die mit zunehmender Cyberkriminalität und Kontrollverlust über die Netzwerkperimeter konfrontiert sind, benötigt zwei Dinge: eine Änderung des Konzepts und mehr Ressourcen.

Das Verständnis eines Netzwerks muss sich ändern. Die Idee eines Netzwerks als Zaun um die Geräte nicht mehr zeitgemäß. Blicken wir der Wahrheit ins Auge: „Das Netzwerk" ist ein Trugbild.Denn schließlich ergibt es sich aus den angeschlossenen Geräten, und jedes ist ein Endpunkt. Die Sicherung des Netzwerks ist dadurch gleichzusetzen mit der Sicherung der Endpunkte. Und jeder Endpunkt besteht aus zwei Elementen: dem Gerät und seinem Nutzer. Beides muss berücksichtigt werden.

Bei diesem Paradigmenwechsel die Sicherheit zu gewährleisten ist komplizierter als in der Umgebung vergangener Tage, bei der Desktop-PCs über Ethernet verbunden waren. Sie benötigt mehr Ressourcen und diese müssen ermöglicht werden.

Die Schwierigkeit besteht darin, den Rest des Unternehmens zu überzeugen. Lediglich 36 % der Teilnehmer meinten, dass ihnen genügend Gelder und Mitarbeiter für die Endpunkt-Sicherheit zur Verfügung stehen. 69 % gaben an, dass der IT-Abteilung nicht genügend Mitarbeiter für einen verbesserten Support zur Verfügung stehen. 71 % meinten, dass Endpunkt-Sicherheitsrichtlinien schwer durchzusetzen wären.[22]

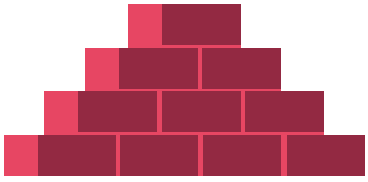
80 % der IT-Sicherheitsleiter fanden, dass die Erfüllung gesetzlicher Auflagen die beste Methode sei, um die Förderung ihrer Sicherheitsprogramme zu rechtfertigen. Gleichzeitig bezeichneten sie die Konformität als den unwichtigsten Finanzierungsgrund. Konformität ist gleichzusetzen mit der Erfüllung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

IT-Entscheidungsträger müssen sich mit Mitgliedern der Vorstandsebene austauschen, um der Bedeutung der Sicherheit gerecht zu werden. Sie sollten die Kosten einer laxen Sicherheit (Aufwendungen für eine Wiederherstellung, Ertragsverlust, Kursverlust von Aktien) und die langfristigen Einsparungen zum Ausdruck bringen. Viele Sicherheitslösungen schaffen zudem auch an anderen Stellen Verbesserungen. Denken Sie an die Produktivitätsverbesserung durch die Einführung einer Druckersicherheit und die Rentabilitätsvorteile durch regelmäßig aktualisierte Technologien in einem flexiblem CYOD-Programm (bspw. HP DaaS).
Der wirtschaftliche Nutzen kann somit vielschichtig sein.

Mit der explosionsartigen Verbreitung von internetfähigen Geräten durch IoT sowie der zunehmenden Komplexität von Cyberkriminalität wird die Aufgabe an die IT langfristig noch gewaltiger werden. Sie ist aber nicht unüberwindbar. Mit der richtigen Technik, der richtigen Strategie und den richtigen Ressourcen können alle Endpunkte geschützt werden.
Daten können auch in Zukunft geschützt werden.

Weitere Informationen und praktische Tipps von den HP-Experten erfahren Sie in unserem Sicherheitsleitfaden auf **hp.de/wissensdatenbank.**

Mehr über HP Device as a Service und wie Sie ein umfassendes, flexibles und sicheres CYOD-Programm implementieren, **erfahren Sie hier: www.hp.com/go/daas.**



Für Updates anmelden
hp.com/go/getupdated

4AA7-1089DEE

[22] Ponemon 2016 State of the Endpoint Report
[23] https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697