proofpoint.

2020

Strategischer Leitfaden E-Mail-Sicherheit

Ein personenorientierter Ansatz, um Malware, Phishing und E-Mail-Betrug zu stoppen

ZUSAMMENFASSUNG

E-Mails sind für Unternehmen unverzichtbar – und stellen aktuell das häufigste Mittel zur Malware-Verbreitung dar.[1] Heute werden über den E-Mail-Kanal sowohl höchst gefährliche Cyberattacken als auch Betrügereien aller Art verschickt.[2] E-Mail ist damit der Bedrohungsvektor Nummer 1. Mittels Social Engineering verleiten Cyberkriminelle Anwender in Unternehmen dazu, auf unsichere Links zu klicken, Anmeldedaten einzugeben oder gar unwissentlich bei der Umsetzung der Angriffe mitzuhelfen (z. B. indem sie Geld an die Betrüger überweisen oder vertrauliche Dateien senden).

Die Bedrohungen haben sich geändert, doch der Cybersicherheitssektor verharrt zum großen Teil weiterhin in veralteten Bedrohungsmodellen. Es wird versucht Verbesserungen an veralteten Strategien vorzunehmen, die jedoch unaufhörlich an Effektivität verlieren.

Es ist Zeit für einen neuen Ansatz. In der aktuellen Bedrohungslage konzentriert sich eine effektive Cybersicherheitsstrategie in erster Linie auf den Menschen.

Anwenderrisiken erfassen, erkennen und melden

Wenn es darum geht, Ihre Anwender zu schützen, besteht der erste Schritt in der Identifizierung der am stärksten gefährdeten Mitarbeiter. Auch wenn viele Unternehmen die einzelnen Risikofaktoren unterschiedlich gewichten, sollten sie stets eine Kombination aus Schwachstellen, Angriffen und Berechtigungen berücksichtigen.

Die Schwachstellen bestimmen, welche Personen einer Bedrohung am ehesten auf den Leim gehen. Mit einer Angriffsanalyse können Sie feststellen, welche Personen in Ihrem Unternehmen angegriffen werden – ebenso von wem und in welchem Umfang. Und indem sie die dem jeweiligen Anwender gewährten Berechtigungen in die Analyse miteinbeziehen, können Sie Prognosen dazu erstellen, wie groß der Schaden eines erfolgreichen Angriffs für Ihr Unternehmen werden könnte.

Wir nennen Anwender, die aufgrund dieser Faktoren ein überdurchschnittliches Risiko darstellen, VAPs bzw. Very Attacked People™. Diese VAPs sollten von Ihrem IT-Sicherheitsteam schnell identifiziert werden. Ausgestattet mit diesen Informationen können sie im Unternehmen entsprechend genutzt werden und die Verteidigungsstrategie gegen Cyberrisiken insgesamt stärken.

[1] Verizon: „2019 Data Breach Investigations Report“ (Untersuchungsbericht zu Datenkompromittierungen 2019), Juli 2019.
[2] Proofpoint: „Bericht: Der Faktor Mensch 2019“, September 2019.

Schwachstelle: Wie arbeiten die Menschen und worauf klicken sie?

Die Bewertung der Schwachstellen, die durch die Arbeitsweise von Mitarbeitern entstehen, beginnt mit dem Wissen um die verwendeten Tools, Plattformen und Anwendungen. Dazu gehören verwendete Cloudanwendungen und der Sicherheitsstatus der genutzten Geräte.

Auch gilt es herausfinden, wie anfällig Ihre Anwender für Phishing und andere Cyberangriffe sind.

Schulungen zur Steigerung des Sicherheitsbewusstseins (Security Awareness) können Erkenntnisse dazu liefern, welche Mitarbeiter am wahrscheinlichsten auf echte Cyberbedrohungen hereinfallen bzw. diese nicht als solche erkennen und melden würden. Im Allgemeinen sind Anwender, die bei Schulungen schlecht abschneiden (oder sie nicht bestehen), stärker gefährdet als Kollegen mit hohen Punktzahlen.

Wie gut Anwender solchen Betrugsversuchen jedoch tatsächlich widerstehen können, lässt sich nur über simulierte Angriffe, die echte Angriffstechniken verwenden, zuverlässig testen. Mit simulierten Angriffen, insbesondere wenn dabei real genutzte Techniken zum Einsatz kommen, lässt sich feststellen, welche Mitarbeiter für welche Taktiken anfällig sind.

Angriffe: Wie werden die Menschen angegriffen?

Auch wenn jeder einzelne Cyberangriff potenziell gefährlich ist, sind einige schädlicher, gezielter oder raffinierter als andere. Deshalb kann die Bewertung dieses Faktors schwieriger sein, als es zunächst scheint.

„Standard"-Bedrohungen, die in großer Masse versendet werden, mögen zahlreicher sein als andere Bedrohungstypen, sie sind den technischen Verteidigungssystemen jedoch bekannt und können leichter blockiert werden.

Andere Bedrohungen kommen vielleicht nur bei einigen wenigen Angriffen zum Einsatz, können jedoch eine größere Gefahr darstellen, da sie raffinierter oder extrem zielgerichtet hinsichtlich der adressierten Personen sind.

Diese Unterscheidung ist daher wichtig, um die stärker gefährdeten Anwender identifizieren zu können, also diejenigen Nutzer, die aus diesem Grund ein höheres Sicherheitsrisiko für das Unternehmen darstellen. Umfangreiche Bedrohungsdaten und zeitnahe Einblicke sind der Schlüssel zur Ermittlung der gezielt angegriffenen Mitarbeiter und zur Klärung der Frage, wie hoch das Risiko dieser Angriffe ist.

Berechtigung: Auf welche Systeme und Daten können die Nutzer zugreifen?

Für die Bewertung der Berechtigungen müssen Sie zunächst erfassen, auf welche potenziell wertvollen Daten die Nutzer Zugriff haben bzw. auf welche Systeme sie zugreifen können. Bedenken Sie auch Befugnisse finanzieller Natur (das Recht, Überweisungen vorzunehmen oder Bankdaten zu aktualisieren) oder das Vorhandensein wichtiger Beziehungen im Unternehmen usw.

Die Position des Anwenders im Organigramm ist natürlich ein wichtiger Faktor bei der Bewertung der Berechtigungen. Sie ist jedoch nicht der einzige Faktor – und häufig noch nicht einmal der wichtigste.

Wenn der Angreifer auf Wirtschaftsspionage aus ist, sind Assistenten möglicherweise ein interessanteres Ziel als andere Mitarbeiter, da sie Zugriff auf den Kalender der Chefetage haben. Im Krankenhaus ist die Situation ähnlich: Krankenschwestern mit Zugriff auf Patientenakten sind für Identitätsdiebe eventuell nützlicher als der Vorstandschef.

Risiken minimieren

Die Identifizierung Ihrer VAPs ist eine wichtige Grundlage für E-Mail-Sicherheit, aber dennoch nur der erste Schritt. Ein personenorientierter Ansatz gewährleistet den Schutz aller Mitarbeiter, da Kontrollen entsprechend des jeweiligen Risikos zur Anwendung kommen.

Basisebene: Sicherheit für alle

Da E-Mail-Angriffe verschiedenste Formen annehmen können, benötigen Sie einen Schutz, der alle Arten von E-Mail-Angriffen stoppt – nicht nur einige. Das sind die wichtigsten Schritte, um moderne E-Mail-Bedrohungen abwehren zu können:

- Stoppen von schädlichen Anhängen und URLs, bevor sie den Posteingang der Anwender erreichen
- Stoppen von Malware-losen Angriffen mit gefälschter Identität wie Business Email Compromise (BEC) und anderen Betrugsformen, einschließlich Angriffen, die mittels kompromittierter E-Mail-Konten innerhalb Ihres Unternehmens erfolgen
- Sicheres Surfen im Web und sicherer Abruf privater E-Mails auf unternehmenseigenen Geräten, indem adaptive Isolierungstechnologie zum Einsatz kommt
- Mehr Nutzersicherheit durch Security-Awareness-Schulungen
- Schutz der Daten vor Sicherheitsverletzungen und Insider-Bedrohungen

VAP-Ebene: Adaptive Kontrollen für Mitarbeiter, die mehr Schutz benötigen

Eine effektive E-Mail-Sicherheitsstrategie schützt alle. Personenorientierte Schutzmaßnahmen berücksichtigen, dass einige Anwender – Ihre VAPs – zusätzlichen Schutz und weitere Kontrollmaßnahmen benötigen.
Bei diesen VAPs besteht möglicherweise ein größeres Risiko, dass sie auf Angriffe hereinfallen, intensiver von Angreifern ins Visier genommen werden und über umfangreiche Zugriffsberechtigungen auf vertrauliche Daten und Systeme verfügen – oder es liegt gar eine Kombination dieser drei Faktoren vor, wodurch das allgemeine Risiko für diese Person deutlich erhöht ist.

Mit diesen grundlegenden Kontrollen werden Anwender als VAPs identifiziert:

- Gezielte Schulungen zur Steigerung des Sicherheitsbewusstseins
- Adaptiver, risikobasierter Schutz, z. B. zusätzliche Authentifizierung, Isolierungstechnologie bei Web-Nutzung und für URLs
- Schutz vor kompromittierten Cloud-Accounts

Effektive Reaktion, wenn Bedrohungen nicht automatisch abgewehrt werden

Wenn ein Angriff durchkommt, kann eine schnelle Eindämmung und Beseitigung darüber entscheiden, ob es sich um einen kurzen Zwischenfall oder eine langfristige Störung handelt.

In vielen Unternehmen ist die Reaktion auf Sicherheitsvorfälle ein sehr langsamer und arbeitsintensiver Prozess. Hier kann Automatisierung erhebliche Vorteile bieten.

Effektive Reaktionsprozesse automatisieren arbeitsintensive Aufgaben wie die Korrelation und Analyse von Sicherheitswarnungen, die Verifizierung von Kompromittierungsindikatoren (IOC, Indicators of Compromise) und die Erfassung forensischer Daten. Automatisierung kann auch die Behebung vereinfachen, z. B. die Aktualisierung der Firewall und der E-Mail-Blocklisten, das Entfernen schädlicher E-Mails aus Postfächern und die Einschränkung der Zugriffsberechtigungen für betroffene Anwender.

Strategisch eingesetzte Automatisierung beschleunigt die Reaktion auf Zwischenfälle und gibt den IT-Sicherheitsverantwortlichen die Möglichkeit, sich auf Dinge zu konzentrieren, die am besten von Menschen durchgeführt werden.

Das Ergebnis

E-Mails sind für moderne Unternehmen unverzichtbar – und das Mittel der Wahl für Cyberangreifer. E-Mail-Angriffe können verschiedenste Formen annehmen, von verschiedensten Absendern stammen und einzigartige Ziele haben. Sie haben jedoch immer eines gemeinsam: Menschen.

Bei E-Mail-Angriffen geht es im Kern immer darum, Menschen zu einer gefährlichen Handlung zu verleiten – zum Öffnen eines schädlichen Anhangs, zum Klicken auf eine unsichere URL, zum Versenden vertraulicher Informationen oder zum Überweisen von Geldern auf ein betrügerisches Konto. Deshalb ist für die Absicherung des E-Mail-Kanals ein personenorientierter Ansatz erforderlich.

Mit der richtigen Strategie und geeigneten Tools, Einblicken und Schulungen können Unternehmen die E-Mail-Risiken unter Kontrolle bringen und den wichtigsten Kanal für ihre Geschäftskommunikation schützen.

EINFÜHRUNG

E-Mail ist der bei weitem häufigste Bedrohungsvektor

Der Kampf um Unternehmensdaten wird an dem Ort ausgetragen, an dem sich Mitarbeiter tagtäglich befinden: im E-Mail-Posteingang.

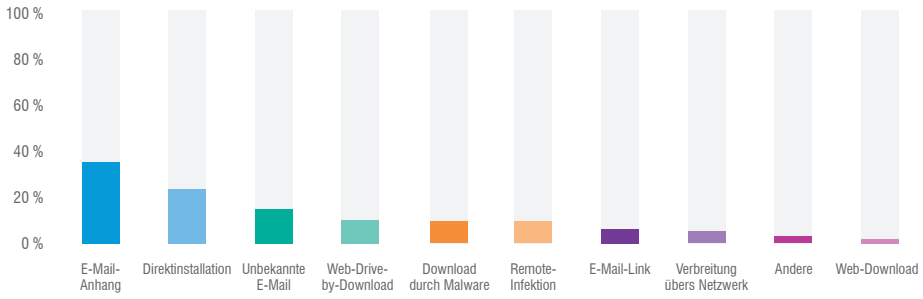
Malware wird primär über E-Mails verbreitet[3] und die E-Mail bietet Cyberangreifern die ideale Plattform für Betrügereien aller Art[4]. Das macht die E-Mail zum Bedrohungsvektor Nummer 1. Mittels Social Engineering verleiten Cyberkriminelle Anwender in Unternehmen dazu, auf unsichere Links zu klicken, Anmeldedaten einzugeben oder gar unwissentlich bei der Umsetzung der Angriffe mitzuhelfen (z. B. indem sie Geld an die Betrüger überweisen oder vertrauliche Dateien senden).

Der Grund für die Begeisterung der Angreifer für E-Mails liegt auf der Hand: Die jahrzehntealte Architektur ist nicht auf Sicherheit ausgelegt. Sie ist universell im Einsatz. Und im Gegensatz zu Computer-Hardware und -Infrastruktur lässt sich mit E-Mail-Angriffen eine Schwachstelle ausnutzen, für die es keine Patches gibt: der Mensch.

Unternehmen bezahlen jedes Jahr Milliarden für Sicherheitstools, mit denen sie ihre Netzwerkperipherie absichern, Netzwerkangriffe erkennen und Endgeräte schützen. Doch heutige Angriffe richten sich nicht gegen Technologie, sondern gegen menschliches Verhalten. Und für Cyberkriminelle ist die E-Mail die einfachste Möglichkeit, die zum Ziel gewordenen Menschen in den Unternehmen zu erreichen.

Es ist Zeit für einen neuen Ansatz. Die heutige Bedrohungslage macht eine neue Denkweise und eine neue Strategie erforderlich, die sich auf den Schutz der Menschen und weniger auf die Infrastruktur konzentriert.

Die häufigsten Malware-Vektoren



Quelle: Verizon: „2019 Data Breach Investigations Report"

Der vorliegende Leitfaden soll als Ausgangspunkt dienen. Sie erhalten Antworten auf folgende Fragen:

- Warum sollte die Sicherheit von E-Mails höchste Priorität erhalten?
- Warum ist die Absicherung von E-Mails so schwer?
- Warum ist ein personenorientierter Sicherheitsansatz effektiver – und kostengünstiger – als Peripherie-basierte Ansätze, die mit aktuellen personenorientierten Bedrohungen nicht mehr Schritt halten können?

DIE FAKTEN

94 %

aller externen Cyberbedrohungen beginnen mit einer E-Mail.[5]

27 %

aller externen Angriffe, die zu einer Sicherheitsverletzung im Unternehmen führen, wurden mit gestohlenen Anmeldedaten durchgeführt, die häufig durch eine einfache Phishing-E-Mail erlangt wurden.[6]

26 Mrd. US-Dollar

Der Verlust durch Business Email Compromise (BEC) und E-Mail-Kontenkompromittierung (EAC) beläuft sich weltweit inzwischen auf 26,2 Milliarden US-Dollar.[7]

90 %

der erkannten Malware-Angriffe gehen per E-Mail ein.[8]

47 Angriffe mit E-Mail-Betrug

Gezielt angegriffene Unternehmen waren allein im 1. Quartal 2019 im Durchschnitt mit 47 E-Mail-Betrugsangriffen konfrontiert.[9]

Mehr als 3x mehr

Pro BEC-Angriff (Business Email Compromise) wurden im Schnitt 24.439 US-Dollar gestohlen – dreimal mehr als bei einer durchschnittlichen Datenkompromittierung.[10]

3 Verizon: *„2019 Data Breach Investigations Report"*, Juli 2019.
4 Proofpoint: *„Bericht: Der Faktor Mensch 2019"*, September 2019.
5 Verizon: *„2019 Data Breach Investigations Report"*, Juli 2019.
6 Forrester Research: *„The Forrester Wave Enterprise Email Security, Q2 2019"* (E-Mail-Sicherheit für Unternehmen, 2. Quartal 2019), Mai 2019.
7 FBI: *„Business Email Compromise: the $26 Billion Scam"* (Business Email Compromise: Der 26-Milliarden-Dollar-Betrug), September 2019.
8 Verizon: *„2019 Data Breach Investigations Report"*, Juli 2019.
9 Proofpoint: *„Proofpoint Quarterly Threat Report Q1 2019"*, (Bedrohungsbericht zum 1. Quartal 2019), Mai 2019.
10 Verizon: *„2019 Data Breach Investigations Report"*, Juli 2019.

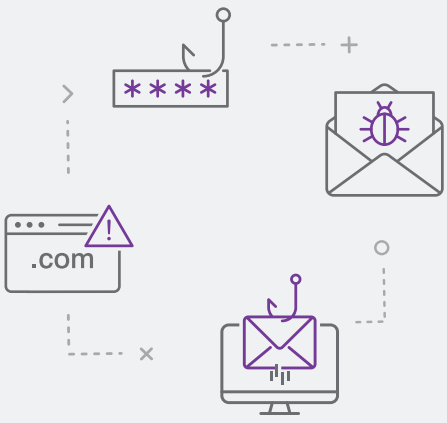
E-Mail-Angriffe verändern sich schneller als die Schutzmaßnahmen

Die Absicherung von E-Mails spielt eine zentrale Rolle für den Schutz der Unternehmen, ist jedoch eine komplexe Herausforderung.

Die Gründe: E-Mail-Bedrohungen sind zahlreich und vielfältig. Die Angriffstechniken entwickeln sich kontinuierlich weiter. Und die menschliche Natur – das schwächste Glied in jedem Unternehmen – steht dauerhaft im Visier der Angreifer.

Daher ist es nicht überraschend, dass Lösungen, die vor zwei oder drei Jahren für die Abwehr von Angriffen entwickelt wurden, heute nicht Schritt halten können.

Aus dem Werkzeugkasten der E-Mail-Angreifer



Mit diesen Methoden attackieren Cyberangreifer Menschen per E-Mail:

Malware: Schädlicher Code, der PCs und Server infiziert. Die Verbreitung erfolgt über einen Dateianhang, einen Link auf eine schädliche URL oder als sekundärer Download durch eine Malware, die bereits auf dem infizierten System installiert ist.

Phishing: Schädliche E-Mails, die Menschen zu einer bestimmten Aktion verleiten sollen, zum Beispiel zum Eingeben ihrer Anmeldedaten, zum Versenden vertraulicher Informationen oder sogar zum Überweisen von Geldern (siehe „E-Mail-Betrug“ unten).

E-Mail-Betrug: Eine Phishing-Form, die Menschen zum Überweisen von Geldern oder Versenden vertraulicher Informationen an den Angreifer verleiten soll. Bei E-Mail-Betrug ist meist keine Malware im Spiel. Stattdessen soll das Opfer per Social Engineering zu bestimmten Aktionen verleitet werden. Bei diesen Angriffen werden meist irreführende Anzeigenamen, Domänen-Spoofing oder Doppelgänger-Domänen eingesetzt, um Vertrauen bei den Empfängern zu erwecken.

Internes Phishing: Diese Phishing-Form verwendet ein kompromittiertes E-Mail-Konto für gezielte Angriffe auf Anwender, die die gleiche E-Mail-Domäne nutzen (meist Kollegen). Die Effektivität dieses Angriffstyps basiert darauf, dass die meisten Unternehmen nicht auf Bedrohungen achten, die aus ihrer eigenen Domäne stammen. Zudem gehen die Empfänger davon aus, dass sie E-Mails von Kollegen vertrauen können.

Webmail-Phishing: Diese Angriffe attackieren Anwender über ihre privaten Webmail-Konten. Viele Mitarbeiter greifen am Arbeitsplatz auf ihre privaten E-Mails zu und setzen ihren Arbeitgeber damit zusätzlichen Bedrohungen aus.

Gründe für einen personenorientierten Ansatz

Cyberangreifer verlagern ihre Anstrengungen von der Infrastruktur auf die Anwender. Dadurch sind die früheren Peripherie-orientierten Cybersicherheitsansätze, die schon vorher nicht immer zuverlässig waren, hoffnungslos veraltet.

Es gibt keine definierte Peripherie mehr, die noch geschützt werden kann. Die Mitarbeiter von heute arbeiten im Home Office oder greifen mobil und von beliebigen Orten über alle möglichen Arten von Geräten, Netzwerken und Plattformen außerhalb des traditionellen Unternehmensnetzwerks auf Unternehmensdaten zu.

Der allgemeine Wechsel in die Cloud hat diesen Trend weiter verschärft. Auch wenn Ihre Cloudinfrastruktur abgesichert ist, sind die Personen, die sie nutzen, weiterhin einfach nur Menschen.

Deshalb müssen sich effektive Cybersicherheitsansätze heute in erster Linie auf den Menschen konzentrieren.

Das VAP-Modell (Vulnerability, Attack, Privilege)

Ebenso wie jeder Mensch einzigartig ist, sind auch sein Wert für die Cyberangreifer und 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).

Schwachstellen

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

Angriffe

Aktuelle Cyberangriffe sind hartnäckig, vielgestaltig und enorm wandlungsfähig. Sie müssen nicht nur verstehen, wer in Ihrem Unternehmen angegriffen wird, sondern auch wissen, wie und von wem der Angriff erfolgt und ob die Attacke Teil einer größeren Kampagne ist. Ein Anwender, der von wenigen, aber besonders raffinierten Bedrohungen ins Visier genommen wird, stellt zum Beispiel ein größeres Risiko dar als jemand, der mit einem relativ wahllos verschickten Massenmailing angegriffen wird.

Berechtigungen

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

Anwenderrisiken erfassen, erkennen und melden

Wenn es darum geht, Ihre Anwender zu schützen, besteht der erste Schritt in der Identifizierung der am stärksten gefährdeten Mitarbeiter. Auch wenn viele Unternehmen die einzelnen Risikofaktoren unterschiedlich gewichten, sollten sie stets eine Kombination aus Schwachstellen, Angriffen und Berechtigungen berücksichtigen.

Die Schwachstellen bestimmen, welche Personen einer Bedrohung am ehesten auf den Leim gehen. Mit einer Angriffsanalyse können Sie feststellen, welche Personen in Ihrem Unternehmen angegriffen werden – ebenso von wem und in welchem Umfang. Und indem sie die dem jeweiligen Anwender gewährten Berechtigungen in die Analyse miteinbeziehen, können Sie Prognosen dazu erstellen, wie groß der Schaden eines erfolgreichen Angriffs für Ihr Unternehmen werden könnte.

Wir nennen Anwender, die aufgrund dieser Faktoren ein überdurchschnittliches Risiko darstellen, VAPs. Diese VAPs sollten von Ihrem IT-Sicherheitsteam schnell identifiziert werden. Ausgestattet mit diesen Informationen können sie im Unternehmen entsprechend genutzt werden und die Verteidigungsstrategie gegen Cyberrisiken insgesamt stärken.

Es ist also erforderlich alle drei Bereiche genau zu analysieren, um personenorientierte Sicherheit gewährleisten zu können. Ohne diese Einblicke wissen Unternehmen nicht, wer zusätzlichen Schutz benötigt und wie die VAPs optimal geschützt werden können.

Schwachstelle: Wie arbeiten die Menschen und worauf klicken sie?

Die Quantifizierung der Anfälligkeit ist mit herkömmlichen Technologie-orientierten Sicherheitstools nicht einfach. Mit einem personenorientierten Ansatz können Sie jedoch die Arbeitsweise und das Klickverhalten Ihrer Mitarbeiter ermitteln.

Bei der Analyse der Arbeitsweise geht es um die Tools, Systeme und Plattformen, mit denen sie arbeiten. Das Klickverhalten gibt den Grad der Sensibilisierung für Sicherheit und die Wahrscheinlichkeit an, dass diejenige Person auf Bedrohungstaktiken hereinfallen würde.

Die Arbeitsweise Ihrer Mitarbeiter

Die Bewertung der Schwachstellen, die durch die Arbeitsweise von Mitarbeitern entstehen, beginnt mit dem Wissen um die verwendeten Tools, Plattformen und Anwendungen. Dazu gehören:

- Verwendete Cloudanwendungen
- Anzahl und Art der Geräte, die für den E-Mail-Zugriff genutzt werden
- Sicherheitsstufe dieser Geräte
- Einhaltung der Empfehlungen und Unternehmensrichtlinien durch die Anwender
- Nutzung von Mehrfaktor-Authentifizierung (MFA)

Je detaillierter Ihre Übersicht, desto besser.

Klickverhalten Ihrer Mitarbeiter

Im zweiten Teil der Ermittlung von Schwachstellen müssen Sie herausfinden, wie anfällig Ihre Anwender für Phishing und andere Cyberangriffe sind.

Security-Awareness-Schulungen sind eine grundlegende Komponente jeder effektiven Sicherheitsstrategie und können Erkenntnisse dazu liefern, welche Mitarbeiter am wenigsten darauf vorbereitet sind, Cyberbedrohungen zu erkennen und zu melden. Im Allgemeinen sind Anwender, die bei Schulungen schlecht abschneiden (oder sie nicht bestehen), stärker gefährdet als Kollegen mit hohen Punktzahlen.

Wie gut Anwender solchen Betrugsversuchen jedoch tatsächlich widerstehen können, lässt sich nur über simulierte Angriffe, die echte Angriffstechniken verwenden, zuverlässig testen.

Da Sie aus guten Gründen sicher nicht bereit sind, anhand echter Bedrohungen zu testen, wer eine Malware-Datei öffnet und Geld an den Angreifer überweist, sind Phishing-Simulationen die beste Möglichkeit, diesen Schwachstellenaspekt 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 solche E-Mails ignorieren, sind weniger gefährdet, während diejenigen, die diese E-Mail an das Sicherheitsteam oder den E-Mail-Administrator melden, das geringste Risiko darstellen.

Angriffe: Wie werden die Menschen angegriffen?

Auch wenn jeder einzelne Cyberangriff potenziell gefährlich ist, sind einige schädlicher, gezielter oder raffinierter als andere. Deshalb kann die Bewertung dieses Faktors schwieriger sein, als es zunächst scheint.

„Standard"-Bedrohungen, die in großer Masse versendet werden, mögen zahlreicher sein als andere Bedrohungstypen, sie sind den technischen Verteidigungssystemen jedoch bekannt und können leichter blockiert werden.

Andere Bedrohungen kommen vielleicht nur bei einigen wenigen Angriffen zum Einsatz, können jedoch eine größere Gefahr darstellen, da sie raffinierter oder extrem zielgerichtet hinsichtlich der adressierten Personen sind.

Diese Unterscheidung ist daher wichtig, um die stärker gefährdeten Anwender identifizieren zu können, also diejenigen Nutzer, die aus diesem Grund ein höheres Sicherheitsrisiko für das Unternehmen darstellen. Umfangreiche Bedrohungsdaten und zeitnahe Einblicke sind der Schlüssel zur Ermittlung der gezielt angegriffenen Mitarbeiter und zur Klärung der Frage, wie hoch das Risiko dieser Angriffe ist.

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 nicht besonders gefährdet zu sein, 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.

Berechtigung: Auf welche Systeme und Daten können die Nutzer zugreifen?

Für die Bewertung der Berechtigungen müssen Sie zunächst erfassen, auf welche potenziell wertvollen Daten die Nutzer Zugriff haben bzw. auf welche Systeme sie zugreifen können. Bedenken Sie auch Befugnisse finanzieller Natur (das Recht, Überweisungen vorzunehmen oder Bankdaten zu aktualisieren) oder das Vorhandensein wichtiger Beziehungen im Unternehmen usw.

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 wichtiger Faktor bei der Bewertung der Berechtigungen. Sie ist jedoch nicht der einzige Faktor – und häufig noch nicht einmal der wichtigste.

Wenn der Angreifer auf Wirtschaftsspionage aus ist, sind Assistenten möglicherweise ein interessanteres Ziel als andere Mitarbeiter, da sie Zugriff auf den Kalender der Chefetage haben. Im Krankenhaus ist die Situation ähnlich: Krankenschwestern mit Zugriff auf Patientenakten sind für Identitätsdiebe eventuell nützlicher als der Vorstandschef.

Für die Angreifer kann jeder ein lohnenswertes Ziel darstellen, der ihnen nützlich ist.

AKTUELLE BEC- UND EAC-ANGRIFFE

Das sind einige bekannte Opfer aktueller BEC- und EAC-Angriffe.

„Shark Tank"-Moderatorin Barbara Corcoran:

400.000 US-Dollar

Regierung von Puerto Rico:

4 Mio. US-Dollar

Nikkei America:

29 Mio. US-Dollar

Red Kite Community Housing:

1,2 Mio. US-Dollar

Unabhängiger Schulkreis Manor (Texas, USA):

2,3 Mio. US-Dollar

Toyota Boshoku:

37 Mio. US-Dollar

Cabarrus County (Kalifornien, USA):

2,5 Mio. US-Dollar

Ocala (Florida, USA):

750.000 US-Dollar

Rijksmuseum Twenthe (Museum, Niederlande):

3,1 Mio. US-Dollar

Ich weiß, wer meine VAPs sind – und jetzt? Personenorientierte Sicherheit in Aktion

Die Identifizierung Ihrer VAPs ist eine wichtige Grundlage für E-Mail-Sicherheit, aber dennoch nur der erste Schritt. Ein personenorientierter Ansatz gewährleistet den Schutz aller Mitarbeiter, da Kontrollen entsprechend des jeweiligen Risikos zur Anwendung kommen.

Basisebene: Sicherheit für alle

E-Mail-Sicherheit beginnt mit zuverlässigem Schutz für alle Anwender. Da E-Mail-Angriffe verschiedenste Formen annehmen können, benötigen Sie einen Schutz, der alle Arten von E-Mail-Angriffen stoppt – nicht nur einige. Das sind die wichtigsten Schritte, um moderne E-Mail-Bedrohungen abwehren zu können:

Stoppen von schädlichen Anhängen und URLs, bevor sie den Posteingang der Anwender erreichen

Die meisten Cyberangreifer setzen darauf, dass das Opfer eine Aktion durchführt – in vielen Fällen heißt das, einen Anhang zu öffnen oder auf eine URL zu klicken. Doch diese von Menschen ausgelösten Angriffe haben nur dann eine Chance auf Erfolg, wenn der Empfänger die Nachricht auch erhält und sieht.

Hier kommt ein sicheres E-Mail-Gateway ins Spiel. Wenn Malware-Bedrohungen gestoppt werden, bevor sie den Posteingang der Anwender erreichen, kann Ihr Gateway Unternehmen vor vielfältigen Malware-Bedrohungen schützen, einschließlich Ransomware, Bank-Trojaner, Remote-Zugriffs-Trojaner, Informationsdiebe (Stealer), Downloader, Botnets usw.

Stoppen von Malware-losen Angriffen mit gefälschter Identität

Das Stoppen von Malware-Bedrohungen ist unverzichtbar, doch einige der schwerwiegendsten E-Mail-Angriffe kommen ganz ohne Malware aus. Stattdessen setzen sie auf Social-Engineering-Taktiken.

Business Email Compromise (BEC), eine Form des Überweisungsbetrugs, ist hierfür ein Beispiel. BEC hat laut FBI seit 2016 Verluste in Höhe von mehr als 26 Milliarden US-Dollar verursacht. Die US-Behörde gibt an, dass es Meldungen von BEC-Angriffen aus 177 Ländern gibt und die betrügerischen Überweisungen in mindestens 140 Länder gingen.[11]

Bei BEC und anderen Malware-losen Angriffen imitieren die Betrüger die Identität einer Person, der der Empfänger vertrauen kann. Dazu verwenden sie gefälschte, kompromittierte oder Doppelgänger-E-Mail-Konten. Unter dieser falschen Identität fordern die Angreifer das Opfer zu einer Aktivität auf, z. B. soll es Geld an ein ausländisches Bankkonto überweisen oder vertrauliche Dateien senden.

Bedrohungen mit gefälschter Identität sind ein komplexes Problem mit vielen Facetten. Um sie stoppen zu können, benötigen Sie einen mehrschichtigen Schutz, der eingehende, ausgehende und interne E-Mails abdeckt – und dabei ganzheitlich und einheitlich vorgeht.

Zusätzlich zu Anwenderschulungen und anderen in diesem Abschnitt beschriebenen Sicherheitskontrollen sollten die folgenden wichtigen Elemente implementiert werden, um das Unternehmen effektiv vor E-Mails zu schützen, die Ihre Nutzer mit gefälschter Identität hinters Licht führen möchten.

[11] FBI: *„Business Email Compromise: the $26 Billion Scam"* (Business Email Compromise: Der 26-Milliarden-Dollar-Betrug), September 2019.

DMARC

Implementieren Sie E-Mail-Authentifizierung per DMARC. Diese im gesamten Internet gültige Richtlinie validiert die Identität des E-Mail-Absenders und überprüft, ob der Absender autorisiert ist, Nachrichten im Namen des Unternehmens zu senden.

Mit DMARC erhalten Sie Transparenz über alle E-Mails, die unter Verwendung Ihrer E-Mail-Domäne versendet werden, einschließlich vertrauenswürdiger externer Versender wie Marketo, Salesforce oder SurveyMonkey. Dank dieser Transparenz können Sie alle gültigen Absender autorisieren, die E-Mails in Ihrem Namen versenden dürfen – und all jene blockieren, die mithilfe Ihrer vertrauenswürdigen Domänen Geld stehlen oder Ihrer Marke schaden wollen.

Dynamische Klassifizierung

Da Sie mit DMARC Bedrohungen stoppen können, die Ihre Domäne missbrauchen, versuchen Angreifer auch mit anderen Taktiken, Ihre Anwender zu täuschen. Deshalb ist die dynamische Analyse und Klassifizierung des E-Mail-Inhalts eine weitere wichtige Komponente zum Schutz vor Malware-losen Bedrohungen.
Bei diesem Aspekt der E-Mail-Sicherheit geht es um die genaue Untersuchung des E-Mail-Inhalts, nicht nur der Absenderdaten. Daher benötigen Sie eine E-Mail-Sicherheitslösung, die nach Hinweisen für Betrug sucht und alle verdächtigen bzw. unsicher erscheinenden Nachrichten blockiert oder genauer analysiert. Dynamische Klassifizierung analysiert E-Mails basierend auf mehreren Faktoren, zum Beispiel:

- Inhalt, Header und IP-Adresse der E-Mail
- Die Reputation des Absenders
- Beziehung zwischen Absender und Empfänger

Schutz für interne E-Mails

In einigen Fällen versuchen die Angreifer erst gar nicht, ihre E-Mail-Adresse zu verschleiern. Stattdessen übernehmen sie einfach ein legitimes Konto. E-Mail-Kontenkompromittierung (Email Account Compromise, EAC) kommt bei verschiedensten Angriffen zum Einsatz, ist aber aus folgenden Gründen besonders bei Betrug mit gefälschter Identität erfolgreich:

- Die meisten Unternehmen untersuchen interne E-Mails nicht so gründlich und mit den gleichen Sicherheitskontrollen wie externe E-Mails.
- Die meisten Anwender vertrauen E-Mails von Personen, die sie kennen, wie beispielsweise Kollegen.
- Angreifer, die ein Konto übernehmen, verfügen über einen ganzen Schatz an Informationen über den kompromittierten Anwender – einschließlich Kontakte, Gesprächsthemen und sogar Schreibstil. Dadurch können sie die kompromittierte Person besonders überzeugend nachahmen.

Mehr Nutzersicherheit durch Security-Awareness-Schulungen

Cyberangreifer sind inzwischen extrem erfolgreich, wenn es darum geht, die menschliche Natur mit überzeugenden Spoofing-Techniken, interessanten Betreffzeilen und unwiderstehlichen Handlungsaufforderungen auszunutzen. Wie wir in unserem Bericht **Der Faktor Mensch 2019** gezeigt haben, erzielten die erfolgreichsten Phishing-E-Mails eine Klickrate von 1,6. Das bedeutet, dass diese Nachrichten sogar an zusätzliche Empfänger weitergeleitet und auch von ihnen angeklickt wurden.[12]

Schutz der Daten vor Sicherheitsverletzungen und Insider-Bedrohungen

Keine E-Mail-Schutztechnologie kann jede Bedrohung stoppen und selbst die am besten geschulten Mitarbeiter können auf besonders gezielte Social-Engineering-Angriffe hereinfallen.

Deshalb sollte jede E-Mail-Sicherheitsstrategie den Einsatz von Tools für Data Loss Prevention (DLP), einschließlich Verschlüsselung, umfassen. Selbst wenn etwas schief geht, können eine schnelle Reaktion und DLP dafür sorgen, dass sich der Angriff nicht weiter ausbreitet und Angreifer nicht an Ihre wertvollsten Daten gelangen.

DLP schützt auch vor Bedrohungen durch Insider. Niemand möchte sich die eigenen Kollegen als potenzielles Sicherheitsrisiko vorstellen. Doch Insider-Bedrohungen – dazu gehören unachtsame, kriminelle und kompromittierte Mitarbeiter – verursachten im Jahr 2018 einen durchschnittlichen Schaden von 8,76 Millionen US-Dollar.[13]

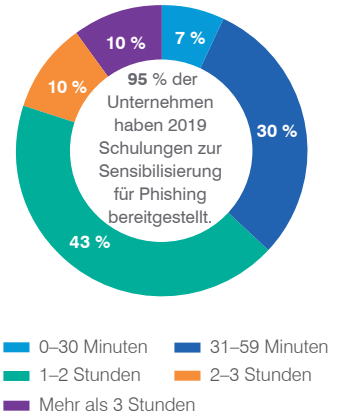
Ganz gleich, ob die Daten über eine interne Sicherheitsverletzung oder durch den Angriff eines Insiders Ihre Umgebung verlassen – mit DLP bleiben sie geschützt.

[12] Proofpoint: *„Bericht: Der Faktor Mensch 2019“*, September 2019.
[13] Ponemon Institute: *„2018 Cost of Insider Threats: Global“* (Kosten von Insider-Bedrohungen 2018: Weltweit), April 2018.

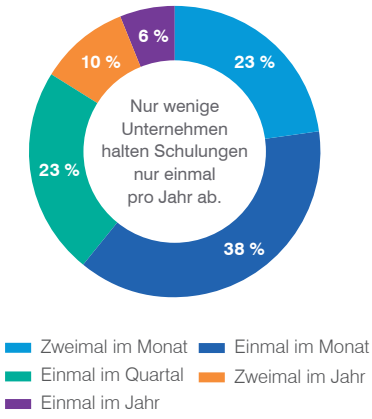
VORGEWARNT UND GEWAPPNET

So implementieren Unternehmen ihre Schulungsprogramme zur Steigerung des Sicherheitsbewusstseins.

Pro Jahr für Schulungen zur Sensibilisierung für Sicherheit vorgesehene Zeit



Häufigkeit von Schulungen zur Sensibilisierung für Sicherheit



Adaptive Ebene: Kontrollen für VAPs

Eine effektive E-Mail-Sicherheitsstrategie schützt alle. Personenorientierte Schutzmaßnahmen berücksichtigen, dass einige Anwender – Ihre VAPs – zusätzlichen Schutz und weitere Kontrollmaßnahmen benötigen. Bei diesen VAPs besteht möglicherweise ein größeres Risiko, dass sie auf Angriffe hereinfallen, intensiver von Angreifern ins Visier genommen werden und über umfangreiche Zugriffsberechtigungen auf vertrauliche Daten und Systeme verfügen – oder es liegt eine Kombination dieser drei Faktoren vor.

Gezielte Schulungen zur Steigerung des Sicherheitsbewusstseins

Unternehmensweite Sicherheitsschulungen sind gut geeignet, um diese Schwachstellen aufzudecken und die menschliche Angriffsfläche zu reduzieren. Mit gezielten Schulungen können nicht nur offensichtliche Wissenslücken geschlossen werden. Sie sind auch eine wertvolle Präventivmaßnahme für alle VAPs – nicht nur für die Personen, die als besonders anfällig gelten.

Anwender, die aufgrund ihres Angriffsprofils als VAPs eingestuft werden, können zum Beispiel gezielte Schulungen zu den Bedrohungen erhalten, die sie ins Visier nehmen. Und Anwender mit umfangreichen Berechtigungen können Zusatzschulungen zu Angriffskampagnen erhalten, die auf die von ihnen abrufbaren Daten abzielen.

Adaptiver, risikobasierter Schutz

Die Implementierung extrem strikter Sicherheitskontrollen für alle Anwender zu jedem Zeitpunkt ist im Allgemeinen nicht nur unpraktisch, sondern unter Umständen auch kontraproduktiv. Übermäßig strikte Kontrollen können die Produktivität der Anwender einschränken und dazu führen, dass sie zur Erledigung ihrer Aufgaben nach Möglichkeiten suchen, die Sicherheitsmaßnahmen zu umgehen.

In einigen Fällen sind zusätzliche Schutzmaßnahmen jedoch zwingend notwendig. Ein Mitarbeiter mit Kundenkontakt könnte besonders für einen Angriffstyp anfällig sein, der gerade in Ihrer Branche umgeht. Ein Forscher könnte in das Visier besonders raffinierter Angreifer geraten oder ein CEO hat aufgrund dieser Position Zugriff auf die sensibelsten Unternehmensdaten.

In einigen Fällen werden Sie die Authentifizierungsanforderungen verschärfen, während Sie in anderen Fällen eine Funktion zur Web-Isolierung aller URLs einsetzen sollten, auf die Anwender in E-Mails klicken.

Für adaptive Schutzmaßnahmen benötigen Sie ein aktuelles Bild der VAP-bezogenen Risikofaktoren, damit die Maßnahmen passend zu diesen Risiken angewendet werden können.

Schutz für Cloud-basierte Konten

Die Kompromittierung von E-Mail-Konten (EAC) – insbesondere von Cloud-Accounts – wird bei Kriminellen immer beliebter, weil diese kompromittierten Konten praktisch die „Lizenz zum Stehlen“ darstellen.

Ein solches Konto lässt sich auf verschiedenste Weise missbrauchen. Wenn Eindringlinge die Kontrolle über ein Konto übernehmen, können sie sich lateral in Ihrer Umgebung bewegen, Daten stehlen oder Ihre Geschäftspartner und Kunden betrügen. Deshalb ist der Schutz Ihrer E-Mail-Konten, und ganz besonders der Cloud-Konten, so wichtig.

Kompromittierungs-situation: So übernehmen Angreifer Cloud-basierte Konten

Bei einem EAC-Angriff *scheint* das E-Mail-Konto nicht nur legitim zu sein – es ist tatsächlich echt. Mit diesen Methoden übernehmen Angreifer die Kontrolle über die Konten Ihrer Anwender.

Brute-Force-Angriff: Der Angreifer probiert, meist mit einem automatisierten Skript, eine Kombination aus Benutzername/Kennwort für unzählige Konten aus, bis eine funktioniert.

Breach-Replay-Angriff: Leider verwenden viele Menschen die gleichen Kennwörter für mehrere Konten. Wenn eines dieser Kennwörter bei einer Datenschutzverletzung geleakt wird, sind die anderen Konten, die die gleiche Kombination aus Benutzername (häufig eine E-Mail-Adresse) und Kennwort verwenden, ebenfalls gefährdet.

Phishing: Herkömmliches Anmeldedaten-Phishing ist weiterhin eine effektive Methode, um an Kennwörter von Anwendern zu gelangen. Wenn keine zusätzlichen Kontrollen wie Mehrfaktor-Authentifizierung (MFA) eingerichtet sind, können verlorene Anmeldedaten die Kompromittierung von Konten ermöglichen.

Effektive Reaktion, wenn Bedrohungen nicht automatisch abgewehrt werden

Sicherheitszwischenfälle lassen sich nicht völlig vermeiden, aber sie müssen nicht zwingend zu einer Katastrophe führen.

Wenn ein Angriff durchkommt, kann eine schnelle Eindämmung und Beseitigung darüber entscheiden, ob es sich um einen kurzen Zwischenfall oder eine langfristige Störung handelt. Deshalb ist ein leistungsstarkes Reaktions-Framework für jede personenorientierte Sicherheitsstrategie wichtig.

In vielen Unternehmen ist die Reaktion auf Sicherheitsvorfälle ein sehr langsamer und arbeitsintensiver Prozess, der folgende Schritte umfasst:

- Untersuchung und Verifizierung des Zwischenfalls
- Eindämmung der Bedrohung
- Bestimmung von Ursache und Ausmaß
- Korrektur oder Wiederherstellung infizierter Systeme

Alle dieser Schritte sind für eine effektive Reaktion unerlässlich. Sicherheitsverantwortliche wissen jedoch aus eigener Erfahrung, dass sich diese Schritte nicht skalieren lassen, solange sie manuell ausgeführt werden. Hier kann Automatisierung erhebliche Vorteile bieten.

Effektive Reaktionsprozesse automatisieren arbeitsintensive Aufgaben wie die Korrelation und Analyse von Sicherheitswarnungen, die Verifizierung von Kompromittierungsindikatoren und die Erfassung forensischer Daten. Automatisierung kann auch die Behebung vereinfachen, z. B. die Aktualisierung der Firewall und der E-Mail-Blocklisten, das Entfernen schädlicher E-Mails aus Postfächern und die Einschränkung der Zugriffsberechtigungen für betroffene Anwender.

Strategisch eingesetzte Automatisierung beschleunigt die Reaktion auf Zwischenfälle und gibt dem Sicherheitsteam die Möglichkeit, sich auf Dinge zu konzentrieren, die am besten von Menschen durchgeführt werden – die Bedrohung vollumfänglich verstehen, priorisieren und die entsprechende Reaktion darauf in die Wege leiten.

Checkliste: Worauf sollten Sie bei einer Sicherheitslösung Wert legen?

Die Cybersicherheitsbranche versteht langsam, dass heutige Angriffe sich nicht gegen Technologien, sondern gegen Menschen richten. Doch personenorientierte Sicherheit ist mehr als nur ein Marketing-Schlagwort – es ist eine grundlegend neue Sichtweise auf Bedrohungen und deren Abwehr.

Die nachfolgende Checkliste zeigt, worauf Sie bei einer Sicherheitslösung Wert legen sollten.

Effektive E-Mail-Sicherheit für alle Anwender

Die beste Abwehr für E-Mail-Angriffe stoppt schädliche Nachrichten, bevor sie die Postfächer erreichen. Suchen Sie nach einer Lösung, die verschiedenste Angriffsformen und Taktiken erkennen kann, zum Beispiel:

- Malware-basierte Angriffe, die Anhänge und URLs verwenden
- Malware-lose Angriffe wie BEC
- E-Mail-Kontenkompromittierung und Übernahmen von Cloud-Konten

Bei heutigen E-Mail-Angriffen spielen Menschen die größte Rolle. Deshalb sollten Schulungen zur Steigerung des Sicherheitsbewusstseins zu den Hauptkomponenten Ihrer E-Mail-Sicherheitsstrategie gehören. Stellen Sie sicher, dass Ihr Schulungsprogramm folgende Bereiche abdeckt:

- Schulungen, die auf bewährten Methodiken und realen Angriffen basieren
- Phishing-Simulationen, die auf realen Kampagnen basieren, um Anwender zu Bedrohungen zu schulen, mit denen sie mit hoher Wahrscheinlichkeit konfrontiert werden
- Gezielte Folgeschulungen für Anwender, bei denen deutliche Schwachstellen sichtbar werden

Um Daten zu schützen, die gestohlen oder versehentlich bzw. mit böswilliger Absicht von einem Insider offengelegt wurden, sind Verschlüsselung und andere DLP-Maßnahmen wertvoll. Effektives DLP umfasst folgende Funktionen:

- Detaillierte Analyse von E-Mail-Inhalten und (bei Bedarf) Blockierung von Teilen ausgehender E-Mails und ähnlichen Inhalten vor dem Versand
- Identifizierung und Schutz aller Standardformate von regulierten Inhalten, z. B. PCI, HIPAA, FINRA
- Automatische Umleitung, Verschlüsselung und Ablehnung von E-Mails, die Sicherheits- und andere Richtlinien verletzen, und Warnung der zuständigen Personen im Unternehmen

Adaptive Kontrollen für VAPs

Aufgrund ihrer Schwachstellen, Angriffsprofile und Berechtigungen stark gefährdete Anwender müssen durch zusätzliche Sicherheitskontrollen geschützt werden. Eine personenorientierte E-Mail-Sicherheitslösung unterstützt Sie bei der Identifizierung dieser VAPs und bei ihrem Schutz mit zusätzlichen Sicherheitsebenen. Suchen Sie nach einer Lösung, die folgende Funktionen umfasst:

- Verwertbare Einblicke in Ihre VAPs basierend auf umfangreichen, aktuellen Bedrohungsdaten sowie detaillierte Erkenntnisse zum Risikoprofil Ihrer Anwender
- Berichtsfunktionen, mit denen Sie einfach die Schwachstellen, Angriffsprofile und Berechtigungen Ihrer Anwender identifizieren und kommunizieren können – einschließlich Abteilungs- und Branchenvergleichen
- Automatische Reaktion auf Änderungen in Anwenderprofilen mit erweiterter Authentifizierung, Einschränkung der Berechtigung, Web-Isolation usw.

Schnelle, effektive Reaktion, wenn Bedrohungen nicht automatisch abgewehrt werden

Durch die Automatisierung wichtiger Teile der Reaktion auf Zwischenfälle können Sie arbeitsintensive Aufgaben optimieren, sodass die Reaktionsteams mehr Zeit für wichtigere Aktivitäten haben. Wählen Sie ein Tool für automatisierte Reaktion, das folgende Funktionen bietet:

- Verifizieren von Bedrohungen, Identifizieren betroffener Anwender und Erfassen von Forensikdaten sowie Kontext zu diesen Anwendern
- Anreichern der Bedrohungsdaten mit umsetzbaren Informationen
- Eindämmen und Beseitigen von Bedrohungen und erneutes Authentifizieren von Konten in der Umgebung, in der Cloud und am Standort

Weitere Informationen

Weitere Informationen zum personenorientierten E-Mail-Sicherheitsansatz finden Sie unter **www.proofpoint.com/de/products/email-protection/email-security-and-protection**.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **proofpoint.com/de**.

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 sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, setzen auf die personenorientierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.de**.

proofpoint.

0301-001-01-01 03/20