LEITFADEN

proofpoint.

SCHUTZ DER ANWENDER

EIN PERSONENORIENTIERTER ANSATZ ZUM UMGANG MIT SICHERHEITSLÜCKEN, ANGRIFFEN UND BERECHTIGUNGEN

proofpoint.com/de

HEUTIGE ANGRIFFE HABEN NICHT DIE INFRASTRUKTUR, SONDERN DEN MENSCHEN IM VISIER.

Unternehmen investieren stärker denn je in Cybersicherheit – und haben immer weniger Nutzen davon: Die Angriffe erreichen trotzdem ihr Ziel, vertrauliche Informationen erreichen in die falschen Hände und Datenschutzverletzungen schaffen es in die Schlagzeilen.

Es wird Zeit, das Thema Sicherheit grundlegend neu anzugehen. Bisherige Cybersicherheitsmodelle wurden für eine andere Zeit entwickelt, als das vorherrschende Sicherheitsmodell darin bestand, die Peripherie abzuriegeln und mit allen Bedrohungen fertig zu werden, die dennoch hindurch gelangten. Dieser Ansatz hatte schon damals gravierende Schwächen, doch heute ist er vollkommen chancenlos.

Der Grund: Das Hauptziel der Angreifer sind nicht Technologien, sondern die Menschen – und diese stellen damit Ihr größtes Risiko dar. Diese Veränderung der Bedrohungslage macht eine neue Denkweise und eine neue Strategie erforderlich, die sich auf den Schutz der Menschen und weniger auf die alte Peripherie konzentriert.

Doch wie sieht dieser neue Ansatz in der Praxis aus? Zur Beantwortung dieser Frage stellt dieser Leitfaden die grundlegenden Elemente eines modernen Sicherheitskonzepts vor.

Er beschreibt die für das Anwenderrisiko maßgeblichen Faktoren, gibt Hinweise zu ihrer Beseitigung und empfiehlt konkrete Schritte, mit denen Sie einen Schutz vor Angriffen aufbauen können, die auf den Menschen abzielen.

3 WARUM BEGINNT DER SCHUTZ BEIM MENSCHEN?

Jedes Jahr geben Unternehmen Milliardenbeträge für Cybersicherheits-Tools aus. Warum zeigt das nicht die erhoffte Wirkung?

SEITENLEISTE – SEITE 3

DIE KUNST DES DIEBSTAHLS

Der reale Ablauf einer Kompromittierung von Cloud-Konten, die den Angreifern Millionen einbrachte – und ohne Malware auskam.

4 BEWERTUNG DES ANWENDERRISIKOS: DAS VAP-MODELL

Bewertung des Anwenderrisikos durch das Abwägen von Schwachstellen, Angriffen und Kontoberechtigungen..

- SCHWACHSTELLEN
- ANGRIFFE
- BERECHTIGUNGEN

SEITENLEISTE – SEITE 5

VAP-SNAPSHOTS

Drei Beispiele für den Einsatz des VAP-Modells an einem Arbeitsplatz.

6 MINIMIERUNG VON ANWENDERRISIKEN: EIN SCHUTZKONZEPT, DAS DEN MENSCHEN IN DEN MITTELPUNKT STELLT

Voraussetzungen für die Minimierung von Sicherheitslücken, gezielte Abwehr von Bedrohungen und Verwaltung privilegierter Zugriffe.

- MINIMIEREN VON SICHERHEITSLÜCKEN
- ABWEHREN VON ANGRIFFEN
- VERWALTEN VON BERECHTIGUNGEN

WARUM BEGINNT SCHUTZ BEIM MENSCHEN?

Es ist offensichtlich, dass das bisher übliche Cybersicherheitsmodell der Peripherie-Verteidigung nicht funktioniert – und das schon seit Jahren nicht. In einer aktuellen Ponemon-Umfrage gingen mehr als zwei Drittel der IT-Sicherheitsexperten davon aus, dass Cyberangriffe den Börsenwert ihres Unternehmens ernsthaft beeinträchtigen würden. Und mehr als 50 % gehen davon aus, dass ihre Cybersicherheits-Lage gleich bleibt oder sich verschlechtert.[1]

Der Grund dafür sind zwei gegenläufige Entwicklungen: Die Peripherie löst sich auf, und Angreifer verlagern ihre Bemühungen weg von Technologien hin zu Menschen.

Und die Mauern stürzten ein

Es gibt einen einfachen Grund dafür, dass die Peripherie-Schutzmaßnahmen nicht funktionieren: In der heutigen mobilen Cloud-Wirtschaft gibt es keine definierte Peripherie mehr, die noch geschützt werden kann. Die Arbeit erfolgt auf vom Unternehmen nicht unterstützten Geräten, auf nicht verwalteten Infrastrukturen und in fremden Kanälen.

Gartner drückt das so aus: „Im Gegensatz zu früher hat die IT-Abteilung einfach keine Kontrolle mehr über die Begrenzungen der Informationen und Technologien."[2]

Menschen sind immer die besten Exploits

Nicht nur die Unternehmen wechseln in die Cloud, sondern auch die Angreifer. Die Cloud-Infrastruktur selbst mag äußerst sicher sein, doch ihre Anwender sind häufig sehr anfällig.

Aus diesem Grund verlassen sich aktuelle Angriffe eher auf das menschliche Verhalten als auf technische Schwachstellen. Mehr als 99 % aller heutigen Cyberangriffe werden von Menschen ausgelöst.[3] Die Angriffe setzen darauf, dass jemand ein manipuliertes Dokument öffnet, auf einen unsicheren Link klickt, Anmeldedaten eingibt oder gar die Anweisungen des Angreifers direkt umsetzt (z. B. Geld überweist oder vertrauliche Dateien sendet).

Anmeldedaten-Phishing, bei dem Anwender zum Eingeben ihrer Konto-Anmeldedaten in ein gefälschtes Formular verleitet werden, ist eines der gefährlichsten Beispiele. Im Zeitalter der Cloud sind diese Anmeldedaten der Schlüssel zu allem – E-Mails, vertraulichen Daten, privaten Terminen und vertrauensbasierten Beziehungen.

Im dritten Quartal 2018 vervierfachte sich die Zahl der Anmeldedaten-Phishing-Angriffe gegen Unternehmen im Vergleich zum dritten Quartal des Vorjahres.[4] Im gleichen Zeitraum stieg auch die Anzahl der E-Mail-Betrugsversuche um 77 %.[5]

DIE KUNST DES DIEBSTAHLS

Die Kompromittierung von Cloud-Konten bringt Angreifern Millionen ein – ganz ohne Malware

Das Folgende fand real bei einem Unternehmen statt, mit dem wir nach einem E-Mail-Betrugsangriff zusammengearbeitet haben. Aus Datenschutzgründen lassen wir einige Details aus.

Im vergangenen Jahr steckte ein CEO in einem intensiven Meeting und führte Verhandlungen mit einem wichtigen Geschäftspartner. Hunderte Kilometer entfernt arbeiteten Cyberangreifer, die sein Office 365-Konto übernommen hatten, an ihrer eigenen, heimlichen Transaktion.

Indem sie das vertrauliche Meeting nutzten und das Vertrauen in die direkten Anweisungen des Managers missbrauchten, konnten sie Millionenbeträge durch gefälschte Überweisungen erbeuten. Ihre einzigen Tools: E-Mails, Geduld und ein wenig Social Engineering.

Die Angreifer hatten Monate zuvor die Kontrolle über die Konten des CEOs erlangt, nachdem sie sein Kennwort in einer Brute-Force-Attacke erraten hatten. (Bei dieser Art von Angriff probieren Cyberkriminelle systematisch hunderte oder gar tausende Kennwörter aus, bis sie das richtige gefunden haben.)

Unerkannt konnten die Angreifer eine E-Mail-Weiterleitungsregel einrichten und so umfassenden Zugriff auf die vertraulichsten Geschäftsdaten des Unternehmens erlangen. Dadurch wussten sie, dass das Partner-Meeting anstand, worum es ging und wann der CEO weder telefonisch noch persönlich erreichbar sein würde.

Während das Meeting in vollem Gange war, erhielt eine leitende Mitarbeiterin der Finanzabteilung eine dringliche E-Mail vom E-Mail-Konto des CEOs: Er sei gerade in intensiven Geschäftsverhandlungen und für den erfolgreichen Abschluss sei schnell eine große Überweisung fällig. Da die Finanzmitarbeiterin nicht mit dem CEO Rücksprache halten konnte, erfüllte sie die Anweisung.

Die E-Mail stammte jedoch nicht vom CEO, die Kontodaten passten nicht zum Geschäftspartner und die üblichen Finanzkontrollen griffen nicht. Auf diese Weise erbeuteten die Angreifer Millionen US-Dollar – ohne eine einzige Malware-Infektion, Phishing-E-Mail oder ausgenutzte technische Schwachstelle.

[1] Ponemon Institute: „Umfrage zu weltweiten Megatrends im Bereich Cybersicherheit 2018", Februar 2018.
[2] Rob van der Meulen (Gartner): „Integration einer adaptiven Sicherheitsarchitektur in Ihr Unternehmen", Juni 2017.
[3] Proofpoint: „Der Faktor Mensch 2017", Dezember 2016.
[4] Proofpoint: „Vierteljährlicher Bedrohungsbericht, 3. Quartal 2018", Dezember 2018.
[5] ebd.

BEWERTUNG DES ANWENDERRISIKOS: DAS VAP-MODELL

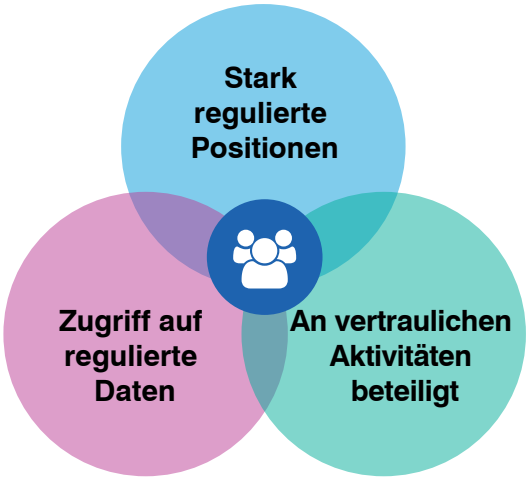
Ebenso wie jeder Mensch einzigartig ist, sind auch sein Wert für die Cyberangreifer und das Risiko für den Arbeitgeber individuell. Menschen haben ihre ganz eigenen digitalen Gewohnheiten und Schwachstellen. Sie werden von Angreifern mit unterschiedlichen Mitteln und wechselnder Intensität ins Visier genommen. Und jeder Mensch hat seine ganz eigenen beruflichen Kontakte und privilegierten Zugänge zu Daten im Netzwerk und in der Cloud.

Die Kombination dieser Faktoren bezeichnen wir als VAP-Index (für engl. Vulnerability, Attacks and Privilege – Schwachstellen, Angriffe und Berechtigungen).

Verständnis mitarbeiter-bezogener Risiken

SICHERHEIT

COMPLIANCE



Schwachstellen

Die erste Schwachstelle der Anwender ist ihr digitales Verhalten – wie sie arbeiten und worauf sie klicken. Manche Mitarbeiter arbeiten vielleicht aus der Ferne oder haben über ihre privaten Geräte Zugriff auf geschäftliche E-Mails. Sie können Cloud-basierte Dateispeicher nutzen und Drittanbieter-Add-Ons für ihre Cloud-Anwendungen installieren. Und einige von ihnen sind besonders empfänglich für die E-Mail-Phishing-Taktiken der Angreifer.

Die Arbeitsweise Ihrer Mitarbeiter

Die Bewertung der Schwachstellen, die durch die Arbeitsweise von Mitarbeitern entstehen, ist größtenteils unkompliziert – und wird doch durch herkömmliche Cyberschutzmaßnahmen erschwert oder gar unmöglich gemacht. Alles beginnt mit dem Wissen um die verwendeten Tools, Plattformen und Anwendungen.

Je detaillierter Ihre Übersicht, desto besser. Beispielsweise ist eine Einschätzung der Schwachstellen auf Anwenderebene nur dann möglich, wenn Sie einen zuverlässigen Überblick über die Anwender haben. In diesem Fall können Sie folgende Faktoren berücksichtigen:

- Verwendete Cloud-Anwendungen
- Anzahl und Art der Geräte, die für den E-Mail-Zugriff genutzt werden
- Sicherheitsstufe dieser Geräte
- Einhaltung der empfohlenen digitalen Vorgehensweisen durch die Anwender
- Nichtnutzung bzw. durchgehende Nutzung mehrstufiger Authentifizierung

Klickverhalten Ihrer Mitarbeiter

Im zweiten Teil der Ermittlung von Schwachstellen müssen Sie herausfinden, wie anfällig Ihre Anwender für Phishing und andere Cyberangriffe sind. Da Sie aus guten Gründen sicher nicht bereit sind, Angreifer eindringen zu lassen und zu schauen, wer eine Malware-Datei öffnet und Geld an den Angreifer überweist, sind Phishing-Simulationen die beste Möglichkeit, diesen Schwachstellen-aspekt zu analysieren.

Mit simulierten Angriffen, insbesondere wenn dabei real eingesetzte Techniken genutzt werden, lässt sich feststellen, welche Mitarbeiter für welche Taktiken anfällig sind.

Anwender, die eine simulierte Phishing-E-Mail und den darin enthaltenen Anhang öffnen, sind wahrscheinlich am stärksten gefährdet. Mitarbeiter, die darauf hereinfallen, schneiden schlechter ab, während diejenigen, die diese E-Mail an das Sicherheitsteam oder den E-Mail-Administrator melden, das geringste Risiko darstellen.

Angriffe

Nicht alle Cyberangriffe sind gleich. Während jeder einzelne Angriff potenziell gefährlich ist, sind einige schädlicher, gezielter oder raffinierter als andere.

Massenhafte „Standard"-Bedrohungen mögen zahlreicher sein als andere Bedrohungstypen, sie sind jedoch meist weniger gefährlich, da sie bekannt sind und leichter blockiert werden können. Andere Bedrohungen kommen vielleicht nur bei einigen wenigen Angriffen zum Einsatz, können jedoch eine größere Bedrohung darstellen, da sie raffinierter sind oder die „richtigen" Empfänger erreichen.

VAP-SNAPSHOTS

HOCH MITTEL GERING

Das VAP-Modell kann wie folgt auf Mitarbeiter in einem typischen Unternehmen angewendet werden.

Jana Becker, Geschäftsführerin

jbecker@beispiel.co

Schwachstellen

Keine ThreatSim-Aktion, nutzt externe Netzwerke und Geräte, inkonsequente Nutzung von mehrstufiger Authentifizierung

Angriffe

Top 10 % aller Anwender beim maximalen Bedrohungswert, davon insgesamt 30 Tage in den Top 5 %

Berechtigungen

Hat Zugriff auf vertrauliche Daten in Office 365 und das Unternehmensnetzwerk

Jana schneidet bei Phishing-Simulationen gut ab. Sie ist jedoch auch sehr viel unterwegs und meldet sich bei E-Mail-Postfächern und Dateifreigaben auf mehreren Geräten innerhalb sowie außerhalb des Unternehmensnetzwerks an. Ihr Bekanntheitsgrad macht sie zum Ziel von Malware- und Phishing-Angriffen, die häufig raffiniert und sehr gezielt erfolgen. Sie hat Zugang zu äußerst vertraulichen Daten und viele hochrangige Mitarbeiter unter sich, darunter solche, die Banküberweisungen tätigen können.

Maria Braune, Assistentin der Geschäftsleitung

mbraune@beispiel.co

Schwachstellen

Niedriger ThreatSim-Wert, nutzt vom Unternehmen gestellte Geräte im Netzwerk

Angriffe

Meist gewöhnliche Bedrohungen, einige jedoch gezielt und mit Social Engineering

Berechtigungen

Hat wenig Zugang zu vertraulichen Daten, kann jedoch E-Mails an die Geschäftsführerin senden und hat Zugriff auf Kalender

Maria arbeitet während der Bürozeiten mit ihrem unternehmenseigenen PC ausschließlich im Unternehmensnetzwerk. Gelegentlich öffnet sie jedoch E-Mails in Phishing-Simulationen. Angesichts ihrer Rolle könnte sie für E-Mail-Betrug empfänglich sein, der die Geschäftsführerin oder andere Führungskräfte imitiert. Neben einer großen Zahl an Standard-E-Mail-Bedrohungen erhält sie einige gezielte und Social-Engineering-E-Mails. Auch wenn sie keinen Zugriff auf vertrauliche Informationen hat, kann sie E-Mails ihm Namen der Geschäftsführung senden und hat Zugriff auf die Kalender der Führungskräfte.

Ernst Jung, Techniker

ejung@beispiel.co

Schwachstellen

Perfekter ThreatSim-Wert, nutzt externe Netzwerke und Geräte, inkonsequente Nutzung von mehrstufiger Authentifizierung

Angriffe

Top 1 % aller Anwender beim maximalen Bedrohungswert, davon insgesamt 30 Tage in den Top 3 %

Berechtigungen

Hat Zugriff auf äußerst wertvolle vertrauliche Daten

Ernst hält die empfohlenen digitalen Vorgehensweisen hervorragend ein, fällt auf keine simulierten Phishing-Angriffe herein, meldet verdächtige Nachrichten sofort und greift nur über VPN auf Unternehmensressourcen zu. Er wird jedoch überdurchschnittlich häufig angegriffen, wobei viele der Angriffe äußerst raffiniert sind. Während sein Netzwerk- und Dateizugriff auf seine eigene Abteilung beschränkt ist, enthalten viele dieser Dateien wertvolles geistiges Eigentum.

Umfangreiche Bedrohungsdaten und zeitnahe Einblicke sind der Schlüssel zur Ermittlung dieser Aspekte des Anwenderrisikos. Diese Faktoren sollten bei der Bewertung der Anwenderrisiken am schwersten wiegen:

- Raffinesse der Cyberkriminellen
- Umfang und Fokus der Angriffe
- Angriffstyp
- Angriffsvolumen insgesamt

Sie sollten diese Faktoren auch im Hinblick auf die Abteilungen, Gruppen oder Geschäftsbereiche gewichten, denen der einzelne Anwender angehört. Beispielsweise scheinen einige Anwender zunächst als nicht gefährdet, wenn nur die Menge oder die Arten der direkt an sie gesendeten schädlichen E-Mails berücksichtigt werden. Sie können jedoch tatsächlich ein größeres Risiko darstellen, da sie in einer sehr häufig attackierten Abteilung arbeiten – und daher in Zukunft eher ein wichtiges Ziel darstellen.

Berechtigungen

Bei den Berechtigungen werden alle potenziell hochwertigen Assets erfasst, auf die Menschen Zugriff haben (z. B. Daten, finanzielle Befugnisse, wichtige Beziehungen). Die Ermittlung dieses Risikoaspekts ist unverzichtbar, da er den potenziellen Gewinn für Angreifer repräsentiert – und das Unternehmen bei einer Kompromittierung schädigt.

Anwender mit Zugriff auf wichtige Systeme oder proprietäres geistiges Eigentum müssen beispielsweise selbst dann zusätzlich geschützt werden, wenn sie nicht außergewöhnlich anfällig sind oder die Angreifer sie noch nicht auf dem Radar haben.

Die Position des Anwenders im Organigramm ist natürlich ein Faktor bei der Bewertung der Berechtigungen. Sie ist jedoch nicht der einzige Faktor – und häufig noch nicht einmal der wichtigste. Für die Angreifer kann jeder ein lohnenswertes Ziel darstellen, der ihnen nützlich ist.

Laut unseren Untersuchungen machten Angriffe auf einzelne einfache Mitarbeiter und Abteilungsleiter etwa

67 %

der personalisierten Malware- und Phishing-Angriffe aus.

Angriffe auf Führungskräfte und hochrangige Manager

stiegen um 4 Prozentpunkte auf rund ein Drittel aller Angriffe.[6]

MINIMIERUNG VON ANWENDERRISIKEN: EIN SCHUTZKONZEPT, DAS DEN MENSCHEN IN DEN MITTELPUNKT STELLT

Der Schutz vor den Faktoren, die das Anwenderrisiko beeinflussen, erfordert einen mehrstufigen Ansatz. Im VAP-Modell bedeutet das:

- Verringerung der Anfälligkeit des Anwenders
- Stoppen von Bedrohungen, die auf sie abzielen
- Kontrolle ihrer Berechtigungen, um die Assets zu schützen, auf die sie Zugriff haben

Minimieren von Sicherheitslücken

Wenn es darum geht, Anwender gegenüber Cyberbedrohungen widerstandsfähiger zu machen, besteht der erste Schritt in der Kommunikation des Risikos. Deshalb sind Schulungen zur Sensibilisierung des Bewusstseins für Cybersicherheit unverzichtbar.

Die effektivsten Schulungsprogramme sind ansprechend, praxisnah und basieren auf Angriffstechniken, die im Alltag vorkommen. Da die Angreifer ihre Methoden ständig weiterentwickeln, müssen die Schulungen ständig auf dem neuesten Stand gehalten werden.

Es genügt nicht, einmal im Jahr eine Schulung über Sicherheitsbewusstsein in einem Schulungsraum durchzuführen. Wie bei jeder langfristigen Verhaltensänderung ist auch hier ein kontinuierlicher Prozess notwendig. Effektive Schulungsprogramme erfüllen folgende Aufgaben:

- Bewertung des Wissensstandes der Anwender
- Schulung der Anwender zu aktuellen Bedrohungen
- Festigung dieser Lektionen durch regelmäßige Auffrischung
- Überwachung der langfristigen Verhaltensänderungen

Insbesondere bei stark gefährdeten Anwendern können zusätzliche Unterweisungen sinnvoll sein. Das Herausstellen und Beheben von Fehlern in Echtzeit ist unverzichtbar. Anwender, die beispielsweise auf (reale oder simulierte) Phishing-E-Mails hereinfallen, sollten erfahren, worauf sie vor dem Klicken hätten achten müssen – und zwar noch während der Vorfall frisch in Erinnerung ist. Die zusätzlichen Unterweisungen sollten für jeden Anwender maßgeschneidert und relevant sein.

Die am wenigsten anfälligen Anwender erkennen die eingehenden Bedrohungen nicht nur, sondern melden sie auch. Je eher das geschieht, desto schneller können Sicherheitsteams sie noch am Gateway blockieren und – falls sie bereits übermittelt wurden – aus den Posteingängen der Anwender entfernen. Die Vereinfachung des Meldevorgangs stärkt Ihre Schutzmaßnahmen für die gesamte Umgebung.

Abwehren von Angriffen

Aktuelle Cyberangriffe sind hartnäckig, vielgestaltig und enorm wandlungsfähig. Selbst mit den besten Schulungen werden einige Anwender unter Umständen dennoch auf manche Bedrohungen klicken.

Der Schutz der Anwender bedeutet auch, dass nicht nur einige Arten von Angriffen, sondern Bedrohungen aus dem gesamten Angriffsspektrum abgewehrt werden – idealerweise, noch bevor sie deren Posteingänge erreichen.

[6] Proofpoint: „Menschen schützen: Eine Quartalsanalyse personalisierter Cyberangriffe“, November 2018.

Malware-Bedrohungen
Den meisten Unternehmen sind die Gefahren durch Malware bewusst. Oft bleibt dabei jedoch unberücksichtigt, auf welchen Wegen die Malware in ihre Umgebung gelangt und welche Rolle die Mitarbeiter dabei spielen.

Sehen Sie sich das typische Sicherheitsbudget an.

Über 80 % der Investitionen gehen in herkömmliche Infrastruktur-Schutzmaßnahmen,

obwohl die meisten Cyberangriffe sich gegen Menschen richten und meist per E-Mail erfolgen.[7]

Ganz gleich, ob es sich um Bank-Trojaner, Anmeldedaten-Diebe, Ransomware oder Remote-Zugriffs-Trojaner handelt: Die meisten Malware-Formen erfordern die Mithilfe des Opfers.

Malware-lose Bedrohungen
Bisherige Sicherheitskonzepte richteten sich ausschließlich gegen Malware-basierte Bedrohungen (und griffen viel zu oft erst, wenn diese bereits in die Umgebung eingedrungen waren). Doch viele der gefährlichsten Bedrohungen verwenden überhaupt keine Malware. Anstatt technische Schwachstellen zu hacken, nutzen sie die menschliche Natur aus.

Beispiele für Malware-lose Bedrohungen:

- Phishing
- Diebstahl von Anmeldedaten
- E-Mail-Betrug (auch bekannt als Business Email Compromise bzw. BEC)
- Kompromittierung von Cloud-Konten

Da diese Bedrohungen auf Social Engineering statt auf böswillige Schaddaten setzen, lassen sie sich mit Infrastruktur-fokussierten Schutzmaßnahmen schwerer erkennen und blockieren.

Webbasierte Bedrohungen
Das Web, einschließlich webbasierter Social-Media-Tools, ist eine der größten Quellen für Bedrohungen. Die meisten Menschen rufen während der Arbeitszeit ihre privaten E-Mails ab und surfen im Internet private Seiten an. Ein Großteil dieser Aktivitäten unterliegt keiner Kontrolle und ist potenziell gefährlich.

Die Absicherung großer Internetbereiche ohne Beeinträchtigung der eigentlichen Arbeit ist schwierig, wenn nicht gar unmöglich. Die Analyse der privaten Anwenderaktivitäten – die zudem immer häufiger standardmäßig verschlüsselt sind – ist kostenintensiv, beeinträchtigt die Netzwerkleistung und erfasst nicht alle Bedrohungen. Zudem führt sie potenziell zu Datenschutz- und Sicherheitsproblemen. Da die vollständige Blockierung der privaten Webnutzung von den meisten Anwendern als übermäßiger Eingriff gewertet würde und daher nicht in Frage kommt, lässt sich diese klaffende Sicherheitslücke kaum schließen.

Ein wesentlich einfacherer Ansatz ist die Isolierung der privaten Webaktivitäten, sodass sie von Anfang an nicht mit Ihrer Umgebung in Berührung kommen. Mithilfe von Technologien zur Webisolierung können Anwender frei im Internet surfen, ohne das Unternehmensnetzwerk irgendwelchen Bedrohungen auszusetzen. Sie können auch ihre privaten E-Mails abrufen, ohne neue Risiken einzuführen oder ihre Privatsphäre aufzugeben.

Verwalten von Berechtigungen

Für ihre Arbeit müssen viele Anwender auf vertrauliche Daten und andere Ressourcen zugreifen. Bei der Verwaltung von Berechtigungen geht es nicht darum, pauschal den Zugriff zu sperren oder autorisierten Anwendern die Arbeit zu erschweren. Sinnvoller ist es, den Zugriff zu kontrollieren, um die Schäden bei einer Kontenkompromittierung und einem unzulässigen Zugriff auf vertrauliche Daten zu minimieren.

Ein erster Schritt dabei ist die Feinanpassung der Zugriffsrechte. Verkaufsmitarbeiter eines Einzelhandelsunternehmens haben im Allgemeinen keinen Grund, auf Daten aus der Finanzabteilung zuzugreifen. Ebenso besteht für den CEO eines Gesundheitsanbieters keine Notwendigkeit, Patientenakten herunterzuladen. Wenn Sie sicherstellen können, dass die richtigen Mitarbeiter – und nur diese – auf die benötigten Daten zugreifen können, dämmen Sie die Schäden für den Fall ein, dass diese Anwender kompromittiert werden.

Zur Beseitigung von berechtigungsbezogenen Risiken gehört auch die zuverlässige Erkennung der Kompromittierung eines privilegierten Kontos. Ungewöhnliche Anmeldungen oder Aktivitäten sollten verschärfte Authentifizierungsmaßnahmen nach sich ziehen oder den Zugriff umgehend vollständig sperren. Wenn Angreifer ein privilegiertes Konto übernehmen können, erhalten sie damit ungehinderten Zugang zu den vertraulichen Daten, auf die normalerweise der Kontoinhaber Zugriff hat. Und jeder, der die Kontrolle über ein E-Mail-Konto erhält, kann Menschen ausnutzen, die diesem Konto vertrauen – innerhalb ebenso wie außerhalb des Unternehmens.

Gleichzeitig können von Anwendern eigenmächtig installierte Anwendungen und Drittanbieter-Add-ons ebenfalls Zugriff auf vertrauliche Daten erhalten. Deshalb sollten sie regelmäßig einem Audit unterzogen werden, um ihre Sicherheit zu gewährleisten. Selbst nicht explizit schädliche Anwendungen können schlecht konzipiert sein oder unzureichende Sicherheits- und Datenschutzrichtlinien haben, sodass sie ein zu großes Risiko für privilegierten Zugriff darstellen.

NÄCHSTE SCHRITTE: SCHUTZMASSNAHMEN, DIE SICH AUF DEN MENSCHEN KONZENTRIEREN

In der heutigen Cloud-unterstützten, mobilen und digital transformierten Arbeitswelt beginnt der Schutz beim Menschen. Daher benötigen Sie eine Lösung, die alle Aspekte des im VAP-Modell vorgestellten Anwenderrisikos abdeckt und folgende Vorteile bietet:

- Schwachstellen der Anwender minimieren
- Angriffe verhindern, abwehren und auf diese reagieren
- Netzwerkrechte überwachen und verwalten, um unzulässige Zugriffe auf vertrauliche Informationen zu verhindern

Proofpoint hat bei der Abwehr hochentwickelter Bedrohungen und Verhinderung von Compliance-Risiken stets einen Ansatz, der den Menschen in den Mittelpunkt stellt, propagiert. Unsere Lösungen konzentrieren sich auf den Schutz der Anwender, der von ihnen erstellten Daten sowie der digitalen Kanäle, die sie tagtäglich nutzen.

[7] Gartner: „2017 Security Spending Forecast“ (Prognose zu Sicherheitsinvestitionen 2017), August 2017.

Weitere Informationen dazu, wie wir mit dem VAP-Modell Menschen bei E-Mail, dem Web, Cloud-Anwendungen, Social Media und anderswo schützen, erhalten Sie unter **proofpoint.com/us/solutions/protecting-end-users**.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) ist ein führendes Cybersicherheitsunternehmen. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter. Denn diese bedeuten für ein Unternehmen zugleich das größte Kapital aber auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Cybersecurity-Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und IT-Anwender in den Unternehmen für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-100-Unternehmen, verlassen sich auf Proofpoint, um ihre wichtigsten Sicherheits- und Compliance-Risiken bei der Nutzung von E-Mails, der Cloud, Social Media und dem Internet zu minimieren.

© Proofpoint, Inc. Proofpoint ist eine Marke von Proofpoint, Inc. in den USA und anderen Ländern. Alle weiteren hier genannten Marken sind Eigentum ihrer jeweiligen Besitzer.