proofpoint.

E-BOOK

2022

Strategischer Leitfaden E-Mail-Cybersicherheit

Ein personenzentrierter Ansatz zum Stoppen von Ransomware, Malware, Phishing und E-Mail-Betrug

proofpoint.com/de

E-Mails sind der wichtigste Bedrohungsvektor

Jeden Tag wird an einem Ort, an dem sich Mitarbeiter tagtäglich befinden, ein verborgener Kampf ausgetragen: im E-Mail-Posteingang.

Malware wird primär über E-Mails verbreitet und die E-Mail bietet Cyberangreifern die ideale Plattform für Betrügereien aller Art. 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.

Der Wechsel zur Cloud und die Arbeit im Homeoffice verschärfen dieses Problem noch zusätzlich.

Unternehmen bezahlen jedes Jahr Milliarden für Sicherheitstools, mit denen sie ihren Netzwerk-Perimeter absichern, Netzwerkangriffe erkennen und Endgeräte schützen. Und dennoch waren die Zahl der Kompromittierungen durch Ransomware, Business Email Compromise (BEC), Anmeldedaten-Phishing und Malware sowie die dadurch entstandenen Kosten noch nie so hoch.[1]

Der Grund: 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.

Wichtige Untersuchungsergebnisse:

14,8 Mio. USD
betragen die durchschnittlichen jährlichen Kosten durch Phishing-Betrug für ein großes Unternehmen – mehr als das Dreifache des Durchschnitts aus dem Jahr 2015[2]

86 %
der Unternehmen haben 2021 massenhafte Phishing-Angriffe erlebt[3]

77 %
aller Unternehmen haben 2021 BEC-Angriffe erlebt[4]

78 %
der Unternehmen haben im Jahr 2021 E-Mail-basierte Ransomware-Angriffe erlebt[5]

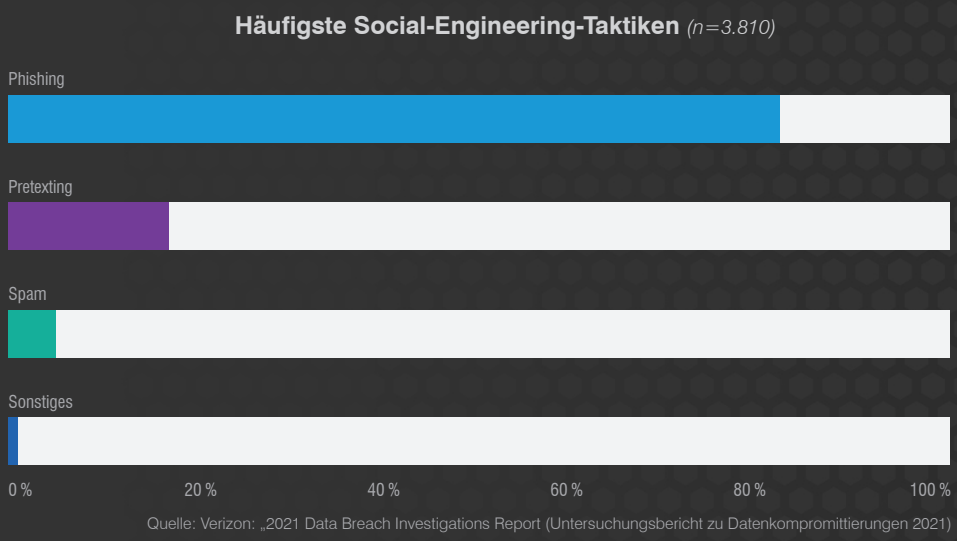
85 %
der Kompromittierungen gehen mit einer menschlichen Komponente einher[6]

1 Ponemon Institute: „Studie zu Kosten durch Phishing 2021“, Juni 2021.
2 Ponemon Institute: „Studie zu Kosten durch Phishing 2021“, Juni 2021.
3 Proofpoint: „State of the Phish 2022“, Februar 2022.
4 ebd.
5 ebd.
6 Verizon: „Data Breach Investigations Report Executive Summary“ (Untersuchungsbericht zu Datenkompromittierungen: Kurzfassung), Mai 2021.

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.

Unabhängig davon, ob Sie ein internationales Sicherheitskontrollzentrum oder ein kleines, gut eingespieltes Sicherheitsteam führen: Dieser Leitfaden soll Ihnen als Startpunkt dienen. Folgende Punkte werden untersucht:

- Warum sollte die Sicherheit von E-Mails höchste Priorität erhalten?
- Warum ist die Absicherung von E-Mails so schwer?
- Warum sind integrierte, mehrstufige personenzentrierte Schutzmaßnahmen effektiver?
- Wo können Ihre E-Mail-Sicherheitsabläufe optimiert werden, um Geld zu sparen und die Reaktion zu verbessern?



Quelle: Verizon: „2021 Data Breach Investigations Report (Untersuchungsbericht zu Datenkompromittierungen 2021)

Abb. 1: Die häufigsten Formen des Social Engineering

ABSCHNITT 1

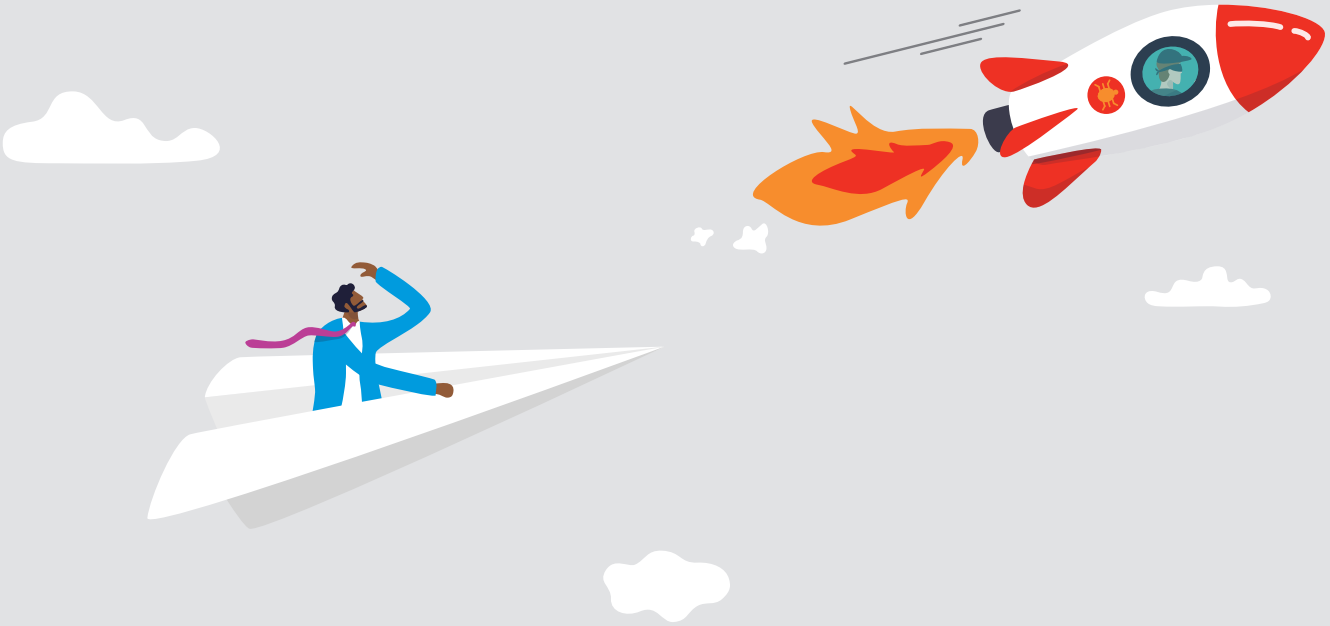
Cyberangriffe verändern sich schneller als herkömmliche Schutzmaßnahmen

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.

In diesem Abschnitt werden einige der Methoden aufgezeigt, mit denen Cyberangreifer Menschen ins Visier nehmen. (In vielen Fällen kombinieren die Angreifer mehrere Techniken, um Schutzmaßnahmen zu umgehen und höhere Erfolgsraten zu erzielen.)



Ransomware

Ransomware ist eine seit langem bekannte Bedrohung, die bis heute Probleme bereitet. Der Begriff Ransomware bezieht sich darauf, dass nach der Sperrung der Dateien des Opfers ein Lösegeld (engl. „ransom“) verlangt wird. Diese Malware-Form ist für moderne Unternehmen eine große Gefahr, da sie derzeit die größten Schäden anrichtet.

Im Jahr 2021 kam es unter anderem in der Kraftstoffindustrie[7], in der Lebensmittelbranche [8] und im Gesundheitswesen[9] zu schwerwiegenden Zwischenfällen – kein Ziel ist dabei tabu.

Etwa drei Viertel der Ransomware-Angriffe beginnen – direkt oder indirekt – mit einer Phishing-E-Mail.[10] Dabei werden die Anwender dazu verleitet, einen schädlichen Anhang zu öffnen oder auf eine schädliche URL zu klicken.

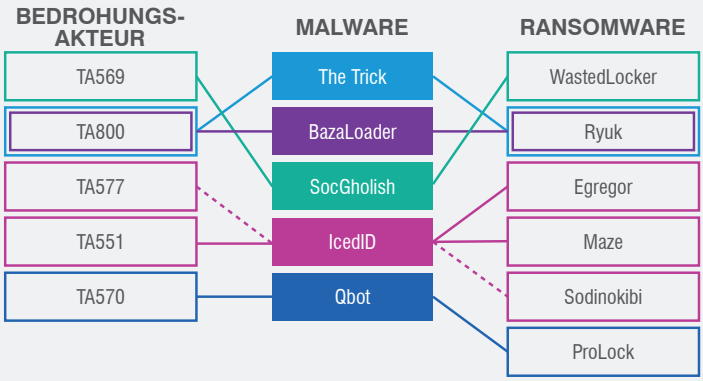


Abb. 2: Verbindungen zwischen Bedrohungsakteuren, Malware der ersten Stufe und Ransomware

Ransomware wird meist als sekundäre Infektion übertragen, nachdem ein System bereits mit einem Trojaner oder Loader infiziert wurde. Viele Angreifer, die sich auf diese Trojaner oder Loader spezialisiert haben, verkaufen den Zugang anschließend an Ransomware-Gruppen. Für die meisten Unternehmen besteht also der beste Schutz vor Ransomware in der Vermeidung anderer Malware-Typen.

Es gibt zwar keine direkte Beziehung zwischen der Erstzugriffs-Malware und der Ransomware-Variante, die an die Opfer verteilt wird, doch haben Proofpoint-Forscher und andere Branchenvertreter einige auffällige Zusammenhänge festgestellt (siehe Abb. 2).

7 David E. Sanger, Clifford Krauss und Nicole Perlroth (New York Times): „Cyberattack Forces a Shutdown of a Top U.S. Pipeline“ (Cyberangriff legt wichtige US-Pipeline still), Mai 2021.
8 Julie Creswell, Nicole Perlroth und Noam Schreiber (New York Times): „Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business“ (Fleischverarbeiter liegt nach größtem Angriff auf kritisches US-Unternehmen still), Juni 2021.
9 Nicole Perlroth und Adam Satariano (New York Times): „Irish Hospitals Are Latest to Be Hit by Ransomware Attacks“ (Irische Krankenhäuser sind neueste Opfer von Ransomware-Angriffen), Mai 2021.
10 Unit 42, Palo Alto Networks: „Ransomware Families: 2021 Data to Supplement the Unit 42 Ransomware Threat Report“ (Daten von 2021 zur Ergänzung des Ransomware-Bedrohungsberichts von Unit 42), Juli 2021.

Business Email Compromise (BEC):

BEC-Betrug (Business Email Compromise), auch bekannt als E-Mail-Betrug, ist eine der kostspieligsten und am wenigsten verstandenen Cyberbedrohungen. Diese stark zunehmende Form von E-Mail-Betrug erregt selten so viel Aufmerksamkeit wie andere medienwirksame Cyberverbrechen, verursacht jedoch erheblich mehr direkte finanzielle Schäden als andere Betrugsformen.

Allein im Jahr 2020 führten BEC-Angriffe bei Unternehmen und Privatpersonen zu Kosten von mehr als 1,8 Milliarden US-Dollar.[11] Das sind 100 Millionen US-Dollar mehr als im Jahr 2019. Gleichzeitig hat BEC einen Anteil von 44 % an den gesamten Verlusten durch Cyberkriminalität.

BEC-Angriffe sind schwer zu erkennen, denn sie enthalten nicht die üblichen Schaddaten wie schädliche URLs oder Dateianhänge, die analysiert werden können. Stattdessen täuschen die Betrüger ihre Opfer mit Nachahmungs- und Social-Engineering-Techniken.

Viele der aktuellen BEC-Maschen sind äußerst raffiniert und werden von kapitalkräftigen Akteuren durchgeführt, die sehr viel Planung und Recherche in ihre Angriffe investieren. Immer mehr Angreifer konzentrieren ihre Bemühungen auf Betrugsversuche mit Lieferantenrechnungen und große B2B-Transaktionen (Business-to-Business), die sie umleiten können.

BEC-Angriffe nutzen menschliches Verhalten und das Vertrauen der Mitarbeiter aus.

Sie gehen dabei wie folgt vor:

1. Zunächst imitieren die BEC-Angreifer Personen oder Unternehmen, denen die Empfänger vertrauen (z. B. Kollegen, Vorgesetzte oder Lieferanten).
2. In E-Mails weisen die Angreifer die Empfänger zu bestimmten Handlungen an, durch sie an Geld oder vertrauliche Informationen des Unternehmens gelangen. Sie nutzen dazu betrügerische Überweisungen, falsche Rechnungen, umgeleitete Gehaltszahlungen, geänderte Bankverbindungen für zukünftige Zahlungen sowie zahlreiche andere Maschen.
3. Wenn die Unternehmen den Fehler bemerken, ist es häufig bereits zu spät, das Geld zurückzuholen.

ARTEN VON BEC-BETRUG

BEC-Betrug gibt es in vielen Formen, die nur durch die Kreativität der Angreifer begrenzt sind. Dies sind die sechs häufigsten Arten:

1. **Rechnungsbetrug:** Bei diesem Angriff werden die Opfer dazu gebracht, gefälschte Rechnungen zu bezahlen oder gültige Zahlungen umzuleiten.
2. **Umleitung von Gehaltszahlungen:** Bei dieser Masche geben sich die Angreifer als Mitarbeiter aus und bitten die Gehaltsabteilung, den Lohn auf ein anderes Konto auszuzahlen.
3. **Erpressung:** Hierbei drohen die Angreifer dem Opfer mit Gewalt oder Bloßstellung, um es zur Zahlung zu bewegen.
4. **Köder und Aufgaben:** Bei dieser Masche werden die Opfer mit einer einfachen Frage wie „Hallo, sind Sie da?“ geködert, was sich dann zu anderen Formen des BEC-Betrugs steigert.
5. **Betrug mit Gutscheinkarten:** Diese Technik bringt die Opfer dazu, Gutscheinkarten zu kaufen und den Betrügern die Nummern und PINs zu schicken.
6. **Provisionsbetrug:** Bei dieser alten Masche bitten die Betrüger um Geld für das Freischalten einer größeren Summe, die niemals kommt.

11. FBI: „Internet Crime Report 2020“ (Bericht zu Internetkriminalität 2020), März 2021.

Kontenkompromittierung und -übernahme

Kontenkompromittierung ist die böswillige Übernahme eines legitimen Anwenderkontos bei einem E-Mail- oder Cloud-Dienst. Damit erhalten die Angreifer weitreichenden Zugriff auf Daten, Kontakte, Kalendereinträge und E-Mails.

Neben den kompromittierten Anwenderdaten können die Angreifer das Konto auch zur Nachahmung des Anwenders per Social Engineering (z. B. bei BEC- und Lieferkettenangriffen) nutzen – sowohl innerhalb als auch außerhalb des Unternehmens.

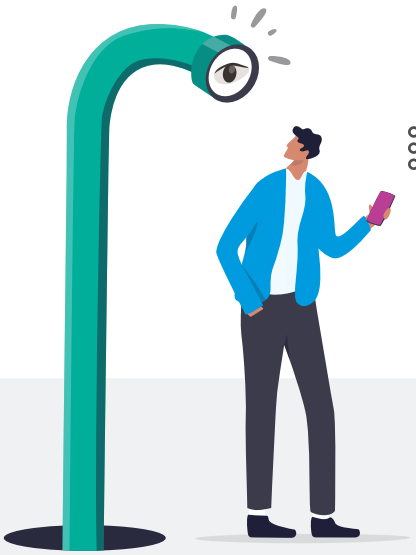
Bedrohungsakteure können auf vertrauliche Daten zugreifen, andere Anwender oder externe Geschäftspartner zu Banküberweisungen verleiten oder den Ruf und die Finanzen eines Unternehmens ruinieren. Zudem können sie Backdoor-Trojaner installieren, die den Zugriff für weitere Angriffe aufrechterhalten.

Der Ablauf einer Cloud-Kontoübernahme

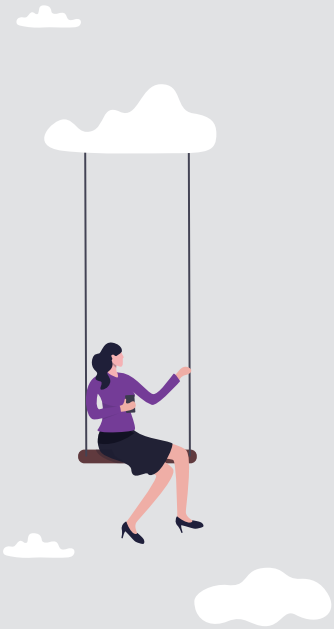
Im Folgenden wird beschrieben, wie die Mehrzahl der Cloud-Kontenübernahmen abläuft.

Diebstahl von Anmeldedaten: Die Angreifer erlangen Zugriff auf die Anmeldedaten von Anwendern durch Anmeldedaten-Phishing (das allein zwei Drittel des gesamten Aufkommens an Phishing-Betrug ausmacht), Brute-Force-Angriffe auf Kennwörter, die Wiederverwendung von Anmeldedaten oder Malware, die Anmeldedaten stiehlt.

Infiltration: Nachdem sich der Angreifer beim Anwenderkonto anmelden konnte, hat er Zugriff auf E-Mails, Kontakte, Dateien und den Kalender des Opfers. Die Angreifer können die Daten entweder direkt stehlen oder damit überzeugend Anwender imitieren. Einige Betrüger antworten auf bestehende E-Mail-Threads oder verschicken E-Mails mit Malware oder gefährlichen URLs an Kollegen und externe Geschäftspartner. Der Angreifer imitiert den kompromittierten Anwender und wendet sich dann mit gefälschten Rechnungen oder Hinweisen zu geänderten Kontoverbindungen an andere Personen innerhalb oder außerhalb des Unternehmens. Mitunter lädt der Angreifer auch Malware auf interne Dateifreigaben hoch oder sabotiert das Unternehmen auf andere Weise.



Persistenz: Häufig richtet der Angreifer heimlich automatische Weiterleitungsregeln ein, durch die er den Zugang zu den E-Mails eines Anwenders behält, selbst wenn dieser das Kennwort ändert. Durch den Einblick in alle eingehenden E-Mails und Kalendereinladungen erhält der Angreifer wichtige Informationen für spätere Nachahmer-Angriffe.



ABSCHNITT 2

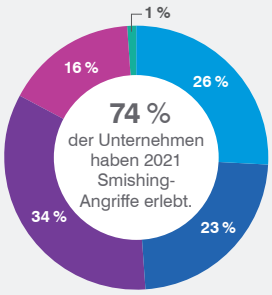
Veränderungen der Bedrohungslandschaft

Die heutigen Remote- und Hybrid-Arbeitsplätze basieren auf Cloud- und mobilen Technologien.

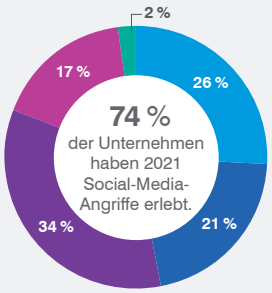
Die abgesicherten Perimeter und traditionellen Netzwerkstrukturen der Vergangenheit sind so gut wie verschwunden. Jetzt sind Ihre Mitarbeiter der neue Perimeter.

Leider halten die meisten Sicherheitsbudgets – bedingt durch andere Prioritäten und Produktkategorien – mit dieser Entwicklung nicht Schritt.

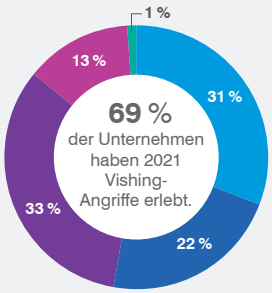
Aufkommen der Smishing-Angriffe



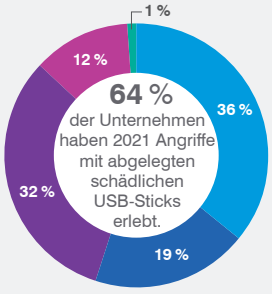
Aufkommen der Social-Media-Angriffe



Aufkommen der Vishing-Angriffe



Aufkommen abgelegter schädlicher USB-Sticks



Quelle: State of the Phish 2022

Angriffe richten sich gegen Menschen, nicht gegen die Infrastruktur

Selbst mit jährlichen Ausgaben in Milliardenhöhe für die Absicherung von Infrastruktur vernachlässigen viele Unternehmen die wichtigsten personenzentrierten Sicherheitsrisiken. Der Mensch ist der einfachste und lukrativste Eintrittspunkt in Ihre Umgebung.

Laut dem „Verizon Data Breach Investigations Report“ ist an sage und schreibe 85 % der Kompromittierungen der Faktor Mensch beteiligt.[12] Ihre Anwender sind einer ständigen Flut von unsicheren Links, schädlichen Anhängen, Anmeldedaten-Diebstahl, Social-Engineering-Maschen und Impostor-Bedrohungen ausgesetzt.

Angriffe erfolgen häufig über mehrere Vektoren

Angriffe auf Mitarbeiter finden immer in den Tools und Plattformen statt, die sie verwenden. Die Angreifer folgen also den Anwendern.

Moderne Workflows sind dynamisch und unvorhersehbar. Die Anwender können eine Konversation per E-Mail beginnen, anschließend ein Treffen in ihrer Chat-Anwendung vereinbaren und gemeinsam an Dateien arbeiten, die in der Cloud gespeichert sind.

Doch auch moderne Angriffe sind dynamisch und unvorhersehbar. Dabei kommen mehrere Kanäle sowie eine Mischung von Taktiken und Tools auf allen Plattformen zum Einsatz, die die Mitarbeiter zum Arbeiten nutzen.

Ein Angriff kann beispielsweise mit einer E-Mail und einem Link auf Malware beginnen, die auf einer Dateitausch-Website gehostet ist. Oder eine nicht autorisierte Cloud-Anwendung stiehlt Anmeldedaten, um ein legitimes Konto zu kompromittieren und darüber BEC-Angriffe auszuführen.

Das Problem nimmt weiter zu. Fortgeschrittene Bedrohungsakteure entwickeln häufig Malware-„Produkte“ und stellen sie dann über eine passende Infrastruktur als leicht zu bedienende Pakete oder Services zur Verfügung. Interessierte Cyberkriminelle können diesen Service dann für ihre Angriffe mieten. Sie bezahlen für einen bestimmten Zeitraum oder bekommen für jede erfolgreiche Kompromittierung einen Anteil an der Beute. In anderen Fällen agieren die Kriminellen als Verteiler, die die Malware über E-Mails versenden und mit einer Provision für jede erfolgreiche Infizierung vergütet werden.

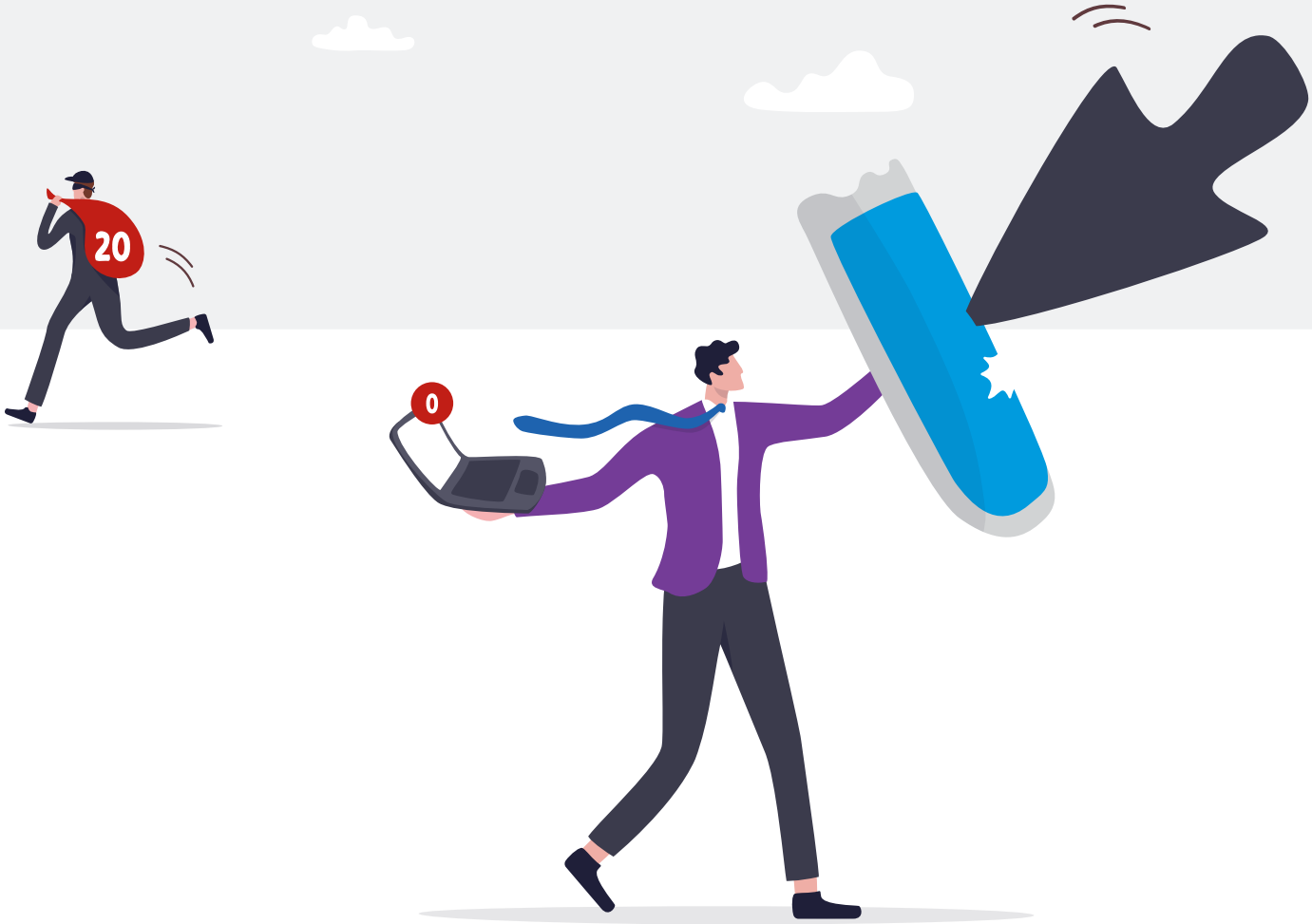
12 Verizon: „Data Breach Investigations Report Executive Summary“ (Untersuchungsbericht zu Datenkompromittierungen: Kurzfassung), Mai 2021.

Es genügt nicht, alle Vektoren abzusichern

Die Unternehmen wissen zwar um die vielschichtige, personenzentrierte Ausrichtung der heutigen Bedrohungen und investieren in Sicherheitstools, die alle potenziellen Risiken minimieren. Allerdings müssen diese Tools auch koordiniert zusammenarbeiten, um den Sicherheitsteams den Überblick und die Erkenntnisse bereitzustellen, die sie für die Bewältigung von Risiken benötigen.

Stellen Sie sich eine Mannschaft von Fußball-Superstars vor, die nicht miteinander trainieren, ein Orchester von Virtuosen, die die anderen Instrumente nicht hören, oder ein Operationsteam, das sich auf keine Vorgehensweise einigen kann. Egal wie kompetent jeder Einzelne ist: Sie werden niemals so gut sein wie ein eingespieltes Team.

Die Angreifer kombinieren heute mehrere Techniken und machen ihre Angriffe damit noch raffinierter. Eigenständige Einzelprodukte erzeugen unnötige Komplexität für das Sicherheitsteam, das bereits mit der Bewältigung der aktuellen Risiken Schwierigkeiten hat. Deshalb erfordern personenzentrierte Sicherheitsmaßnahmen einen ganzheitlichen und koordinierten Ansatz.



ABSCHNITT 3

Fokus auf die besonders gefährdeten Anwender

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 mit welchen Bedrohungen 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.

Konzentrieren Sie sich auf Anwender, die aufgrund dieser Faktoren ein überdurchschnittliches Risiko darstellen. Aufgrund ihres Status bedürfen sie besonderer Aufmerksamkeit seitens des Sicherheitsteams und der Verantwortlichen, die wissen sollten, wie und weshalb sie gefährdet sind.

Sie müssen alle drei Bereiche genau analysieren, um personenzentrierte 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 personenzentrierten 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.

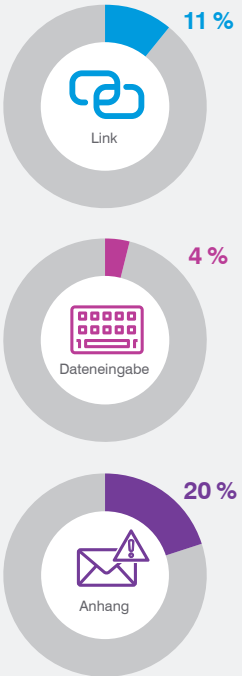
Die Arbeitsweise Ihrer Mitarbeiter

Sie erhalten eine allgemeine Vorstellung über die Anfälligkeit von Anwendern, wenn Sie sich die Tools, Plattformen und Anwendungen anschauen, die sie verwenden. Dazu gehören unter anderem folgende Faktoren:

- Genutzte Cloud-Anwendungen und ob diese von der IT-Abteilung autorisiert wurden
- Anzahl und Art der Geräte, die für den E-Mail-Zugriff genutzt werden
- Sicherheitsstufe dieser Geräte
- Einhaltung digitaler Hygiene (z. B. starke individuelle Kennwörter) und ob Software auf dem neuesten Stand gehalten wird
- Durchgängige Nutzung von Multifaktor-Authentifizierung für den Zugriff auf Unternehmens- und sogar private Konten

Je detaillierter Ihre Übersicht, desto besser.

Phishing-Vorlagen-Typen: Durchschnittliche Fehlerquoten



Quelle: State of the Phish 2022

Klickverhalten Ihrer Mitarbeiter

Die Anfälligkeit lässt sich anhand von Sicherheitsschulungen, simulierten Phishing-Angriffen und der Reaktion auf tatsächliche Bedrohungen präziser bewerten.

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.

Bevor Sie Angreifer ins System lassen, um zu sehen, wer auf einen Link klickt, ein Formular ausfüllt oder eine Datei öffnet, sind Phishing-Simulationen eine äußerst wirkungsvolle Methode, um diese potenzielle Schwachstelle zu beurteilen.

Und nicht zuletzt sollten Sie unbedingt die Anwender beobachten, die auf bekanntermaßen schädliche E-Mails hereinfallen, selbst wenn die angeklickte URL blockiert, isoliert oder geändert wurde.

Mithilfe der praxisbezogenen Daten und der Informationen über das Sicherheitsbewusstsein erhalten Sie einen ganzheitlichen Überblick über die Anfälligkeit für E-Mails, da das Bestehen von Schulungen und Phishing-Simulationen sowie die Reaktion auf echte schädliche Nachrichten erfasst wird.

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 hinsichtlich der angesprochenen Personen extrem zielgerichtet 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. Bei Proofpoint nennen wir diese Anwender Ihre Very Attacked People™ (VAPs), also die besonders häufig angegriffenen Personen. Durch eine vollständige Übersicht über den gesamten E-Mail-Verkehr und die Verknüpfung mit Bedrohungsdaten lässt sich erfassen, wer in welchem Maß angegriffen wird.

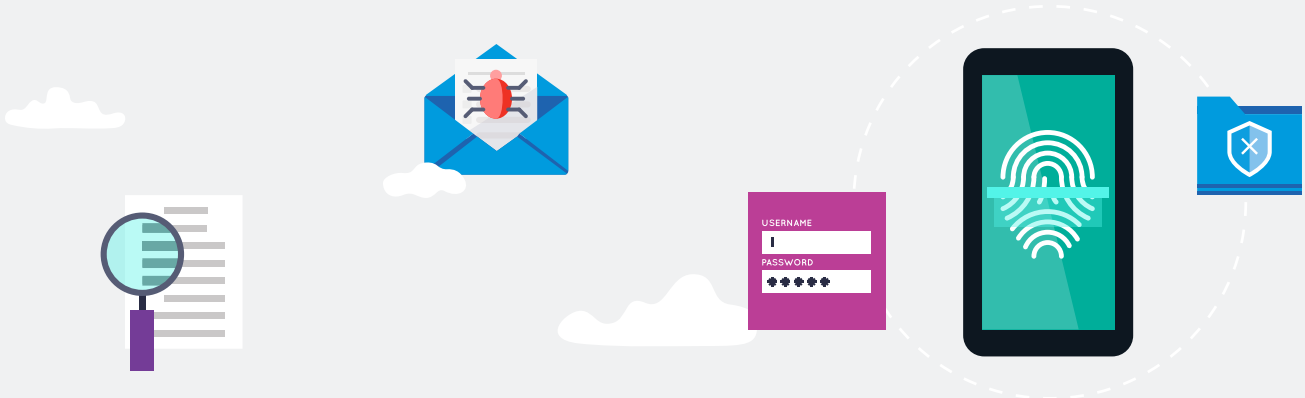
Diese Faktoren sollten bei der Bewertung der Anwenderrisiken am schwersten wiegen:

- 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.

Durch gute Bedrohungsdaten können die von den Angreifern verwendeten Tools ermittelt und scheinbar für sich allein stehende Zwischenfälle größeren Kampagnen zugeordnet werden.



Berechtigungen: 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. Sie sollten wissen, wo sich die vertraulichsten Daten befinden und welche Nutzer und Anwendungen Zugriff darauf haben.

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.

Umfassend berechtigte Anwender müssen unbedingt vor äußeren Angriffen geschützt werden. Doch genauso wichtig ist der Schutz des Unternehmens vor ebendiesen Anwendern. In den falschen Händen kann Insider-Zugriff aus Böswilligkeit, Fahrlässigkeit oder durch eine Kompromittierung missbraucht werden. Kompromittierte Konten könnten vertrauliche Dateien exportieren oder versuchen, andere interne Anwender zu kompromittieren oder zu betrügen.

ABSCHNITT 4

Aufbau personenzentrierter Schutzmaßnahmen

Ein personenzentrierter Ansatz gewährleistet den Schutz aller Mitarbeiter, da Kontrollen entsprechend des jeweiligen Risikos zur Anwendung kommen. Er wirkt zudem unabhängig davon, welche Plattform die Mitarbeiter nutzen, welche Taktik die Angreifer einsetzen und über welchen Bedrohungsvektor ein Angriff erfolgt.

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.

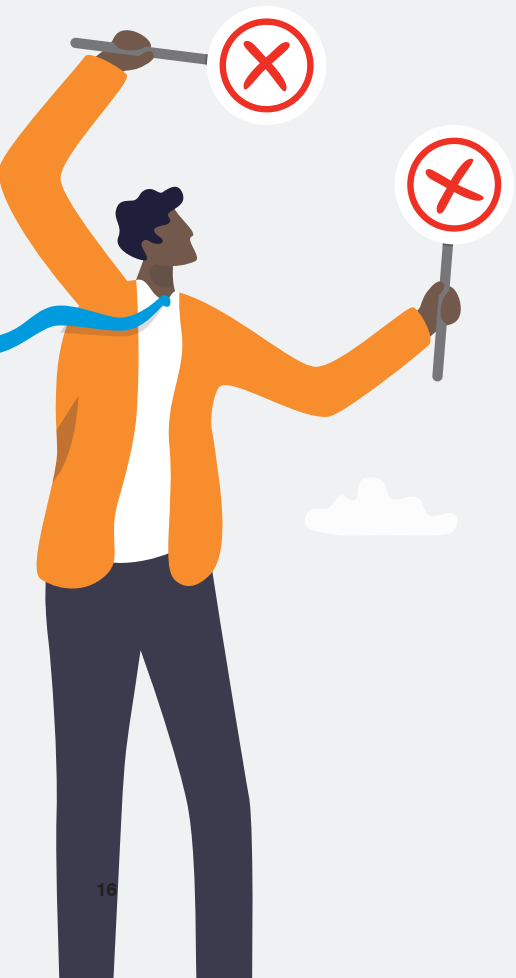
Das sind die wichtigsten Schritte, um moderne E-Mail-Bedrohungen abwehren zu können:

- Stoppen von schädlichen Anhängen und URLs, bevor sie den Posteingang der Anwender erreichen
- Stoppen von Schaddaten-losen Angriffen mit gefälschter Identität wie 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 unternehmens-eigenen Geräten, indem adaptive Isolierungstechnologie zum Einsatz kommt
- Mehr Anwendersicherheit durch Security-Awareness-Schulungen und kontextbezogene Hinweise
- Anwendung von Kontrollen wie Web-Isolierung, um potenziell unsichere Surfgewohnheiten der Anwender von der Unternehmensumgebung fernzuhalten
- Einbeziehung von Datenschutz in die E-Mail-Sicherheitsstrategie

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 kommen die erweiterten E-Mail-Sicherheitsmaßnahmen ins Spiel. Wenn Schaddaten gestoppt werden, bevor sie den Posteingang der Anwender erreichen, kann eine effektive Lösung Unternehmen vor vielfältigen Malware-Bedrohungen schützen, darunter Ransomware, Bank-Trojaner, Remote-Zugriffs-Trojaner, Informationsdiebe (Stealer), Downloader, Botnets usw.



Stoppen von Bedrohungen mit gefälschter Identität, die nur schwer erkennbar sind

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

BEC, eine Form des Überweisungsbetrugs, ist hierfür ein Beispiel. Laut dem FBI gibt es Meldungen von BEC-Angriffen aus allen 50 US-Bundesstaaten und 177 Ländern – und die betrügerischen Überweisungen gingen dabei in mindestens 140 Länder.[13]

Bei BEC und anderen Formen von E-Mail-Betrug 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 mehrschichtigen Schutz, der eingehende, ausgehende und interne E-Mails abdeckt – und dabei ganzheitlich und einheitlich vorgeht.

13. FBI: „Internet Crime Report 2020“ (Bericht zu Internetkriminalität 2020), März 2021.

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.

DMARC

Setzen Sie E-Mail-Authentifizierung per DMARC (Domain-based Message Authentication, Reporting and Conformance) ein. 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 usw. 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:

- E-Mail-Header, IP-Adresse und Versender-Reputation
- Machine Learning-basierte Inhaltsanalysen, bei denen nach Manipulationen des Reply-To-Felds sowie nach bestimmten Wörtern und Formulierungen gesucht wird
- Beziehung zwischen Absender und Empfänger
- Kontextinformationen zum Absender, z. B. ob ein bekannter Lieferant nachgeahmt wird

Erkenntnisse zu Schutzmaßnahmen für interne E-Mails und Lieferantenrisiken

In einigen Fällen versuchen die Angreifer erst gar nicht, ihre E-Mail-Adresse zu verschleiern. Stattdessen übernehmen sie einfach ein legitimes Konto des Unternehmens oder eines Lieferanten bzw. Partners. 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.

Der Schutz interner Anwender sowie Kontextinformationen zu Lieferantenrisiken sind für eine effektive E-Mail-Sicherheit entscheidend.

Mehr Anwendersicherheit 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. Viele dieser E-Mails werden nicht nur vom Empfänger, sondern durch Weiterleitungen auch von anderen angeklickt.

Security-Awareness-Schulungen können – insbesondere als Grundlage einer umfassenden Sicherheitskultur – entscheidend dazu beitragen, die Anwender zu einer starken letzten Verteidigungslinie zu machen. Sie müssen jedoch gezielt, kontinuierlich und zeitnah erfolgen, um die gewünschte Wirkung erzielen zu können. Ganz allgemeine Schulungen einmal im Jahr tragen nicht dazu bei, das Verhalten der Anwender zu ändern oder eine Sicherheitskultur aufzubauen.

Zudem steigern E-Mail-Tags mit kontextbezogenen Hinweisen über die jeweilige Nachricht die Wahrscheinlichkeit, dass Anwender potenzielle Bedrohungen erkennen und melden. Wenn der E-Mail-Tag beispielsweise darauf hinweist, dass die E-Mail von einer externen Adresse stammt oder aber die E-Mail-Domäne einer vertrauenswürdigen Marke täuschend ähnlich ist, können Anwender potenzielle Phishing-Versuche leichter erkennen.

Als weitere Kontrollmaßnahmen dienen Web- und E-Mail-Isolierung, um automatisch Klicks einzudämmen und zu scannen, die bei Nachrichten erfolgen, die zu gefälschten Anmeldedaten-Websites führen oder schädliche Anhänge mit bzw. URLs zu Malware oder anderen Bedrohungen enthalten können. Dies lässt sich je nach Risiko auf Ihre am meisten gefährdeten Anwender, VIPs oder eine breitere Nutzerschicht anwenden.

15,4 Mio. USD

Schäden pro angegriffenem Unternehmen im Jahr 2021.

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, Datenverlustprävention), 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 2021 pro Unternehmen einen durchschnittlichen Schaden von 15,4 Millionen US-Dollar.[14]

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

14 Ponemon Institute: „2022 Cost of Insider Threats: Global Report“ (Kosten von Insider-Bedrohungen 2022: Weltweit), Januar 2022.

Adaptive Ebene: adaptive Kontrollen für stärker gefährdete Anwender

Personenzentrierte Schutzmaßnahmen berücksichtigen, dass einige Anwender zusätzlichen Schutz und weitere Kontrollmaßnahmen benötigen. Bei diesen Anwendern besteht möglicherweise ein größeres Risiko, dass sie Opfer von Angriffen werden, oder sie werden intensiv von Angriffen ins Visier genommen oder sie verfügen über umfangreiche Berechtigungen für Zugriffe auf vertrauliche Daten und Systeme oder es liegt eine Kombination dieser drei Faktoren vor, wodurch das allgemeine Risiko weiter steigt.

Dies sind grundlegende Kontrollen für stärker gefährdete Anwender:

- 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

Gezielte Schulungen zur Steigerung des Sicherheitsbewusstseins

Unternehmensweite Sicherheitsschulungen sind gut geeignet, um 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 gefährdeten Anwender – nicht nur für die Personen, die als besonders anfällig gelten.

Anwender, die aufgrund ihres Angriffsprofils als besonders gefährdet 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.

Adaptive, risikobasierte Kontrollen

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 seiner 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

Für Cyberkriminelle bieten kompromittierten Konten praktisch die „Lizenz zum Stehlen“.

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.

Reaktionsebene: Bedrohungen schneller und effizienter stoppen

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 personenzentrierte 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
- Isolierung unsicherer E-Mails
- 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 den IT-Sicherheitsverantwortlichen die Möglichkeit, sich auf Dinge zu konzentrieren, die am besten von Menschen durchgeführt werden. Statt auf eine Flut an Bedrohungen nur zu reagieren, können sie auf diese Weise proaktive Maßnahmen ergreifen.

Die Rolle von künstlicher Intelligenz und Machine Learning

Angriffe zielen auf Menschen ab und nutzen deren Schwächen aus. Und letztendlich sind auch die Angreifer einfach Menschen.

Um sie zu stoppen, sind moderne Lösungen erforderlich, die sich an das menschliche Verhalten anpassen können. Deshalb ist Machine Learning (ML) eine entscheidende Komponente jeder personenzentrierten Sicherheitsstrategie.

ML ist schneller und effektiver als manuelle Analysen und kann sich im Gegensatz zu traditionellen regelbasierten Algorithmen zudem schnell an neue und sich verändernde Bedrohungen und Trends anpassen.

ML zur Abwehr von BEC-Betrug

Nehmen wir als Beispiel BEC-Betrug. BEC-Angriffe mit Lieferantenrechnungen sind raffinierte und komplexe Betrugsversuche, mit denen die Angreifer Geld stehlen wollen. Hierbei werden häufig betrügerische Rechnungen versendet oder aber die Angreifer versenden Benachrichtigungen über geänderte Bankverbindungen (wobei das neue Konto vom Angreifer kontrolliert wird).

Traditionelle Sicherheitstools tun sich mit dieser Angriffsart schwer, da die Angriffe sehr gezielt erfolgen und keine Schaddaten enthalten. ML kann dynamisch eine breite Palette an Nachrichtenattributen analysieren (z. B. Header-Informationen, Domäne und Nachrichtentext), um Impostor-Nachrichten oder kompromittierte Lieferanten zu erkennen.

Analyse von Anmeldedaten-Phishing

Anmeldedaten-Phishing ist ein weiteres Beispiel. Bei diesen Social-Engineering-Angriffen werden die Opfer häufig über gefälschte Anmelde-Websites dazu gebracht, ihre Anmeldedaten herauszugeben. Die Seiten sind in der Regel so gut gemacht, dass der menschliche Betrachter keinen Unterschied feststellen kann. Moderne Sicherheitstools können jedoch dank der schnellen Überprüfung und Analyse von URLs durch ML und Computer Vision alle E-Mails erkennen und blockieren, die auf gefälschte Websites verweisen. ML kann erkennen, wenn riskante URLs (selbst wenn sie neu registriert sind) auf einer Dateiaustausch-Website gehostet sind oder hochentwickelte Umgehungstechniken wie CAPTCHA verwenden.

Garbage in, garbage out

Im Gegensatz zu den herkömmlichen regelbasierten Softwaresystemen basiert das ML-Verhalten auf Daten und wird nicht vom Menschen programmiert. Das bedeutet, dass ML-Systeme nur so gut sind, wie die Menschen, die sie trainieren, und die dabei genutzten Daten.

Achten Sie bei der Bewertung von Anbietern und den angepriesenen ML-Funktionen auf ML-basierte Modelle, die mit großen Bedrohungsdatensätzen trainiert wurden. Die Daten sollten Erkenntnisse enthalten, die bei führenden Unternehmen der Fortune 100, Fortune 1000 und Fortune Global 2000 sowie von so vielen Internetdienstleistern sowie kleinen und mittleren Unternehmen wie möglich gewonnen wurden. Zudem sollten sie unbedingt mehrere Angriffsvektoren wie E-Mail, die Cloud, Netzwerke und soziale Medien umfassen, da die Angreifer nicht nur E-Mail-basierte Bedrohungen nutzen.

Vergessen Sie außerdem nicht, welche Rolle kompetente Bedrohungsforscher beim Training von ML-Modellen spielen. Selbst die besten Datenwissenschaftler können effektive ML-Modelle nicht allein entwickeln. Sie benötigen Fachkompetenz, die durch langjährige Erfahrung in der Forschung und Analyse von Bedrohungen entsteht.

CHECKLISTE

Worauf sollten Sie bei einer Sicherheitslösung Wert legen?

Personenzentrierte Sicherheit ist mehr als nur ein Marketing-Schlagwort – es ist eine grundlegend neue Sichtweise auf Bedrohungen und deren Abwehr. Am Anfang steht der richtige Ansatz. Es sind jedoch auch die richtigen Tools und Funktionen erforderlich.

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

Eine einheitliche, integrierte und skalierbare Plattform

Eine personenzentrierte Sicherheitslösung ist weit mehr als die Summe ihrer Teile. Mit Einzellösungen können Sie einen Teil Ihres Sicherheitsproblems bewältigen. Die Abwehr moderner Bedrohungen erfordert jedoch einen ganzheitlichen integrierten Ansatz, der alle von den Angreifern verwendeten Taktiken, Tools und Vektoren berücksichtigt – auf allen Geräten, Plattformen und Kanälen, die Ihre Mitarbeiter nutzen.

Durch nicht integrierte Sicherheitsprodukte mit mehreren Konsolen entstehen sich überschneidende und unübersichtliche Workflows, wodurch Zeit und Ressourcen verschwendet werden. Die Folge sind eine zusammenhanglose Sicht auf Bedrohungen, unnötige Arbeit und erhöhte Verwaltungskomplexität.

Suchen Sie nach Lösungen, die eine breite Palette an Bedrohungen abdecken und mit Ihrem Sicherheitsökosystem zusammenarbeiten. Abhängig vom jeweiligen Unternehmen gehören dazu Komponenten wie Firewalls der nächsten Generation sowie Tools für SIEM (Sicherheitsinformations- und Ereignis-Management) und Identitätsverwaltung.

Effektive Sicherheit für alle Anwender

Die beste Methode zur Abwehr von E-Mail-Angriffen ist ein mehrstufiger Ansatz, wie er von Gartner und anderen Experten seit langem empfohlen wird.

Folgende Bedrohungen sollte Ihr Sicherheitssystem abwehren können:

- Spam- und unerwünschte Massen-E-Mails
- Angriffe mit schädlichen Anhängen und URLs
- Angriffe ohne Schaddaten, z. B. 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:

- Kurzschulungen, um Motivation und Verhaltensänderung zu gewährleisten
- Phishing-Simulationen, die auf realen Kampagnen basieren, um Anwender zu Bedrohungen zu schulen, mit denen sie mit hoher Wahrscheinlichkeit konfrontiert werden
- Fortlaufende datenbasierte Schulungen für anfällige Anwender, die gezielt angegriffen werden oder mit echten Phishing-Nachrichten interagieren
- E-Mail-Tags, die Anwender auf verdächtige Nachrichten hinweisen, inklusive integrierter Meldungsmechanismen und Feedback an Anwender

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 und Klassifizierung von Inhalten sowie bei Bedarf Blockieren von E-Mail-Versand, Transfer in die Cloud oder Übertragung auf USB-Gerät
- Identifizierung böswilliger, fahrlässiger oder kompromittierter Anwender sowie Unterstützung der IT-, Personal-, Rechts- und Sicherheitsabteilungen beim Ergreifen angemessener Maßnahmen zur Verhinderung von Schäden
- Identifizierung und Schutz aller Standardformate von regulierten Inhalten, z. B. PCI DSS, HIPAA, FINRA
- Automatische Umleitung, Verschlüsselung und Ablehnung von E-Mails, die Sicherheits- und andere Richtlinien verletzen, sowie Warnung der zuständigen Personen im Unternehmen

Adaptive Kontrollen für stärker gefährdete Anwender

Aufgrund ihrer Schwachstellen, Angriffsprofile und Berechtigungen stark gefährdete Anwender müssen durch zusätzliche Sicherheitskontrollen geschützt werden. Eine personenzentrierte 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 die Schwachstellen, Angriffsprofile und Berechtigungen Ihrer Anwender auf einfache Weise 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 in der Umgebung, in der Cloud und am Standort, einschließlich automatisierter Korrekturmaßnahmen wie Analyse von Anwendern gemeldeter E-Mails, Entfernen verifizierter Bedrohungen aus den Posteingängen der Anwender und Zurücksetzen der Kennwörter kompromittierter Konten

WEITERE INFORMATIONEN

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

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. 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 75 Prozent der Fortune-100-Unternehmen, setzen auf die personenzentrierten 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.

0301-001-01-03 03/22