proofpoint.

E-BOOK

Handbuch zur Sensibilisierung für Sicherheit

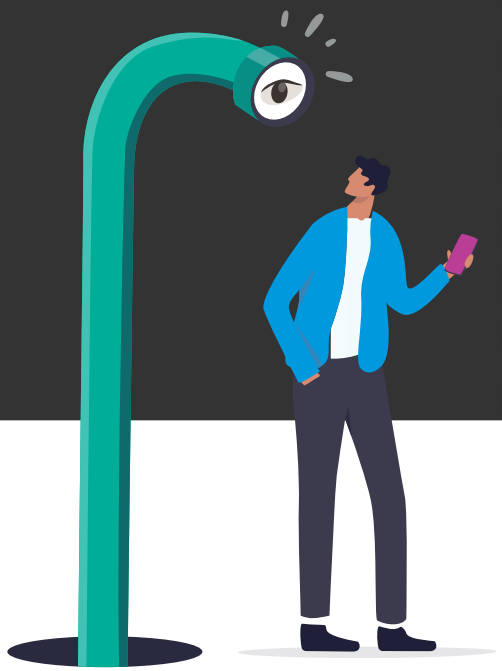
Sechs wichtige Themen, die alle Anwender kennen und Unternehmen in Schulungen berücksichtigen sollten

Einführung

Moderne Cyberbedrohungen setzen auf menschliche Interaktionen und nicht nur auf technische Exploits. Laut dem Data Breach Investigations Report (Untersuchungsbericht zu Datenkompromittierungen) von Verizon werden 82 % aller Datenschutzverletzungen durch menschliches Verhalten verursacht. Dort heißt es: „[…] der Mensch rückt angesichts dieser Fakten in den Mittelpunkt jeder Sicherheitsstrategie“.[1]

Durch Social Engineering verleiten Angreifer ihre Opfer dazu, auf unsichere URLs zu klicken, schädliche Anhänge zu öffnen, ihre Anmeldedaten einzugeben, vertrauliche Daten weiterzugeben, Geld zu überweisen und vieles mehr.

Deshalb können Sie die Sicherheit Ihres Unternehmens nur dann gewährleisten, wenn Sie Ihre Mitarbeiter in der Abwehr von Cyberbedrohungen schulen. Bedrohungsschutz- und Erkennungstechnologien können nicht jeden Angriff stoppen.



Ihre Mitarbeiter müssen darauf vorbereitet werden, diese modernen Bedrohungen zu erkennen und angemessen zu reagieren.

Dem Angriffsaufkommen und der Vielzahl der verwendeten Vektoren sind nur durch die Kreativität der Bedrohungsakteure Grenzen gesetzt. Doch die meisten Taktiken gehören zu den wenigen Kategorien, die sich auf die aktive Beteiligung der Opfer verlassen. Die gute Nachricht: Sie können Ihre Anwender darin schulen, diese Bedrohungen zu erkennen, abzuwehren und zu melden, bevor dauerhafter Schaden für das Unternehmen entsteht.

In diesem E-Book werden die Risiken erläutert, mit denen Ihre Anwender am wahrscheinlichsten konfrontiert werden:

- Social Engineering
- Phishing
- Business Email Compromise (BEC)
- Soziale Netzwerke
- Ransomware
- Risiken durch Insider

Wir gehen dabei detailliert auf jede Bedrohung ein, sehen uns die jeweilige Funktionsweise sowie den potenziellen Schaden an und zeigen auf, wie Sie Ihre Anwender dafür sensibilisieren und darauf vorbereiten können.

1 Verizon: „2022 Data Breach Investigations Report“ (Untersuchungsbericht zu Datenkompromittierungen 2022), Juni 2022.

Inhaltsverzeichnis

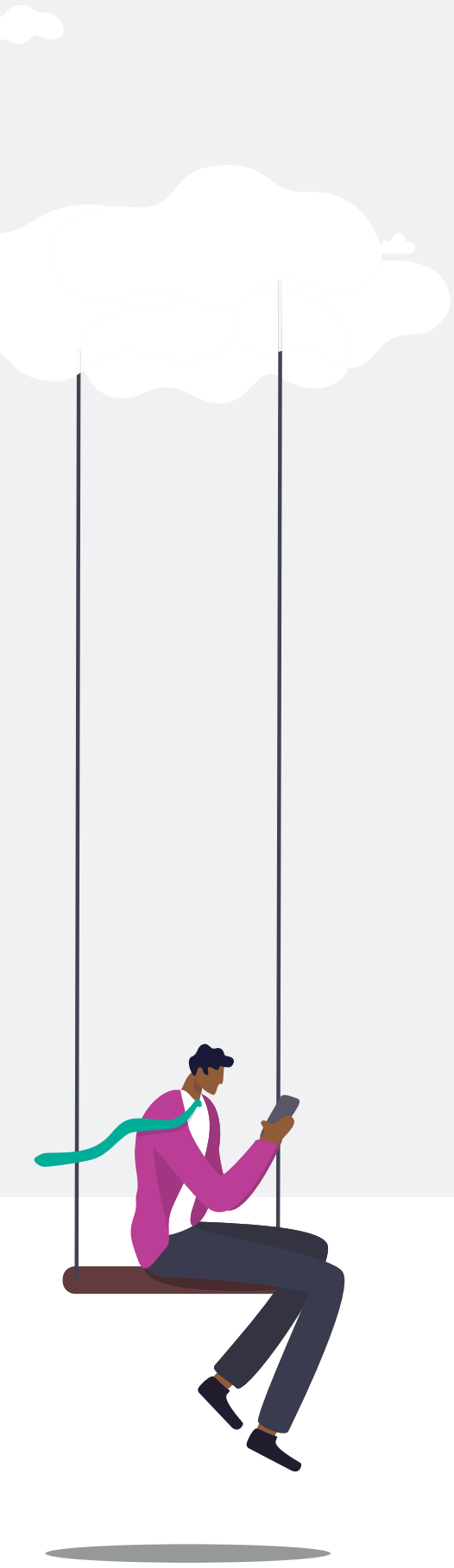
ABSCHNITT 1

Social Engineering

Das Ziel eines Security-Awareness-Programms besteht darin, das menschliche Risiko zu verringern und eine robuste Sicherheitskultur aufzubauen, die Verhaltensänderungen fördert.

Anwender müssen motiviert werden und ihre wichtige Rolle als Verteidiger des Unternehmens an vorderster Front annehmen. Sie müssen wissen, wie Angreifer versuchen, sie zu den gewünschten Aktionen zu bewegen, und warum sie angegriffen werden. Deshalb gehört Social Engineering, das bei praktisch allen personenzentrierten Angriffen eine Rolle spielt, zu den wichtigsten Themen bei Schulungen zur Steigerung der Cybersicherheitsbewusstseins.

Aber auch sehr erfahrene Anwender profitieren davon, sich die Grundlagen des Social Engineering noch einmal anzusehen. Beginnen wir also mit einer Definition.



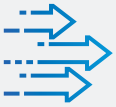
Was ist Social Engineering?

Als Social Engineering werden verschiedene Taktiken bezeichnet, die von böswilligen Akteuren eingesetzt werden, um die menschliche Psychologie zu manipulieren und ihre Opfer zu verschiedenen Aktionen zu verleiten, zum Beispiel:

Weitergeben von Kontoanmeldedaten

Weitergeben von vertraulichen Daten

Ausführen von schädlichem Code



Überweisen von Geldern

Warum setzen Angreifer für so viele Kampagnen stark auf Social Engineering? Weil sie wissen, dass Menschen den leichtesten Weg in eine geschützte Umgebung darstellen. (Außerdem: Warum sollten sie sich die Hände schmutzig machen, wenn sie jemanden dazu bringen können, das für sie zu tun?)

Wie setzen Angreifer Social Engineering ein, um den Faktor Mensch auszunutzen?

Wenn Sie bei Cybersicherheitsschulungen über Social Engineering sprechen, gehen Sie dabei auf jeden Fall auch darauf ein, *wie* Angreifer dabei vorgehen. Erklären Sie zum Beispiel, dass Bedrohungsakteure diese menschlichen Eigenschaften ausnutzen:

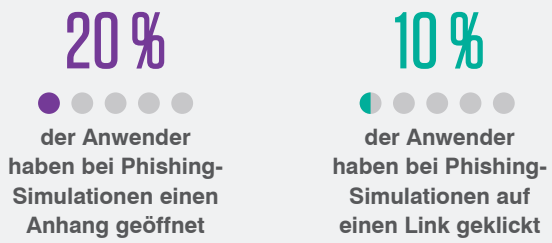
- **Emotionen:** Sie schaffen ein Gefühl von Dringlichkeit, erzeugen Begeisterung für eine Gelegenheit oder schüren Angst davor, Geld zu verlieren oder sich falsch zu verhalten.
- **Vertrauen:** Sie geben sich als eine Person aus, der der Anwender vertraut, oder missbrauchen eine vertrauenswürdige Marke oder Organisation (z. B. Steuerbehörde, UPS, Amazon, Microsoft).
- **Müdigkeit:** Sie starten ihre Angriffe zu einem Zeitpunkt, zu dem die Anwender häufig müde oder abgelenkt sind und daher eher rein emotionale Entscheidungen treffen.

Arten von Social-Engineering-Angriffen

Security-Awareness-Schulungen zum Thema Social Engineering sollten einige gängige Techniken abdecken.

Phishing

Bei dieser Methode werden schädliche E-Mails gesendet, die Menschen zu einer bestimmten Aktion verleiten sollen, z. B. auf einen schädlichen Web-Link in der E-Mail klicken oder einen Anhang öffnen. Untersuchungen für den State of the Phish 2022-Bericht von Proofpoint zeigen, wie häufig und effektiv Phishing ist: Im Jahr 2021 haben 86 % der Unternehmen massenhafte Phishing-Angriffe erlebt. Bei Phishing-Simulationen öffnen 20 % der Anwender E-Mail-Anhänge und 10 % klicken auf einen Link.



Social-Media-Spionage

Angreifer nutzen häufig soziale Netzwerke, um Informationen zu Anwendern zu sammeln, die sie anschließend bei Kampagnen einsetzen. Sie können zum Beispiel bei LinkedIn Informationen zu einer Führungskraft eines Unternehmens finden und diese Person daraufhin bei einer Phishing-Kampagne nachahmen, um Mitarbeiter der Finanzabteilung anzugreifen. Die Spionagemaßnahmen können jedoch auch das soziale Umfeld eines Ziels einschließen.

Vishing und Smishing

Bei dieser Social-Engineering-Technik verwenden Angreifer Textnachrichten und Stimmverzerrer, um SMS-Nachrichten an Anwender zu senden oder sie über Robocalls anzurufen. Bei diesen Nachrichten stellen sie häufig Geschenke oder Services als Gegenleistung für eine Zahlung in Aussicht. Diese Betrugsformen werden als Vishing (Voice-Phishing) und Smishing (SMS-/Testnachrichten-Phishing) bezeichnet. (Lesen Sie unseren Blog, um mehr über die Unterschiede zwischen Vishing und Smishing zu erfahren.)

Angriffe per Telefon

Wie wir in unserem Bericht zum Faktor Mensch 2022 gezeigt haben, ist die Zahl von Angriffen per Telefon (auch als Callback-Phishing bezeichnet) in den vergangenen Monaten enorm gestiegen. Diese Angriffe beginnen häufig mit einer E-Mail und erfolgen über mehrere Kanäle. Doch der Angelpunkt bei diesem Ansatz ist ein individuelles Telefongespräch.

Naturgemäß erfordern diese Angriffe die aktive Mitwirkung des Opfers. Angriffe per Telefon beginnen mit einer E-Mail, die vorgibt, von einer legitimen Quelle zu stammen, und eine Telefonnummer zur Kundenberatung nennt. Anrufer bei dieser Nummer landen bei Fake-Kundendienstmitarbeitern, die das Opfer durch den Angriff führen. Sie leiten das Opfer zum Beispiel an, Fernzugriff auf ihren Computer zu gewähren, oder fordern sie zum Herunterladen einer Datei auf, die sich als Malware herausstellt.

Worin sollten Sie Ihre Anwender schulen?

Schließen Sie Ihre Schulung zu Social Engineering mit Hinweisen ab, die Ihre Anwender direkt in Aktionen umwandeln können. Zu den Empfehlungen können zum Beispiel gehören:

- Vertrauen Sie niemals blind Personen, die Sie per E-Mail, Telefon oder Social Media kontaktieren.
- Halten Sie inne und überlegen Sie zweimal, bevor Sie aktiv werden, z. B. einer Aufforderung zur Geldüberweisung folgen oder Gutscheinkarten kaufen, ohne vorher zu prüfen, ob der Absender (und die Anfrage selbst) echt ist.
- Geben Sie in Social-Media-Beiträgen niemals personenbezogene Informationen weiter, z. B. Telefonnummern oder Postanschriften.
- Seien Sie vorsichtig beim Klicken auf Links und Öffnen von Anhängen und geben Sie niemals Ihre Anmeldedaten weiter.
- Gesunder Menschenverstand kann enorm helfen, Social-Engineering-Angriffe zu vermeiden. Wenn etwas zu gut klingt, um wahr zu sein, ist es wahrscheinlich ein Betrugsversuch. Und wenn etwas verdächtigt aussieht oder klingt, ist wahrscheinlich etwas nicht in Ordnung.

ABSCHNITT 2

Phishing

Phishing gibt es schon seit Jahrzehnten und ist nach wie vor eine der größten und am schnellsten wachsenden Cyberbedrohungen.

Bereits vor der COVID-19-Pandemie war Phishing eine kaum zu bändigende Herausforderung. Seitdem hat sich die Situation weiter verschärft. Laut dem aktuellen jährlichen Internet Crime Report (Bericht zu Internetkriminalität) des vom FBI geführten Internet Crime Complaint Center (IC3) sind die Verluste durch Internetbetrug, der typischerweise eine Phishing-Komponente hat, im Jahr 2022 um 50 % auf 10,3 Milliarden US-Dollar gestiegen. Und das sind nur die gemeldeten Phishing-Angriffe. Die Dunkelziffer dürfte deutlich höher liegen.

Offensichtlich sind Cyberangreifer erfolgreicher denn je, wenn es um das Ausnutzen menschlicher Schwächen geht. Aus dem Proofpoint-Untersuchungsbericht State of the Phish 2023 geht hervor, dass nur 58 % der berufstätigen Erwachsenen wissen, was Phishing ist.

Unsere Botschaft an Unternehmen: Machen Sie Phishing zum Schwerpunkt Ihrer Security-Awareness-Programme. Wenn möglicherweise nur etwa die Hälfte Ihrer Anwender weiß, was Phishing ist, sollten Sie Schulungen zu diesem extrem wichtigen Cybersicherheitsthema mit einer Erläuterung dieses Begriffs einleiten.

Was ist Phishing?

Phishing ist eine Social-Engineering-Taktik, bei der Angreifer mit einer Kombination diverser Techniken wie Fälschung, Irreführung und Lüge versuchen, die menschliche Psyche zu manipulieren.

Phishing-E-Mails nutzen Social Engineering, um Anwender zu schnellen, unbedachten Handlungen zu verleiten. Waren die Angreifer mit ihren Phishing-E-Mails erfolgreich, lässt die „Belohnung" – in Form von Zugriff auf vertrauliche Daten, kritische Systeme und Netzwerke, Cloud-Konten und oft auch Geld – nicht lange auf sich warten.

Die meisten Phishing-Nachrichten werden per E-Mail an die Opfer verschickt. Einige Angreifer sind zu anderen Methoden übergegangen, darunter Smishing und Vishing (dabei werden Textnachrichten und Stimmverzerrer verwendet, um SMS-Nachrichten an Anwender zu senden oder sie über Robocalls anzurufen).

Die drei häufigsten Strategien bei Phishing-Nachrichten

Nachdem Sie Ihre Anwender darüber informiert haben, worum es bei Phishing geht, zeigen Sie einige typische Strategien auf, die Angreifer anwenden, um die Empfänger der Phishing-E-Mails zu kompromittieren.

Schädliche Links

Angreifer nutzen oft schädliche URLs in ihren Phishing-Nachrichten. Wenn Anwender auf einen schädlichen Link klicken, gelangen sie zu einer gefälschten oder mit Malware (schädlicher Software) infizierten Website. Oft werden diese Links in den Phishing-Nachrichten so gut getarnt, dass sie von denen aus vertrauenswürdigen Quellen kaum zu unterscheiden sind. Dazu verwenden sie Firmenlogos oder registrieren E-Mail-Domains, die denen renommierter Marken oder Firmen zum Verwechseln ähnlich sind.

Allzu oft hat der Angreifer damit Erfolg. Bei den Untersuchungen zu unserem Bericht State of the Phish 2023 haben wir im Rahmen von Phishing-Simulationen festgestellt, dass 10 % der Anwender auf schädliche Links klicken.

Infizierte Anhänge

Mit Malware infizierte Anhänge können Computer und Dateien kompromittieren. Oft sehen sie wie legitime Dateianhänge aus. Bei Phishing-Simulationen, die wir für Kunden durchgeführt haben, haben 16 % der Anwender E-Mail-Anhänge geöffnet.

Es ist wichtig, dass Sie Ihren Anwendern die Gefahr vor Augen führen, die von Phishing ausgeht. Malware-Infektionen und Ransomware, die über einen Phishing-Angriff eingeschleust werden, können sich ungehindert auf alle vernetzten Geräte ausbreiten – auch auf Cloud-Systeme.

Betrügerische Anfragen

Mit diesen Anfragen sollen die Empfänger dazu verleitet werden, vertrauliche Informationen wie Anmeldedaten, Kreditkartennummern usw. preiszugeben. Oft kommt dabei ein Formular zum Einsatz (z. B. von einer vermeintlichen Steuerbehörde, die eine Erstattung in Aussicht stellt) und der Anwender wird aufgefordert, vertrauliche Angaben zu machen.

Sobald der Anwender das Formular ausgefüllt und übermittelt hat, können Bedrohungsakteure die Daten zu ihrem persönlichen Vorteil nutzen.

Alle Phishing-Angriffe nutzen Social Engineering

Wie bereits erwähnt: Phishing-Angriffe sind eine Form von Social Engineering. Weisen Sie daher in Ihren Security-Awareness-Schulungen auf einige der Methoden hin, mit denen Angreifer Ihre Opfer mit psychologischen Tricks manipulieren:

- Der Angreifer gibt vor, jemand zu sein, den der Anwender kennt und dem er vertraut.
- Der Angreifer nutzt Emotionen wie Angst aus (und sei es nur die Angst, etwas zu verpassen), um Anwender zu schnellem Handeln zu motivieren.
- Der Angreifer macht interessante (und teils absurde) Versprechungen.

Böswillige Akteure starten ihre Angriffe oft dann, wenn ihre Opfer vermutlich nicht besonders wachsam sind. Viele Angreifer erkundigen sich sogar über den Fakturierungszyklus oder den Zeitpunkt wichtiger Besprechungen im Unternehmen, bevor sie ihren Phishing-Angriff starten.

Auswirkungen von Phishing auf die Unternehmensbilanz

Im Rahmen Ihres Sensibilisierungsprogramms für Endnutzer sollten Sie auch auf einige prägnante Vorfälle eingehen, um herauszustellen, wie kostspielig Phishing-Angriffe für Unternehmen sein können. Solche Argumente sind besonders für leitende Führungskräfte überzeugend, zumal sie aufgrund ihres Zugangs zu Daten und ihrer Autorität beliebte Zielpersonen sind bzw. ihre Identität von Angreifern besonders oft in Phishing-Kampagnen nachgeahmt wird.

Nachfolgend einige reale Beispiele:

- In einem Vergleichsvorschlag im Zusammenhang mit einer massiven Datenschutzverletzung im Jahr 2021 erklärte sich ein Mobilfunkunternehmen in den USA bereit, Kunden, deren Daten mutmaßlich offen gelegt worden waren, eine Entschädigung von insgesamt 350 Millionen US-Dollar zu gewähren. Von dem Vorfall waren mehr als 76 Millionen Kunden betroffen.[2]

- Eine Führungskraft des Sportmode-Giganten Nike verlor geschätzte 173.000 US-Dollar in Form digitaler Token, nachdem er im Januar 2023 Opfer eines nach eigenen Angaben „cleveren" Phishing-Angriffs geworden war. „Ich bin natürlich sehr verärgert und verletzt", schrieb die Führungskraft in einem Tweet. „Ich war einen ganzen Tag lang wie gelähmt."[3]

- Mit einem Phishing-Angriff wurde ein Mailchimp-Mitarbeiter dazu verleitet, seine Anmeldedaten herauszugeben. Dadurch konnten Cyberkriminelle die Kontodaten von fast 320 Kunden und mehr als 100 Marketing-E-Mail-Listen stehlen. Erschwerend kommt hinzu, dass die Angreifer anschließend weitere Phishing-Angriffe starteten und sich dabei selbst als Mailchimp-Mitarbeiter ausgaben.[4]

- Zwei führende US-Technologieunternehmen – eine Social-Media-Plattform und eine Internetsuchmaschine – haben bei einem raffinierten Phishing-Angriff mehr als 100 Millionen US-Dollar verloren. Die Angreifer gingen sogar so weit, dass sie ein falsches Unternehmen gründeten und gefälschte E-Mail-Adressen und Rechnungen verwendeten.[5]

Worin sollten Sie Ihre Anwender schulen?

Damit Ihre Sensibilisierungsschulungen für Cybersicherheit bei den Anwendern Früchte tragen, müssen die Anwender verstehen, dass sich Phishing-Muster auch auf ihren eigenen Geldbeutel auswirken können. Sensibilisieren Sie Ihre Anwender für folgende Phishing-Taktiken:

- Online-Shopping (z. B. „Klicken Sie hier und erhalten Sie 60 % Rabatt! Zusätzlich nehmen Sie an der Verlosung für einen Einkaufsgutschein in Höhe von 1.000 $ für unseren Online-Shop teil.")

- Hilfsorganisationen (z. B. „Urlaub für die einen, Hunger für die anderen. Die Zeit drängt. Unterstützen Sie uns jetzt mit einer Spende. Nutzen Sie dazu das beigefügte Formular.")

- Versandunternehmen (z. B. „Wir konnten Ihre Sendung leider nicht zustellen. Bitte prüfen Sie die beigefügten Versandinformationen, um Ihre Bestelldaten zu bestätigen.")

Weisen Sie Ihre Anwender auch auf Streaming-Betrüger hin. Die Angreifer treten dabei als Anbieter beliebter Streaming-Dienste auf und bieten Sonderkonditionen an (z. B. „Einen Monat lang kostenlos streamen") oder sie versuchen, Anwender zur Anmeldung bei ihrem Konto zu verleiten (z. B. „Aktualisieren Sie Ihre Daten, um Ihr Abonnement zu reaktivieren").

2 Jonathan Stempel und Sara Merken (Reuters): „T-Mobile to pay $350 mln in settlement over massive hacking" (T-Mobile muss nach massivem Hacker-Angriff 350 Mio. USD Entschädigung zahlen)", Juli 2022.

3 Matthew Kish (Insider): „A Nike exec says a phisher stole his NFTs. Here are 3 things everyone should do to protect a digital wallet" (Nike-Führungskraft hat durch Phisher NFTs verloren. Mit diesen drei Schritten schützen Sie Ihre digitale Geldbörse), Januar 2023.

4 Ryan McCurdy (Security Boulevard): „The Biggest Phishing Breaches of 2022 and How to Avoid them for 2023" (Die größten Phishing-Angriffe von 2022 und wie Sie sie 2023 vermeiden können), November 2022.

5 Vanessa Romo (NPR): „Man Pleads Guilty to Phishing Scheme That Fleeced Facebook, Google of $100 Million" (Mann bekennt sich des Phishing-Angriffs schuldig, der Facebook, Google um 100 Mio. USD schröpfte), März 2019.

Einfache Tipps für erfolgreiche Sicherheit

Schließen Sie Ihre Sensibilisierungsschulung für Cybersicherheit zum Thema Phishing mit einigen Tipps, die sich einfach umsetzen lassen und verhindern, dass Ihre Anwender in die Phishing-Falle tappen. Mit diesen Verhaltensweisen reagieren Ihre Anwender sensibler auf Angriffe:

- Vertrauen Sie keinem Absender spontan, auch wenn die Nachricht von einer vertrauenswürdigen Quelle oder Firma zu sein scheint.
- Überprüfen Sie die Absenderadresse und alle Links, die scheinbar vom Versandunternehmen kommen (z. B. „Wir konnten Ihre Sendung leider nicht zustellen. Bitte prüfen Sie die beigefügten Versandinformationen, um Ihre Bestelldaten zu bestätigen.“)
- Öffnen Sie dazu eine neue Browser-Registerkarte oder ein neues Fenster und geben Sie manuell die Domain ein, auf die der jeweilige Link anscheinend verweist.
- Klicken Sie nicht auf Schaltflächen oder Links, die zu einer Handlung auffordern, wie „Konto überprüfen“ oder „Jetzt anmelden“.
- Gehen Sie nicht davon aus, dass Links für Dateifreigaben grundsätzlich sicher sind.

Fordern Sie Ihre Anwender auf, verdächtige Nachrichten zu melden. Das Melden verdächtiger E-Mails sollte ein wichtiger Bestandteil Ihrer Cyberschutzstrategie sein. Mit Tools wie die PhishAlarm-Phishing-Schaltfläche von Proofpoint werden Ihre Anwender zu wachsamen und proaktiven Verteidigern.

ABSCHNITT 3

Business Email Compromise

Ein Buchhalter überweist Geld an das Bauunternehmen, das die Büroräume renoviert hat. Ein Lohnbuchhalter aktualisiert die Kontodaten für eine frisch verheiratete Mitarbeiterin. Dies sind typische Szenarien und Routine-Aufgaben in Unternehmen.

Die entsprechenden Mitarbeiter sind gleichzeitig die Ziele für einige der heimtückischsten Cyberbedrohungen, die als Business Email Compromise (BEC) bezeichnet werden. BEC-Angriffe tarnen sich als alltägliche geschäftliche E-Mails und nutzen die Vertrautheit und das Vertrauen, um Geld und Informationen an Kriminelle umzuleiten.

BEC-Angriffe setzen ganz auf Social-Engineering-Taktiken und auf den Faktor Mensch. Ihre Anwender müssen verstehen, was BEC ist, wie sie solche Angriffe erkennen und wie sie sie stoppen können.

Was ist Business Email Compromise?

Business Email Compromise ist eine Form von E-Mail-Betrug, bei der Kriminelle eine Person nachahmen, der die Empfänger vertrauen können. Dazu verwenden die Kriminellen gefälschte, kompromittierte oder Doppelgänger-E-Mail-Konten. Sie senden gezielte E-Mails an Mitarbeiter, Geschäftspartner oder Kunden. Die Empfänger halten die E-Mail für legitim und führen Aktionen durch, durch die vertrauliche Informationen oder Gelder direkt in die Hände der Kriminellen gelangen.

Auswirkungen von BEC-Angriffen

BEC-Angriffe verursachen erheblichen Schaden. Laut einem FBI-Bericht von 2022 betrugen die bereinigten Verluste durch BEC im Jahr 2021 insgesamt 2,4 Milliarden US-Dollar. Das ist 49 Mal mehr als die Verluste durch Ransomware und entspricht 35 % aller in diesem Jahr gemeldeten Verluste. Eine einzige umgeleitete Überweisung kann ganz schnell dazu führen, dass Ihr Unternehmen riesige Geldbeträge verliert.

2,4 Mrd. $

Bereinigte Verluste durch BEC-Angriffe

x49

Faktor im Vergleich zu Verlusten durch Ransomware

Anteil der Verluste durch BEC-Angriffe bezogen auf alle im Jahr 2021 gemeldeten Verluste

Häufig verwendete Taktiken

Dies sind die vier wichtigsten Taktiken, mit denen die Bedrohungsakteure bei BEC-Angriffen vertrauenswürdige Personen nachahmen:

- **Domain-Spoofing:** Angreifer nutzen Lücken in Ihrem E-Mail-Authentifizierungssystem (oder das gänzliche Fehlen eines solchen Systems) aus, um E-Mails zu versenden, die scheinbar von einer vertrauenswürdigen Domain stammen.
- **Display Name-Spoofing:** Angreifer verändern den Namen des Absenders, sodass die E-Mail scheinbar von einer Person stammt, die der Empfänger kennt. Das kann eine Autoritätsperson oder auch eine beliebige (interne oder externe) Person sein, der das Opfer vertraut.
- **Doppelgänger-Domain:** Angreifer registrieren Domains, die Ihrer Firmen-Domain zum Verwechseln ähnlich sind, und ahmen Ihre Marke oder eine vertrauenswürdige Person nach. Beispiel: ihrefinnendomain.com anstelle von ihrefirmendomain.com.
- **Kompromittiertes Konto:** Angreifer verwenden verschiedene Taktiken wie Social Engineering und Phishing, um Zugang zu den E-Mail-Anmeldedaten eines Anwenders zu erlangen. Anschließend missbrauchen sie dieses kompromittierte Konto, um BEC-Angriffe durchzuführen. Alternativ nutzen sie ein kompromittiertes Konto eines vertrauenswürdigen Anbieters, um Kunden und Geschäftspartner zu täuschen. Bei dieser Variante, bei der die Lieferkette (oder Supply Chain) zu einem neuen Bedrohungsvektor wird, imitieren die Angreifer oft den Lieferanten und kompromittieren gleichzeitig seine Konten.

Häufig verwendete Themen

Verschiedene Themen werden bei BEC-Nachrichten immer wieder beobachtet. Sie alle fordern Anwender dazu auf, eine Aufgabe auszuführen oder Informationen zur Verfügung zu stellen.

- **Köder und Aufgaben:** Angreifer nutzen einfach scheinbar harmlose Fragen oder Aufforderungen, um potenzielle Opfer zu identifizieren, zu verifizieren oder vorzubereiten. Damit versuchen sie, an weitere Informationen zu gelangen, die E-Mail-Adresse zu bestätigen oder festzustellen, ob das Ziel ein leichtes Opfer darstellt.
- **Umleitung von Gehaltszahlungen:** Angreifer senden eine E-Mail an die Personal- oder Gehaltsabteilung und geben sich als Mitarbeiter aus, dessen Bankverbindungsdaten aktualisiert werden müssen. Durch die Änderung wird das Gehalt jedoch auf das Bankkonto des kriminellen Akteurs überwiesen.
- **Rechnungsbetrug:** Ein Angreifer imitiert oder kompromittiert eine interne Quelle oder einen Lieferanten und bittet darum, Zahlungen auf ein neues Konto zu überweisen.
- **Erpressung:** E-Mail-Betrug mit Erpressung funktioniert genauso wie andere Formen der Erpressung. Die Angreifer drohen den Opfern damit, Eigentum zu zerstören, Gewalttaten zu verüben oder vertrauliche, peinliche oder kompromittierende Informationen zu veröffentlichen, um sie dazu zu bringen, den Angreifern Geld (in der Regel Kryptowährung) zu zahlen oder andere Wertsachen zu überlassen.
- **Betrug mit Gutscheinkarten:** Beim Betrug mit Gutscheinkarten erbeuten Bedrohungsakteure Geld in Form von Gutscheinkarten. Die Opfer werden dazu gebracht, die Karten zu kaufen und den Angreifern die Nummern und PINs zu schicken. Diese lösen die Karten ein oder verkaufen sie weiter.
- **Provisionsbetrug:** Provisionsbetrug ist eine alte Methode und wird in einigen Fällen – irreführenderweise – als „419“, „Nigerian 419“ oder „Nigerianischer Prinz“ bezeichnet. Der Bedrohungsakteur bittet das potenzielle Opfer um einen kleinen Geldbetrag als Vorschuss für einen späteren großen Gewinn. Die angefragte Geldsumme wird in der Regel als Startkapital dargestellt, das dazu dient, die versprochene Belohnung freizuschalten oder zu überweisen.

Meet-and-Cheat: BEC im Zeitalter von Zoom

Mit der Zunahme der Remote-Arbeit hat bei BEC-Angriffen auch das Thema virtuelle Meetings an Bedeutung gewonnen. Die Angreifer nutzen diese Technologie auf verschiedene Weise, z. B.:

- Versand von Meeting-Einladungen und Verweis auf „Tonprobleme“ zu Beginn des Meetings, anschließend Verwendung der integrierten Chat-Funktionen oder von Follow-up-E-Mails, um zur Überweisung von Geld oder Übermittlung von Informationen aufzufordern
- Verwendung von „Deep-Fake“-Audio oder -Video, um eine Person nachzuahmen, der das Opfer vertraut
- Nachahmung von hochrangigen Führungskräften, die „in einem Meeting festsitzen“ und ihre Mitarbeiter auffordern, finanzbezogene Aufgaben durchzuführen
- Verwendung eines kompromittierten Mitarbeiter-E-Mail-Kontos, um Zugriff auf vertrauliche Informationen zu erlangen, Terminpläne abzurufen und sich in laufende E-Mail-Unterhaltungen einzuklinken

Unabhängig von der eingesetzten Methode müssen Anwender in der Lage sein, BEC-Versuche zu erkennen, die Remote- und Hybrid-Arbeit ausnutzen.

Worin sollten Sie Ihre Anwender schulen?

BEC-Angriffe sind äußerst unauffällig, weil sie alltäglichen geschäftlichen E-Mails so ähnlich sehen. Sie enthalten nicht immer URLs und Anhänge, sodass sie von klassischen Sicherheitstools kaum erkannt werden können. Ihre Anwender können jedoch dafür sensibilisiert werden, ungewöhnliche Details zu erkennen und Anfragen zu verifizieren, z. B. indem sie den Absender persönlich über einen anderen Kommunikationskanal wie das Telefon kontaktieren.

- **Rechtschreibfehler:** Rechtschreibfehler sind noch kein Beweis, sollten jedoch ein Anlass sein, sich die E-Mail genauer anzusehen und sich zu vergewissern, dass die Anfrage echt ist.
- **Plötzliche Änderungen der Vorgehensweise:** E-Mails, die darum bitten, plötzlich von der etablierten Vorgehensweise abzuweichen, sollten immer mit Argwohn behandelt werden. Das gilt besonders dann, wenn Finanzen oder vertrauliche Firmendaten involviert sind.
- **Anfragen zu Bankverbindungen oder Finanzen:** Mitarbeiter sollten die Aufforderung, die Bankverbindung für Rechnungen oder Gehaltszahlungen zu ändern, immer überprüfen.
- **Dringlichkeit:** Wenn eine E-Mail ein Gefühl der Dringlichkeit schafft, sollten bei Ihren Mitarbeitern ebenfalls die Alarmglocken schrillen. Angreifer nutzen diese Taktik, um beim Empfänger eine emotionale Reaktion auszulösen.
- **Abweichungen beim Anzeigenamen:** Überprüfen Sie, ob es sich bei der Absenderadresse um eine Doppelgänger-Domain handelt. Beim Beantworten einer E-Mail sollten Anwender immer prüfen, ob die Antwortadresse mit der Absenderadresse übereinstimmt.

Ihre Mitarbeiter können Ihrem Unternehmen auf verschiedene Weise dabei helfen, BEC-Angriffe abzuwehren. Vermitteln Sie diese empfohlenen Vorgehensweisen:

- Seien Sie vorsichtig, wenn Sie personenbezogene oder persönliche Informationen online posten. Angreifer führen häufig Recherchen zu ihren Opfern durch, um ihre Nachahmungen noch überzeugender wirken zu lassen.
- Vertrauen Sie grundsätzlich keinem Absender, sondern achten Sie immer auf Hinweise für Nachahmungen.
- Kontaktieren Sie im Zweifelsfall das Sicherheitsteam.
- Verifizieren Sie Aufforderungen, Geld zu überweisen oder Informationen weiterzugeben, immer mit anderen Kommunikationsmethoden, um sicherzustellen, dass sie tatsächlich vom scheinbaren Absender gesendet wurden.

ABSCHNITT 4

Soziale Netzwerke

Vor weniger als 20 Jahren nutzten nur 5 % der US-Amerikaner soziale Netzwerke. Heute liegt die Zahl bei 72 %, denn Plattformen wie Facebook, Twitter, Instagram, TikTok und zahllose andere sind zu einem Teil des täglichen Lebens geworden.[6]

Gleichzeitig haben sich die sozialen Netzwerke auch zu einer Brutstätte für Kriminalität entwickelt. Nach Angaben der US-Bundeshandelskommission (FTC) wurden im Jahr 2021 mehr als 25 % der gemeldeten Betrugsfälle mithilfe von sozialen Netzwerken verübt. Dabei gibt es keine typischen Opfer: Es fallen nicht nur ältere Menschen auf Betrug in sozialen Netzwerken herein, sondern alle Altersgruppen. Genau genommen waren es laut FTC im Jahr 2021 Menschen zwischen 18 und 39 Jahren, die im Vergleich zu Menschen über 40 doppelt so häufig Opfer solcher Betrugsfälle wurden.[7]

6 Pew Research Center: „Social Media Use in 2021“ (Social-Media-Nutzung 2021), April 2021.

7 FTC: „Social media a gold mine for scammers in 2021“ (Social Media – die Goldmine für Betrüger 2021), Januar 2022.

Warum die sozialen Netzwerke?

Die Angreifer lieben die sozialen Netzwerke, da die meisten Menschen mindestens ein Social-Media-Konto haben. Die Netzwerke sind informell und Teil des täglichen Lebens, sodass viele Anwender dort weniger wachsam sind. Zudem nutzen sie die Netzwerke häufig auch dann, wenn sie müde oder abgelenkt sind, zum Beispiel abends nach der Arbeit oder beim Anstehen. All diese Faktoren machen soziale Netzwerke zu einem leichten Ziel für Angreifer.

Arten von Social-Media-Angriffen

Anwender müssen in sozialen Netzwerken mit vielen Arten von Bedrohungen rechnen. Angreifer nutzen verschiedene Methoden, um Anwender dazu zu bringen, personenbezogene oder persönliche Informationen, Anmeldedaten oder Geld herauszugeben.

Nachahmung

Die Angreifer ahmen Personen im Bekanntenkreis oder Vertreter einer Organisation (z. B. das Finanzamt oder Banken) nach, denen die Anwender vertrauen.

Beispielsweise könnten Ihre Mitarbeiter eine Nachricht erhalten, die von einem Freund zu stammen scheint. Der Freund behauptet, bestohlen worden zu sein und deshalb im Ausland festzustecken. Der Empfänger soll deshalb dringend Geld schicken, um die Rückreise zu ermöglichen.

Oder Ihre Mitarbeiter erhalten eine Nachricht von ihrer Bank, in der steht, dass man sie nicht erreichen konnte und dringender Handlungsbedarf besteht (z. B. dass sie auf einen Link klicken sollen, um sich bei einem Konto anzumelden oder ihre Adresse zu bestätigen).

Betrug im Gesundheitsbereich

Bei dieser Betrugsart werden Themen aus dem Gesundheitsbereich wie COVID-19 oder die Affenpocken missbraucht. Die Anwender werden dazu gebracht, auf einen Link zu klicken oder persönliche Informationen preiszugeben, um dafür beispielsweise Folgendes zu erhalten:

- Test-Kits, die nicht geliefert werden oder gefälscht sind
- Gefälschte COVID-19-Impfausweise
- Impfungen, Therapien und Medikamente, die oft gefälscht sind

Zudem bieten die Angreifer häufig Geld oder Geschenke als Dankeschön für die Teilnahme an „Umfragen“ zu Impfungen oder Therapien an. Diese Umfragen dienen jedoch nur dazu, persönliche Daten und medizinische bzw. finanzbezogene Informationen zu stehlen.

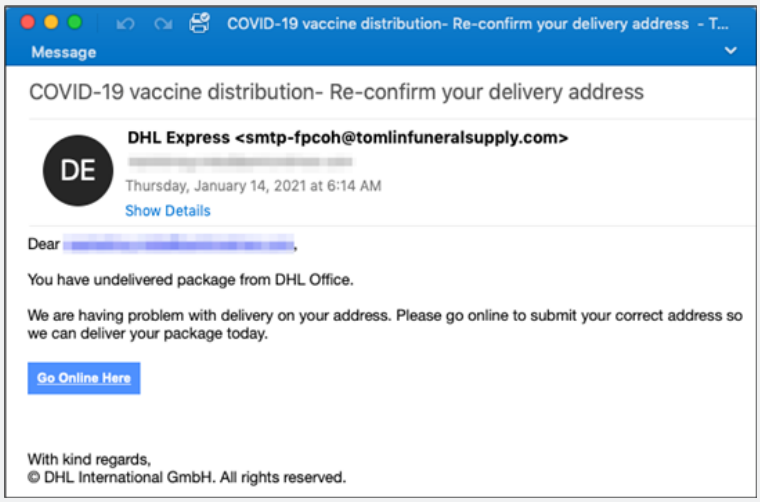


Abb. 1: Screenshot einer E-Mail über ein angeblich nicht zugestelltes DHL-Paket mit Impfstoffen.

Clickbait

Beim Clickbait-Betrug werden Anwender mit der Aussicht auf schockierende oder brisante Inhalte dazu verleitet, auf schädliche Links zu klicken. Oftmals erhalten Anwender eine Privatnachricht (die scheinbar von einer vertrauenswürdigen bekannten Person stammt), die suggeriert, dass der Absender ein anstößiges oder anderweitig kompromittierendes Foto oder Video des Empfängers gefunden hat.

Wenn die Anwender auf den Link klicken, um sich die Inhalte anzusehen, werden sie aufgefordert, die zur Anzeige erforderliche Software zu aktualisieren, woraufhin Malware installiert wird. Da die Betroffenen das Foto oder den Inhalt schnell entfernen wollen und sich dadurch möglicherweise peinlich berührt fühlen, prüfen sie nur selten, ob der verschickte Link auch sicher ist. Dies ist nur eine von vielen Methoden, mit denen Angreifer Emotionen ausnutzen.

Phishing

Social-Media-Phishing erfolgt hauptsächlich auf zwei Arten.

Bei der ersten Methode verschicken die Angreifer E-Mails, die von einer Social-Media-Plattform zu stammen scheinen. Darin steht, dass das Kontokennwort der Anwender kompromittiert wurde. Sie sollen dann auf einen Link klicken, um Zugriff auf ihr Konto zu erhalten. Der Link führt zu einer gefälschten Anmeldeseite, die die Anmeldedaten der Anwender erfasst. Diese Methode funktioniert, weil die Angreifer die Gefühle des Opfers ausnutzen und es unter Zeitdruck setzen, wodurch das Opfer das Gefühl bekommt, schnell handeln zu müssen, um sein Social-Media-Konto zurückzuerlangen.

Bei der zweiten Methode erhalten die Anwender eine Freundschaftsanfrage von scheinbar bekannten Personen. Diese Konten, die entweder kompromittiert oder gefälscht sind, posten Inhalte mit schädlichen URLs, die zu einer gefälschten Anmeldeseite führen. Mithilfe von Social Engineering versuchen die Angreifer hier, das grundlegende Bedürfnis von Menschen auszunutzen, Kontakte zu knüpfen und persönliche Beziehungen zu Mitmenschen aufzubauen. Das bringt die Anwender dazu, Freundschaftsanfragen schnell und ohne Überprüfung der Identität der betreffenden Person zu akzeptieren.

Romance Scams

Romance Scams sind eine Form des Nachahmungsbetrugs. Bei Romance Scams nehmen die Angreifer eine falsche Identität an, um eine romantische Beziehung zu Anwendern aufzubauen. Dies kann sich über einen längeren Zeitraum hinziehen. Wenn ein Vertrauensverhältnis aufgebaut wurde, bringen sie das Opfer meist dazu, ihnen Geld zu schicken.

Im September 2021 wurde ein ehemaliger Reservist der US-Armee zu 46 Monaten Haft verurteilt, weil er an einem Betrug beteiligt war, bei dem fast 70 Opfer im ganzen Land um mehr als 1,8 Millionen US-Dollar betrogen wurden. Die Täter gaukelten älteren Männern und Frauen romantische Beziehungen mit gefälschten Identitäten vor und nutzten ihre Gefühle aus, um an ihr Geld zu kommen.

Und wer hat nicht schon einmal von dem berüchtigten „Tinder Swindler“ (auch bekannt als Shimon Hayut oder Simon Leviev) gehört? Unter dem Deckmantel des Playboy-Sohns eines Diamantenmagnaten überhäufte Shimon Hayut Frauen mit Geschenken, Zuwendung und spontanen Urlauben – um sie anschließend um Geld zu bitten, um mysteriöse „Feinde“ abzuwehren.

Gewinnspiel- und Lotteriebetrug

Beim Gewinnspiel- und Lotteriebetrug werden Gewinne versprochen, um Anwender dazu zu verleiten, persönliche oder finanzielle Informationen herauszugeben.
Die Angreifer wissen, dass Menschen immer an Geldgewinnen interessiert sind, und versuchen daher, sich die Aufregung und Freude über einen unerwarteten Geldsegen zunutze zu machen.

Ratespiele und Umfragen

Ratespiele und Umfragen, die in Social-Media-Feeds auftauchen, mögen zunächst wie eine unterhaltsame und harmlose Beschäftigung erscheinen. Doch häufig nutzen Angreifer Quiz-Betrug, um persönliche Informationen von Anwendern zu erfassen, darunter auch Antworten auf gängige Sicherheitsfragen.

Betrug mit Remote-Arbeit und dem schnellen Geld

Diese Betrugsarten gehören zum Employment Fraud (Betrug mit Stellenanzeigen). Die Angreifer geben sich als Personalvermittler aus und ködern Anwender mit Anzeigen für hochbezahlte, einfache Arbeit, die von zu Hause aus erledigt werden kann. Diese Betrugsversuche mit Remote-Arbeit dienen jedoch nur als Deckmantel, um persönliche Informationen und Geld von denen zu stehlen, die darauf antworten.

So können diese Betrügereien Ihrem Unternehmen schaden

Obwohl die meisten Ihrer Mitarbeiter soziale Netzwerke wahrscheinlich nicht im Rahmen ihrer regulären Arbeit nutzen, können Social-Media-Angriffe Ihrem Unternehmen dennoch schaden. Werden Mitarbeitergeräte oder -konten durch diese Angriffe kompromittiert, können die Angreifer in Ihr Netzwerk gelangen und von dort aus Angriffe starten.

Durch die Arbeit im Homeoffice nutzen die Mitarbeiter heute ihre privaten Geräte sowohl für die Arbeit als auch das Privatleben. Daher kann ein Angriff dazu führen, dass vertrauliche Unternehmensdaten kompromittiert werden und dem Unternehmen erheblicher Schaden entsteht.

Worin sollten Sie Ihre Anwender schulen?

Mit den folgenden Tipps können Sie Ihren Mitarbeitern den sicheren Umgang mit sozialen Netzwerken vermitteln:

- Behandeln Sie Anfragen nach Geld und Anmeldedaten immer mit größten Misstrauen, selbst wenn sie scheinbar von jemandem stammen, den Sie kennen. Wenn eine Person Sie um Geld oder Anmeldedaten bittet, sollten Sie sie zur Sicherheit immer über einen anderen Kanal kontaktieren.
- Vorsicht bei Werbeaktionen, Stellenanzeigen und Popup-Nachrichten mit Versprechungen, die zu schön sind, um wahr zu sein.
- Geben Sie Ihren Benutzernamen oder Ihr Kennwort nur dann auf einer Website ein, wenn Sie die Website direkt angesteuert und die URL in Ihrem Browser überprüft haben.
- Löschen Sie alle Anfragen nach vertraulichen Daten und melden Sie sie Ihrem Sicherheitsteam, wenn Sie die Anfragen über ein Firmenkonto erhalten.
- Kontaktieren Sie den Support und Ansprechpartner für soziale Netzwerke nur über die Website oder App des sozialen Netzwerks.
- Vorsicht bei Nachrichten, in denen Sie dringend um Geld gebeten werden, auch wenn sie von Personen stammen, die Sie kennen. Nehmen Sie sich immer die Zeit, die Person, die die Anfrage stellt, außerhalb der sozialen Netzwerke zu kontaktieren.
- Wenn Sie glauben, dass Ihr Konto kompromittiert wurde, sollten Sie sich sofort anmelden und Ihren Benutzernamen oder Ihr Kennwort zurücksetzen. Melden Sie Probleme an die jeweilige Social-Media-Website.
- Öffnen Sie Social-Media-Websites nicht im selben Browserfenster wie die Website Ihrer Bank oder andere vertrauliche Websites, denn Angreifer könnten auf diese Weise wichtige Informationen abfangen.

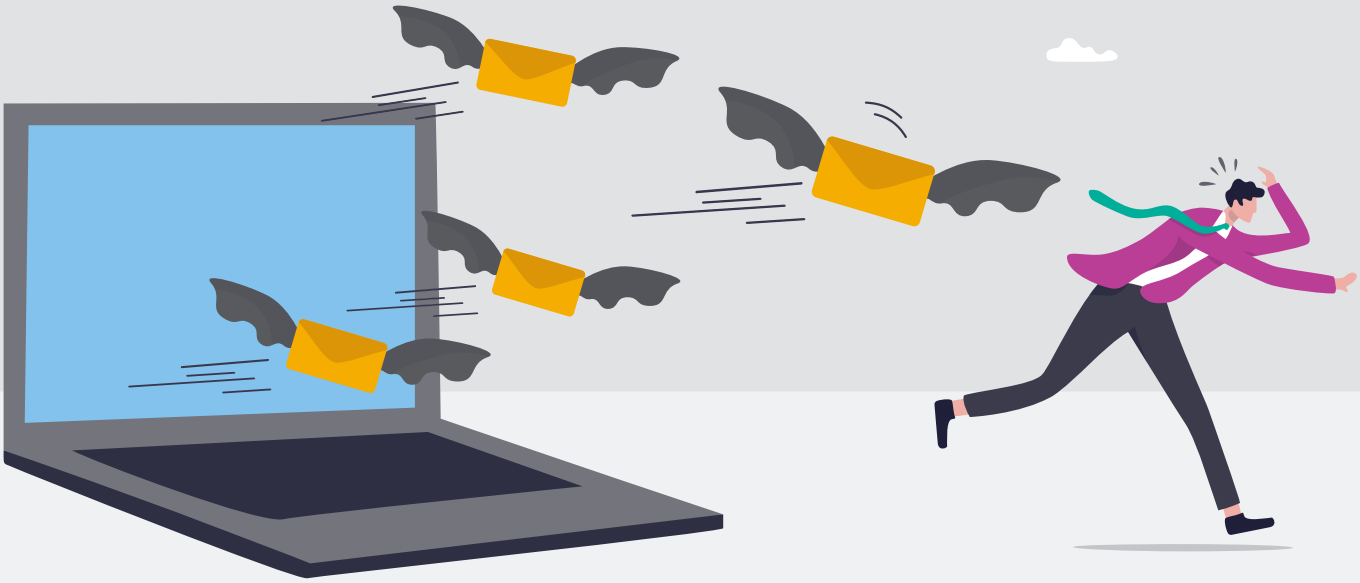
ABSCHNITT 5

Ransomware

Ransomware existiert seit mehr als drei Jahrzehnten, zählt aber nach wie vor zu den verheerendsten Arten von Cyberangriffen.

Diese Malware-Kategorie (die nach dem englischen Wort für „Lösegeld“ benannt wurde, das nach dem Sperren von Dateien verlangt wird) lässt sich bis zum Jahr 1989 zurückverfolgen, als ein Evolutionsbiologe das „AIDS-Virus“ über eine Diskette verbreitete, um Gelder von AIDS-Forschern in 90 Ländern zu erpressen. Die Opfer sollten das Geld, das der Angreifer als „Lizenzgebühren“ bezeichnete, an ein Postfach in Panama schicken. Nach Erhalt der Zahlung schickte er den Opfern per Post einen Entschlüsselungsschüssel. Der Angreifer profitierte kaum von dieser Aktion und wurde schließlich verhaftet.

Ransomware-Angriffe haben sich seitdem deutlich weiterentwickelt. Häufig handelt es sich dabei um raffinierte Kampagnen mit weitreichenden Folgen und Zahlungen in Millionenhöhe. Ransomware-Angriffe können auch verheerende Folgen haben, wenn sie kritische Infrastrukturen und Dienstleister wie das Gesundheitswesen, Strafverfolgungsbehörden und Energieversorger ins Visier nehmen – was immer häufiger der Fall ist. Dieser Bedrohungstyp wird zudem als Problem der nationalen Sicherheit betrachtet, da viele Angreifer mit staatlichen Akteuren verbunden sind oder von diesen finanziert werden. Deshalb werden die Opfer in den USA auch dazu aufgefordert, Ransomware-Zwischenfälle an die US-Regierung zu melden.



Ransomware-Angriffe sind in den letzten Jahren immer häufiger geworden. Das liegt wahrscheinlich daran, dass die Angreifer enormen Profit aus solchen Zwischenfällen schlagen können. Eine Untersuchung der Unit 42 von Palo Alto Networks zeigt, dass die durchschnittliche Lösegeldforderung im Jahr 2021 um 144 % auf 2,2 Millionen US-Dollar und das durchschnittlich gezahlte Lösegeld um 78 % auf 541.010 US-Dollar stieg.[8]

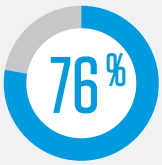
144 %

Anstieg an Lösegeldforderungen im Jahr 2021

541.010 $

Durchschnittliche Lösegeldzahlung

Zudem zeigen unsere eigenen Untersuchungen für den *State of the Phish-Bericht 2023* folgende Ergebnisse:



der Unternehmen haben 2022 Ransomware-Angriffe per E-Mail erlebt

der Unternehmen wurden mit Ransomware infiziert

der infizierten Unternehmen zahlten Lösegeld

Ein Drittel der erwachsenen Anwender kann Ransomware nicht erkennen

Ransomware ist eine kostspielige, schwerwiegende Cyberbedrohung, die Unternehmen im Rahmen ihrer Security-Awareness-Programme ansprechen müssen. Lösegeld zu zahlen ist zwar mitunter unvermeidlich, ermutigt die Angreifer jedoch nur in ihren Aktivitäten und trägt zur Finanzierung des nächsten Angriffs bei. Es ist besser, die Ransomware daran zu hindern, überhaupt in das System einzudringen. Das Potenzial, Anwender für die Risiken von Ransomware zu sensibilisieren, ist groß, denn 40 % der von Proofpoint befragten erwachsenen Anwender konnten Ransomware nicht korrekt identifizieren. (Die Ergebnisse dieser Bewertung finden Sie in unserem *State of the Phish-Bericht 2023*.)

Untersuchungen von Unit 42 zeigen, dass Ransomware zu mehr als 75 % über E-Mails und zu etwa 20 % über Webbrowser verbreitet wird. Häufig verwenden die Ransomware-Betreiber Social-Engineering-Taktiken und nutzen menschliches Verhalten aus, um Anwender zu kompromittieren und Angriffe zu starten. Ihre Anwender müssen verstehen, was Ransomware ist, wie sie sie erkennen und welche Maßnahmen sie gegen diese äußerst gefährlichen Angriffe ergreifen können.[9]

8 Ryan Olson (Palo Alto Networks): „Ransomware Trends: Higher Ransom Demands, More Extortion Tactics“ (Ransomware-Trends: Steigende Lösegeldforderungen, mehr Erpressungstaktiken), März 2022.

9 ebd.

Was ist Ransomware?

Ransomware dient im Wesentlichen der Erpressung. Sie ist eine Form von Schadsoftware (Malware), die den Zugriff auf Computersysteme oder Daten blockiert. Dies erfolgt meist durch Verschlüsselung, bis das Opfer ein Lösegeld an den Angreifer zahlt.

Zu Ransomware-Infektionen kommt es, wenn Anwender die Malware unwissentlich auf ihren Rechner herunterladen, indem sie einen E-Mail-Anhang öffnen, auf Werbung klicken, einem Link folgen oder einfach nur eine Website aufrufen, in die Malware eingebettet ist.

In der Regel verlangen die Angreifer eine Lösegeldzahlung in Kryptowährung (z. B. Bitcoin), da diese schwer zu verfolgen ist. In vielen Fällen läuft bei der Lösegeldforderung ein Countdown. Wenn das Opfer nicht rechtzeitig zahlt, sind die Daten für immer verloren, erhöht sich das Lösegeld oder die Angreifer veröffentlichen die Daten. Wenn es sich um besonders skrupellose Angreifer handelt, kann es vorkommen, dass das Opfer das Lösegeld bezahlt und die Daten dennoch verliert.

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 der beste Schutz vor Ransomware daher in der Vermeidung anderer Malware-Typen.

Worin sollten Sie Ihre Anwender schulen?

Ransomware ist eine personenzentrierte Bedrohung, d. h. die Anwender spielen eine wichtige Rolle, wenn es darum geht, sich und ihr Unternehmen vor diesen Cyberangriffen zu schützen. Die Angreifer entwickeln ihre Taktiken ständig weiter, sodass selbst technische Kontrollen und die Maßnahmen des IT-Sicherheitsteams nicht vollständig verhindern können, dass Malware-Bedrohungen die Anwender erreichen.

Um Ihre Anwender bei der Abwehr von Ransomware zu unterstützen, sollten Sie die folgenden wichtigen Verhaltensregeln zu diesem Thema in Ihr Security-Awareness-Programm integrieren:

Antworten und klicken Sie NICHT auf verdächtige E-Mails und laden Sie KEINE Anhänge von diesen E-Mails herunter.

Prüfen Sie sorgfältig, ob eine Nachricht verdächtig sein könnte. Stellen Sie sich folgende Fragen:

- Handelt es sich um eine normale Nachricht – und wenn nicht, kam sie unerwartet?
- Stammt die Nachricht von einer Person, die mir unbekannt ist oder mit der ich bisher nicht kommuniziert habe?
- Hat die Nachricht einen unerwarteten Inhalt?
- Versucht der Absender, Zeitdruck oder Angst zu erzeugen? (Beispiel: „Klicken Sie jetzt oder wir sperren Ihr Konto.“)
- Werde ich in der Nachricht aufgefordert, mein Konto zurückzusetzen oder meine Anmeldedaten einzugeben?
- Verlangt der Absender, dass ich vertrauliche Daten weitergebe?
- Werde ich aufgefordert, etwas zu tun? (Beispiel: „Könnten Sie mich bitte anrufen?“ oder „Würden Sie bitte diese Angaben aktualisieren?“)

Machen Sie sich bewusst, dass nicht alle schädlichen E-Mails auf den ersten Blick verdächtig sind.

Häufig verwenden die Angreifer bekannte Marken oder sie versuchen, ihre Nachrichten so aussehen zu lassen, als kämen sie von einer vertrauenswürdigen Person, beispielsweise Kollegen oder Vorgesetzte. Um Fehler zu vermeiden, sollten Sie Folgendes tun:

- Schicken Sie eine Nachricht an die Person oder rufen Sie sie an, um zu bestätigen, dass die Nachricht von ihr stammt.
- Rufen Sie die Website des Anbieters über eine Suchmaschine auf, um zu überprüfen, ob die Nachricht tatsächlich von diesem Anbieter stammt.

Rufen Sie verdächtige Websites NICHT auf und laden Sie verdächtige Anwendungen NICHT herunter.

Nachfolgend finden Sie drei Tipps zu diesen Handlungsempfehlungen, die Sie Anwendern geben können, die zum Thema Ransomware sensibilisiert werden:

- Wenn eine Website zu gut klingt, um wahr zu sein – wenn darauf zum Beispiel unbegrenzt kostenlose Musik, Filme und Anwendungen angeboten werden – ist sie wahrscheinlich unseriös und zudem möglicherweise schädlich.
- Beachten Sie, dass Anwendungen, auch wenn sie in beliebten App-Stores zu finden sind, dennoch schädlich sein können. Seien Sie vorsichtig und suchen Sie nach Apps von bekannten Anbietern mit einer hohen Zahl von Downloads.
- Plugins für Browser, E-Mail-Clients und andere Anwendungen können ebenso gefährlich sein wie schädliche Anwendungen. Erkundigen Sie sich bei Ihrer IT-Abteilung, bevor Sie Plugins herunterladen und nutzen.

Melden unbedingt Sie alles Verdächtige – auch wenn Sie einen Fehler gemacht haben!

Es ist immer besser, das IT- oder Sicherheitsteam zu informieren, wenn etwas schief gelaufen ist, zum Beispiel in folgenden Situationen:

- Sie haben eine verdächtige E-Mail erhalten, bei der es sich um eine Phishing-E-Mail handeln könnte.
- Sie haben eine E-Mail erhalten, die von einem Kollegen zu stammen scheint, die Ihnen jedoch verdächtig vorkommt oder unerwartet kam.
- Sie haben versehentlich auf einen Link geklickt, Ihre Anmeldedaten eingegeben oder einen Anhang heruntergeladen und festgestellt, dass dieser schädlich sein könnte.
- Sie haben eine Website besucht, die Ihnen vertrauenswürdig erschien, doch danach hatten Sie das Gefühl, dass etwas nicht stimmt.

ABSCHNITT 6

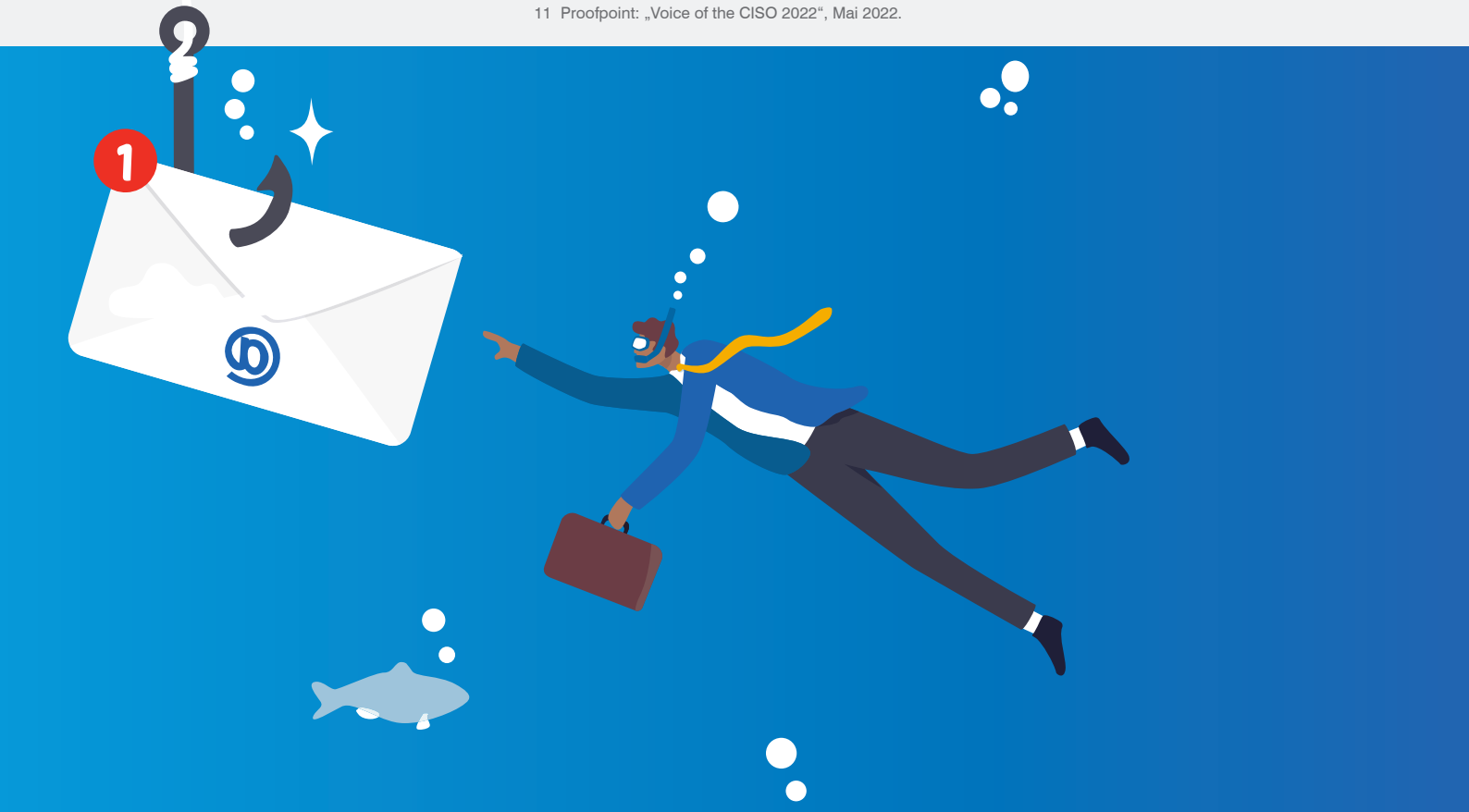
Risiken durch Insider

In den letzten Jahren hat sich die moderne Arbeitswelt massiv gewandelt. Remote- und Hybrid-Arbeit, der massenhafte Wechsel zur Cloud und eine zunehmende Mitarbeiterfluktuation haben den Schutz von Daten zu einer immer größeren Herausforderung gemacht. Es überrascht nicht, dass Insider-Bedrohungen im Jahr 2022 um 44 % gestiegen sind.[10]

Laut dem *Voice of the CISO-Bericht 2022* sind viele Cybersicherheitsverantwortliche davon überzeugt, dass Insider-Bedrohungen proaktiv angegangen werden müssen, denn letztlich ist kein Unternehmen vor Insider-Risiken gefeit. Tatsächlich gehören Insider-Bedrohungen für Chief Information Security Officers (CISOs) weltweit zu den größten Sicherheitsproblemen. Mehr als ein Drittel der befragten CISOs gab an, dass die Abwehr von Insider-Bedrohungen für ihre IT-Abteilung in den nächsten zwei Jahren oberste Priorität haben wird.[11]

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

11 Proofpoint: „Voice of the CISO 2022“, Mai 2022.



Was ist ein Insider-Risiko?

Insider sind Personen, die in irgendeiner Form beruflich mit einem Unternehmen verbunden sind. Aufgrund ihrer Rollen und Berechtigungen haben (oder hatten) sie autorisierten Zugang zu kritischen Daten und Systemen. Insider können aktuelle oder ehemalige Mitarbeiter, Auftragnehmer oder Geschäftspartner sein, die alle oder einige dieser Kriterien erfüllen:

- Sie haben Zugriff auf Rechner oder Netzwerke des Unternehmens.
- Sie entwickeln Produkte und Services für das Unternehmen.
- Sie kennen die langfristige Strategie des Unternehmens.
- Sie haben Zugang zu geschützten Informationen.

Kurz gesagt sind Insider Personen in einer Vertrauensstellung. Diese Anwender sind ohne Zweifel eine Bedrohung, wenn sie in böswilliger Absicht handeln und ihre Vertrauensstellung wissentlich zur persönlichen Bereicherung oder zum eigenen Vorteil nutzen. Weniger offensichtlich ist hingegen, dass Anwender, die ihre Zugriffsrechte versehentlich missbrauchen oder falsch handhaben, genauso viel Schaden anrichten können. Das Gleiche gilt für Anwender, deren Insider-Zugriffsrechte kompromittiert sind und von externen Angreifern missbraucht werden.

Die Begriffe „Insider-Risiken“ und „Insider-Bedrohungen“ werden zwar manchmal synonym verwendet, sie bedeuten jedoch nicht dasselbe. Insider-Bedrohungen sind ein Teilbereich der Insider-Risiken: Alle Insider stellen ein Risiko für ein Unternehmen dar, da sie Zugriff auf die Daten und Systeme dieses Unternehmens haben. Doch nicht jeder Insider wird zu einer Bedrohung. Diese Unterscheidung ist wichtig und erfordert einen strategischen und taktischen Ansatz, damit Sie Bedrohungen effektiv abwehren können.

Arten von Insider-Bedrohungen

Dies sind die drei wichtigsten Arten von Insider-Bedrohungen:

Fahrlässiges Verhalten

Fahrlässig handelnde Insider sind Anwender mit guten Absichten, die falsche Entscheidungen treffen und damit die Veröffentlichung oder den Diebstahl wertvoller Daten ermöglichen. Dazu zählen beispielsweise das Herunterladen von Dateien auf einen USB-Stick oder die versehentliche Weitergabe vertraulicher Daten (z. B. Kreditkarteninformationen von Kunden). Fahrlässige Anwender verursachen 56 % aller Insider-Vorfälle.[12]

Bedrohungen durch fahrlässige Anwender entstehen durch:

Menschliche Fehler: Das kann sowohl Server-Konfigurationsfehler als auch die Weitergabe von Dateien an mehr Personen als nötig umfassen.

Mangelhaftes Urteilsvermögen: Dazu gehören unter anderem bequeme Lösungen, die das Unternehmen gefährden, wie beispielsweise die Übertragung von Dateien auf einen USB-Speicher oder ein privates Konto eines Speicherdienstes.

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

Böswilliges Verhalten

Diese Insider sind vom persönlichen Vorteil motiviert und möchten dem Unternehmen schaden. Beispiele hierfür sind das Exfiltrieren von Finanzdaten oder Geschäftsgeheimnissen oder die Vernichtung vertraulicher Informationen. Untersuchungen des Ponemon Institute zu Insider-Bedrohungen zeigen, dass böswillige Insider mehr als ein Viertel (26 %) aller Insider-Zwischenfälle verursachen.[13]

Böswillige Anwender verursachen unter anderem folgende Bedrohungen:

Sabotage: Böswillige Insider versuchen, Unternehmenssysteme zu beschädigen oder Daten zu vernichten.

Betrug: Hierbei wollen die Insider Daten stehlen oder manipulieren, um Geschäftsabläufe zu stören oder sich einen finanziellen Vorteil zu verschaffen.

Diebstahl von geistigem Eigentum: Alle proprietären Informationen, die wertvoll für ein Unternehmen sind, können als geistiges Eigentum bezeichnet werden. Böswillige Insider stehlen geistiges Eigentum, um finanzielle Vorteile zu erzielen oder einem Unternehmen langfristigen (finanziellen oder anderweitigen) Schaden zuzufügen.

Spionage: Wenn böswillige Insider vertrauliche Geschäftsgeheimnisse, Dateien und Informationen eines Unternehmens stehlen und diese an Mitbewerber des Unternehmen oder auch staatliche Akteure verkaufen, betreiben sie Spionage.

Kompromittierung

Kompromittierte Anwender sind oft Very Attacked People™ (VAPs), also besonders häufig angegriffene Personen mit privilegiertem Zugriff auf Informationen. Sie besitzen Anmeldedaten und Zugriffsrechte, mit denen sich Bedrohungsakteure Zugang zu den kritischen Systemen und Daten eines Unternehmens verschaffen könnten. Die Angreifer nutzen Social-Engineering-Techniken wie Phishing, um an diese Anmeldedaten zu gelangen. In diesem Jahr wurden bei etwa 18 % aller Insider-Zwischenfälle gestohlene Anmeldedaten genutzt.[14]

Insider-Bedrohungen durch kompromittierte Anwender haben meist folgende Ursachen:

Gestohlene Anmeldedaten

Phishing

Malware

Unbeabsichtigte Beihilfe durch Social-Engineering-Angriffe

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

14 ebd.

Worin sollten Sie Ihre Anwender schulen?

Unternehmen sollten ihren Mitarbeitern dabei helfen, zu vermeiden, selbst Teil einer Insider-Bedrohung zu werden. Dazu müssen sie zunächst für fahrlässiges Verhalten und das Potenzial böswilliger Insider-Aktivitäten sensibilisiert werden. Sicherheitsbewusstsein kann Anwender mit böswilligen Absichten zwar nicht stoppen, doch es kann anderen helfen, verdächtiges Verhalten zu erkennen und zu melden.

Dies sind die zentralen Punkte, die Ihre Anwender im Hinblick auf dieses wichtige Thema beachten sollten:

Erst denken, dann handeln. Der bequemste Weg kann zwar mitunter Ihre Arbeit – oder die Ihrer Kollegen – erleichtern, aber auch Risiken bergen. (Beispiel: Geben Sie niemals Anmeldedaten weiter und nutzen Sie für die Datenweitergabe keine USB-Geräte.)

Bleiben Sie auf dem Laufenden. Informieren Sie sich über die Unternehmensrichtlinien für Daten und Systemzugriff bzw. -nutzung. (Beispiel: Verwenden Sie nur die Anwendungen und Tools, die vom Unternehmen bereitgestellt oder von der IT-Abteilung genehmigt wurden.)

Melden Sie dem Sicherheitsteam jedes verdächtige Verhalten. Wenn Sie bei Kollegen Verhalten beobachten, das Ihnen ungewöhnlich vorkommt (wenn z. B. nach Zugangsdaten gefragt wird, um auf eine Anwendung zuzugreifen, für die die Person nicht autorisiert ist), könnte es sich um böswillige oder kompromittierte Anwender handeln.

Weisen Sie Ihre Anwender zudem darauf hin, dass sie eine große Verantwortung für den Schutz der Daten Ihres Unternehmens tragen, und betonen Sie ihre Rolle beim Schutz des Unternehmens. Die Implementierung der oben beschriebenen einfachen Maßnahmen in den Alltag kann wesentlich dazu beitragen, Insider-Bedrohungen zu minimieren und einzudämmen.

ABSCHNITT 7

Schlussfolgerung und Empfehlungen

Mitarbeiter sind der neue Perimeter. Jeder kann zum Ziel werden oder die Sicherheit des Unternehmens durch einen Fehler oder eine böswillige Handlung beeinträchtigen. Die meisten Sicherheitsverantwortlichen sind sich dieser Tatsache bewusst. Sie wollen jedoch vor allem wissen, wie sie den Spieß umdrehen und die größte Angriffsfläche ihres Unternehmens zu einer wichtigen Verteidigungslinie machen können.

Kurz gesagt: Sie müssen das Verhalten Ihrer Mitarbeiter ändern, indem Sie eine umfassende und nachhaltige Sicherheitskultur aufbauen, die auf Ihr Unternehmen zugeschnitten ist.

Doch selbst kleine Änderungen können zu entscheidenden Verbesserungen führen, besonders was die Cybersicherheit angeht. Um das Sicherheitsbewusstsein der Anwender zu stärken und sie zu motivieren, sich aktiv gegen Cyberbedrohungen zu wehren, muss jedoch das Umfeld verändert werden – und das geschieht nicht über Nacht. Kleine Verhaltensänderungen, die mit der Zeit zu dauerhaften Angewohnheiten werden, können eine enorme Wirkung entfalten.

Weitere Informationen und Ressourcen zur Sensibilisierung für Sicherheit finden Sie im Proofpoint Informationsportal: Cybersicherheitsschulungen.

Vorteile von Proofpoint

Wir analysieren täglich mehr als:

2,6 Mrd. E-MAILS	**49 Mrd.** URLs	**1,9 Mrd.** ANHÄNGE
1,7 Mrd. MOBILGERÄTE-NACHRICHTEN	**430 Mio.** WEB-DOMAINS	**143.000** SOCIAL-MEDIA-KONTEN

Auf unsere Lösungen vertrauen mehr als:

- **75 %** DER FORTUNE 100
- **60 %** DER FORTUNE 1000
- **30 %** DER FORTUNE GLOBAL 2000

- **8.000** GROSSUNTERNEHMEN
- **200.000** KLEINE UNTERNEHMEN

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.

0504-007-04-01 04/23