E-BOOK

Den Spieß umdrehen

Wie die bevorzugten Ziele von Angreifern durch intelligente E-Mail-Meldungen und Behebungsmaßnahmen zu Ihrer besten Verteidigung werden

proofpoint.

Einführung

Die Corona-Pandemie hat zu einer verstärkten Migration zu Remote- und Hybrid-Arbeitsplätzen geführt. Doch schon vorher haben Cyberkriminelle anstelle von Infrastrukturen zunehmend Personen ins Visier genommen. Mehr als je zuvor zielen Angriffe heute darauf ab, nicht nur technische, sondern auch menschliche Schwachstellen auszunutzen. In den meisten Fällen geschieht dies durch E-Mails. Sie sind noch immer eine weit verbreitete Kommunikationsplattform – und bei ihrer Entwicklung spielte die Sicherheit zunächst überhaupt keine Rolle.

Laut dem *2021 Verizon Data Breach Investigations Report* ist an 85 % der Datenschutzverletzungen der „Faktor Mensch“[1] beteiligt. Dabei sind E-Mails der bevorzugte Ansatzpunkt für Social Engineering.[2]

15 Mio. $

Die **durch Phishing verursachten Kosten** haben sich für Unternehmen nahezu vervierfacht – auf fast 15 Millionen $ pro Jahr bzw. oder 1.500 $ pro Mitarbeiter.[3]

2X

Allein im Jahr 2020 hat sich die Anzahl der Phishing-Angriffe verdoppelt.[4]

75 %

Etwa drei Viertel der gesamten Ransomware gehen auf E-Mail-Phishing zurück, den wichtigsten Angriffsvektor für diese wachsende Bedrohung.[5]

1 Verizon: „Data Breach Investigations Report Executive Summary“ (Untersuchungsbericht zu Datenkompromittierungen: Kurzfassung), Mai 2021.
2 Verizon: „Data Breach Investigations Report“ (Untersuchungsbericht zu Datenkompromittierungen), Mai 2021.
3 Ponemon: „Studie zu Kosten durch Phishing 2021, August 2021.
4 APWG: „Phishing Activity Trends Report 4th Quarter 2020“ (Bericht zu Trends bei Phishing-Aktivitäten: 4. Quartal 2020), Februar 2021.
5 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.

E-Mails sind universell, für moderne Unternehmen unverzichtbar – und grundsätzlich unsicher! Das E-Mail-Kommunikationssystem wurde entwickelt, lange bevor das Internet zum Mainstream wurde. Dabei spielten Privatsphäre und Sicherheit zunächst überhaupt keine Rolle. In den 45 Jahren, die seitdem vergangen sind, haben sich E-Mails zu einer grundlegenden Säule der modernen Geschäftskommunikation entwickelt – und zu einem zentralen Punkt für alle Arten von Angriffen.

Jeden Tag gehen Milliarden von E-Mails in den Postfächern von Anwendern ein. Die meisten sind harmlos. Viele sind unerwünscht. Einige sind wichtig. Und viel zu viele sind gefährlich. Für einen vollständigen Schutz Ihres Unternehmens vor diesen Bedrohungen sind mehrere Schutzebenen erforderlich.

Die gute Nachricht: Sie können den Spieß umdrehen und die Taktiken der Angreifer gegen diese einsetzen. Wenn Sie E-Mail-Meldungen und Behebungsmaßnahmen in das Zentrum einer mehrschichtigen Verteidigung stellen, können Sie jedes potenzielle Opfer in einen schützenden Engpass verwandeln.

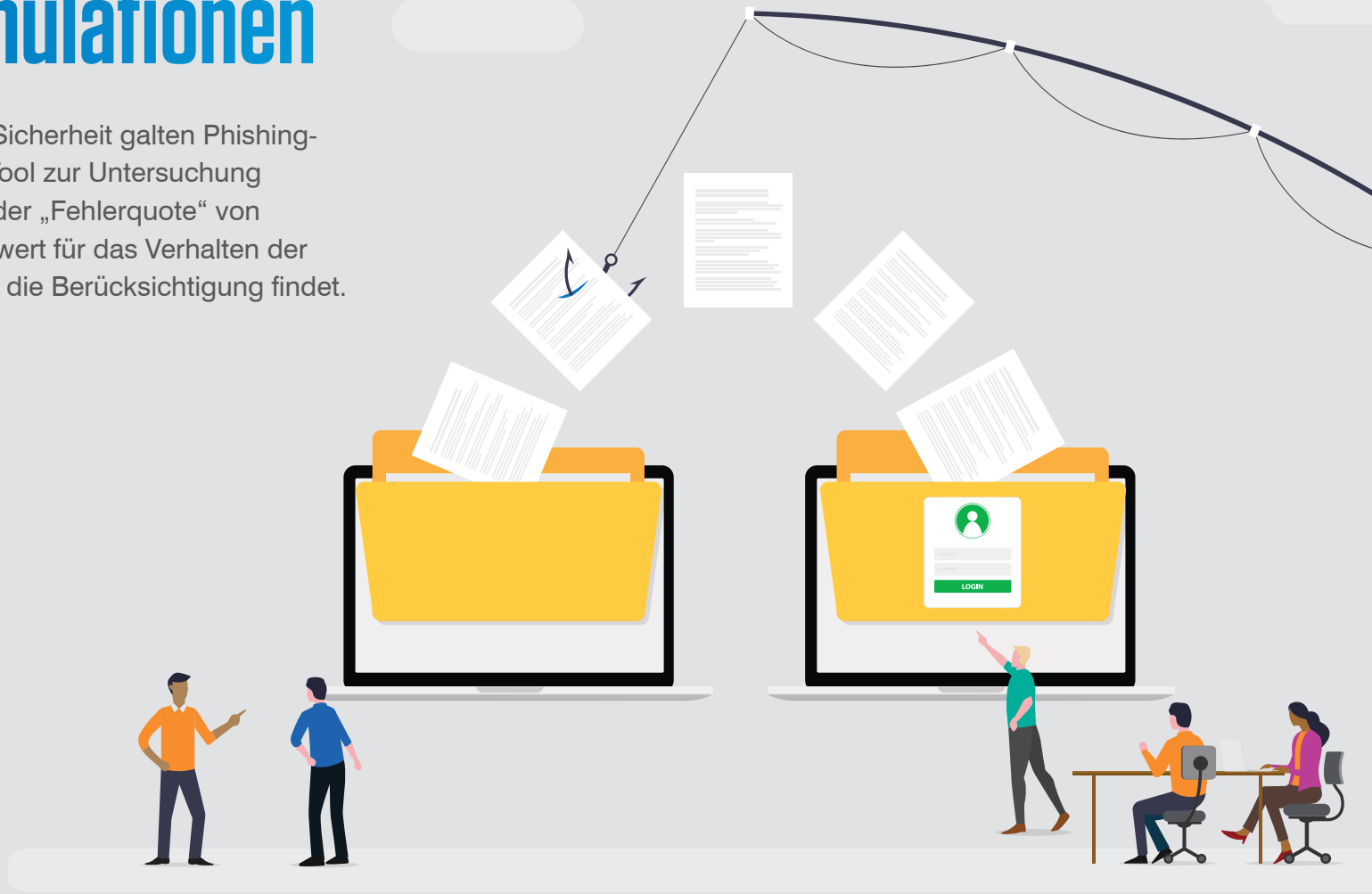
In diesem E-Book wird erläutert, wie Sie Anwender schulen, damit sie verdächtige E-Mails erkennen und melden – ohne dabei einen unnötigen Mehraufwand zu erzeugen, der die IT- und Sicherheitsteams dazu zwingt, blinden Alarmen auf den Grund zu gehen.

Das E-Book geht auch auf neue Untersuchungen zum Anwenderverhalten bei simulierten E-Mail-Bedrohungen ein. Zudem werden Möglichkeiten erörtert, wie mehr Anwender dazu gebracht werden, verdächtige E-Mails zu melden. Abschließend werden praktische Schritte genannt, mit denen Sie Ihre Reaktion auf gemeldete verdächtige E-Mails optimieren und den Anwendern dabei helfen können, wirkliche Bedrohungen besser zu erkennen.

ABSCHNITT 1

Anwender-Meldungsraten bei Phishing-Simulationen

Bei Programmen zur Sensibilisierung für Sicherheit galten Phishing-Simulationen schon immer als beliebtes Tool zur Untersuchung des Benutzerverhaltens. Die „Klickrate“ oder „Fehlerquote“ von Simulationen ist jedoch kein idealer Kennwert für das Verhalten der Anwender, wenn sie die einzige Metrik ist, die Berücksichtigung findet.



Vereinfachte E-Mail-Meldungen – für Anwender, IT- und Sicherheitsteams

Für Anwender ist es bequem, Phishing-E-Mails an ein Abuse-Postfach zu melden, das über eine E-Mail-Adresse wie phishing@IhrUnternehmen.net erreichbar ist. Abuse-Postfächer sind durchaus effektiv, erfordern jedoch häufig Rückfragen der IT-Abteilung bei den Anwendern, um wichtige Details wie E-Mail-Header zu erhalten.

Aus diesem Grund setzen sich zunehmend Add-ins oder Schaltflächen zur Meldung verdächtiger E-Mails durch. Dazu gehört auch Proofpoint PhishAlarm, das sich unkompliziert bedienen lässt und umfangreichere Funktionen als ein Abuse-Postfach bietet.

Die Fehlerquote wird als Worst-Case-Szenario für den jeweiligen Typ der simulierten Phishing-E-Mail definiert. Dabei geht es vereinfacht ausgedrückt um die Frage: Ist der Anwender auf den Köder hereingefallen und hat er als Reaktion auf den Link geklickt, den Anhang geöffnet oder Anmeldedaten bzw. personenbezogene Informationen eingegeben?

Sie können die Meldungsfunktion noch effektiver machen, indem Sie zusätzlich Kontext angeben, anhand dessen die Anwender schädliche E-Mails leichter erkennen können, und so für noch zuverlässigere Meldungen sorgen. Sie können Anwender zum Beispiel vor E-Mails warnen, in denen gängige Phishing-Techniken wie Spoofing und Doppelgänger-Domänen eingesetzt werden.

Suchen Sie bei der Bereitstellung eines solchen Meldungs-Tools nach Lösungen mit HTML-basierten Bannern, die kontextbezogen, anpassbar und mit möglichst geringem IT-Aufwand implementierbar sind.

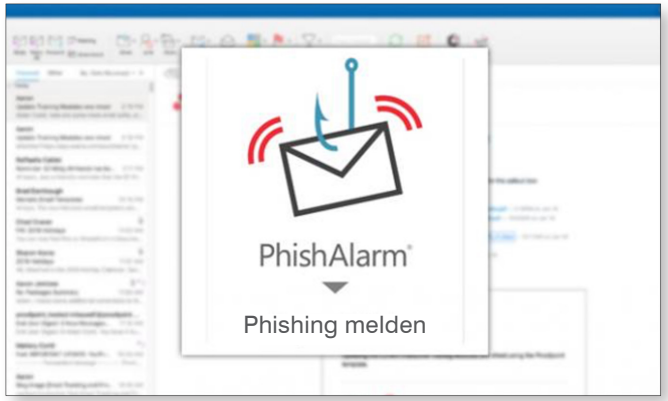


Abb. 1: Proofpoint PhishAlarm-Schaltfläche zur E-Mail-Meldung.

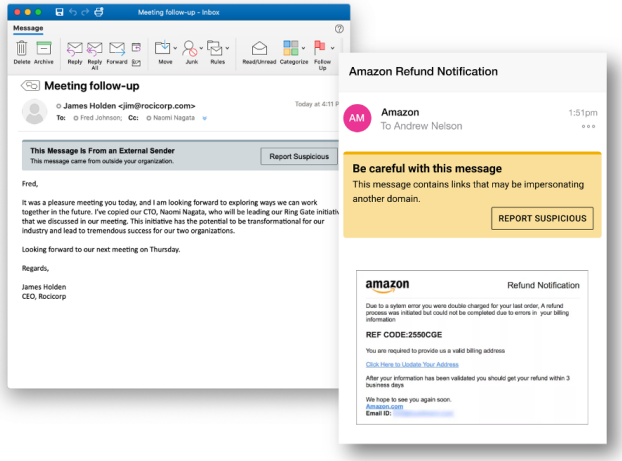


Abb. 2: Die E-Mail-Warnhinweise mit Meldungsoption von Proofpoint helfen Kunden bei der Verbesserung der Zuverlässigkeit von E-Mail-Meldungen und der E-Mail-Sicherheit.

Nicht immer ausreichend – die Fehlerquote

Doch die Fehlerquote allein ist nicht die beste Möglichkeit zur Auswertung des Anwenderverhaltens. Zunächst kann die Fehlerquote je nach Typ der simulierten Phishing-E-Mails stark variieren. In diesem Fall kann es schwierig sein, Muster oder Trends zu erkennen.

Weniger anspruchsvolle Vorlagen haben beispielsweise nur einstellige Fehlerquoten, während andere wie die Netflix-Vorlage in Abb. 3 in einigen Kampagnen auf bis zu 100 % kommen.

Vollständiger Überblick

Wenn es um die Einschätzung des Anwenderrisikos geht, haben Fehlerquoten nur eine begrenzte Aussagekraft. Einen umfassenderen Überblick erhalten Sie erst, wenn Sie auch die Meldungsrate von Phishing-Simulationen berücksichtigen.

Die Meldungsrate zeigt, dass Anwender nicht nur böswillige Nachrichten meiden, sondern auch richtig handeln und ihren Beitrag zur Absicherung des Unternehmens leisten. Je höher die Meldungsrate, desto größer ist die Wahrscheinlichkeit, dass Anwender wirklich verdächtige Nachrichten an Ihre IT- und Sicherheitsteams melden, sodass diese echte Bedrohungen besser beheben können, noch bevor ernsthafter Schaden entsteht.

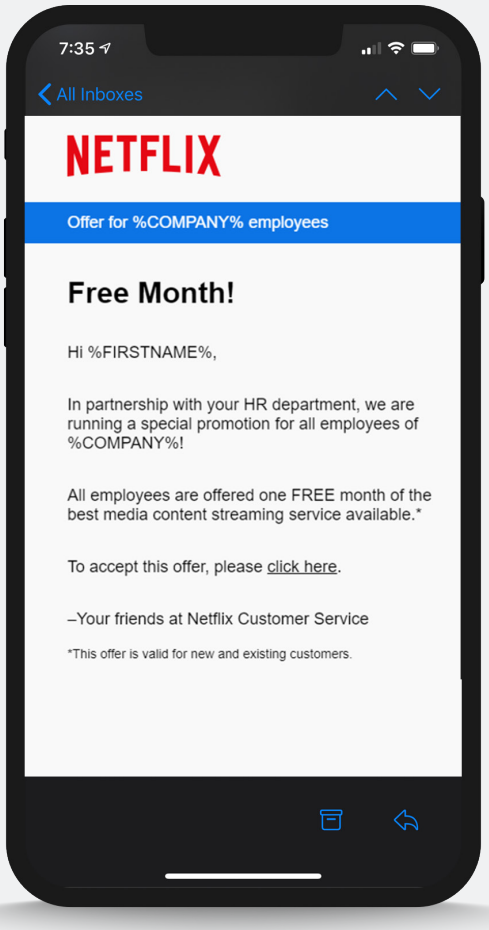


Abb. 3: Vorlage für simulierte Phishing-E-Mail mit gefälschtem Netflix-Aktionsangebot als Köder.

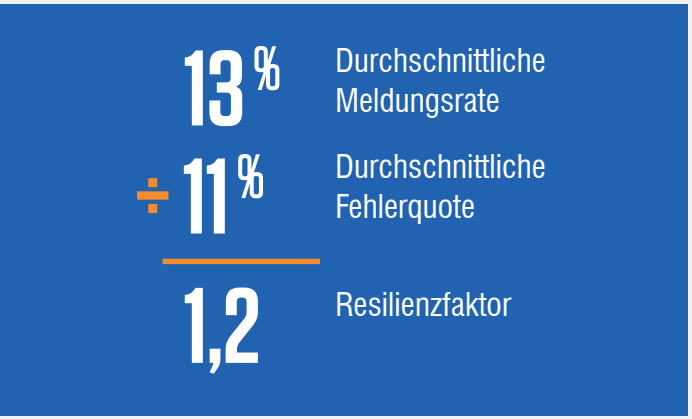


Abb. 4: Auf Grundlage dieser Formel liegt der durchschnittliche Resilienzfaktor von Proofpoint-Kunden bei 1,2.

Bewertung des Resilienzfaktors

Wenn Sie die Fehlerquote von Anwendern mit ihrer Meldungsrate kombinieren, erhalten Sie den sogenannten Resilienzfaktor.

So funktioniert diese Formel:

1. **Beginnen Sie mit der durchschnittlichen Meldungsrate für Phishing-Simulationen.** Bei typischen Proofpoint-Kunden beträgt sie 13 %. (Jeder Anwender meldete pro Jahr im Durchschnitt also etwas mehr als fünf Nachrichten.) Wir gehen davon aus, dass diese Zahl in den nächsten Jahren erheblich steigen wird, da Unternehmen ihre Schulungsinitiativen ausweiten und Anwender sich immer mehr daran gewöhnen, verdächtige Nachrichten zu melden.)
2. **Dividieren Sie die Zahl durch die durchschnittliche Fehlerquote für diese Simulationen.** Bei typischen Proofpoint-Kunden beträgt sie 11 %. Die Fehlerquote liegt praktisch nie bei 0 % und kann bei gezielteren und schwierigeren Simulationen erheblich abweichen.
3. **Das Ergebnis ist der Resilienzfaktor.** Bei Proofpoint-Kunden beträgt er 1,18 (in Abb. 4 aufgerundet auf 1,2).[6] Als Fernziel empfehlen wir einen Resilienzfaktor von 14 bzw. eine durchschnittliche Meldungsrate von 70 % und eine Fehlerquote von höchstens 5 %.

Der Resilienzfaktor ist einer der zuverlässigsten Indikatoren für das Anwenderrisiko. Einige Kunden haben einen Faktor von 14 erreicht. Mit dem richtigen Schulungsprogramm und einer Kultur des Sicherheitsbewusstseins können Sie diesen Faktor ebenfalls erreichen oder sogar übertreffen. Eine Änderung des Anwenderverhaltens erfordert jedoch Zeit und ständiges Engagement.

6 Bedenken Sie, dass sich unsere Kunden in den verschiedensten Phasen des Wegs zu mehr Sicherheitsbewusstsein befinden. Dieser Durchschnittswert schließt Resilienzfaktoren sowohl für Programme ein, die gerade erst starten, als auch solche, die bereits ausgereift sind.

14

Der Resilienzfaktor ist einer der zuverlässigsten Indikatoren für das Anwenderrisiko. Mit dem richtigen Schulungsprogramm und einer Kultur des Sicherheitsbewusstseins haben einige Kunden sogar einen Resilienzfaktor von 14 erreicht.

Meldungsraten und Fehlerquoten nach Typ

Wir nennen es das „Anhangsparadox“: Simulierte Phishing-E-Mails mit Anhängen führen zur höchsten Meldungsrate – und zur höchsten Fehlerquote (siehe Tabelle 1). Viele Anwender finden Anhänge wegen der darin versprochenen Daten verlockend (z. B. angebliche Corona-Infektionsdaten oder Bonuszahlungen). Ein gewisser Anteil der Nutzer ist bei Anhängen jedoch (zurecht) vorsichtiger und meldet diese häufiger.

TYP DES SIMULIERTEN PHISHING-ANGRIFFS	DURCHSCHNITTLICHE MELDUNGSRATE	DURCHSCHNITTLICHE FEHLERQUOTE	DURCHSCHNITTLICHER RESILIENZFAKTOR
ANHANG	18 %	20 %	0,9
DATENEINGABEN/ ANMELDEDATEN	15 %	4 %	3,8
LINKS	13 %	12 %	1,1

Tabelle 1: Fehlerquote und Meldungsrate nach Typ.[7]

Der Resilienzfaktor für Dateneingaben/Anmeldedaten-Phishing-Simulationen war deutlich höher als bei den beiden anderen Typen. Dieser Angriffstyp erfordert von den Anwendern jedoch einen zusätzlichen Schritt: Sie müssen auf den Link klicken und ihre Anmeldedaten eingeben, um der Fehlerquote zugerechnet zu werden.

7 Die Zahlen zu Fehlerquoten und Meldungsraten in diesem Abschnitt stammen aus unserem *State of the Phish-Bericht 2021*.

Genauer hingesehen: Resilienzfaktoren nach Branche

Tabelle 2 enthält einen Überblick über branchenspezifische Daten zu Fehlerquoten, Klickraten und Resilienzfaktoren. Die Finanzdienstleistungsbranche verzeichnete die höchste Meldungsrate (20 %). Den insgesamt größten Resilienzfaktor weist jedoch die Rechtsbranche auf (2,1).

BRANCHE	MELDUNGSRATE	FEHLERQUOTE	RESILIENZFAKTOR
FINANZDIENSTLEISTER	20 %	11 %	1,8
ENERGIE- UND VERSORGUNGSUNTERNEHMEN	18 %	11 %	1,6
VERSICHERUNGEN	17 %	10 %	1,7
RECHTSBRANCHE	17 %	8 %	2,1
KONSTRUKTION	16 %	16 %	1
AUTOMOBILBRANCHE	15 %	8 %	1,9
GESCHÄFTLICHE DIENSTLEISTUNGEN	14 %	11 %	1,3
TECHNOLOGIEANBIETER	13 %	12 %	1,1
BEHÖRDEN	13 %	10 %	1,3
BERGBAU	13 %	13 %	1
LEBENSMITTEL/GETRÄNKE	11 %	11 %	1
FERTIGUNGSINDUSTRIE	10 %	10 %	1
GESUNDHEITSWESEN	10 %	10 %	1
UNTERHALTUNG/MEDIEN	10 %	9 %	1,1
TRANSPORTWESEN	10 %	12 %	-1,2
TELEKOMMUNIKATION	9 %	14 %	-1,6
BAUINDUSTRIE	9 %	11 %	-1,2
EINZELHANDEL	9 %	13 %	-1,4
BILDUNGSEINRICHTUNGEN	6 %	12 %	-2
GASTGEWERBE/FREIZEIT	5 %	10 %	-2

Tabelle 2: Meldungsraten und Fehlerquoten nach Branche.

Verbesserung von Anwender-Meldungsraten

Wie Abb. 5 zeigt, erzielen einige wenige Unternehmen in unserem Datensatz die höchste Zahl an gemeldeten simulierten Phishing-E-Mails. Die meisten Unternehmen weisen nur geringe Meldungsraten auf.

Die Meldungsrate hängt vom Sicherheitsbewusstsein im Unternehmen sowie davon ab, wie lange die Anwender bereits ein Add-in oder eine Schaltfläche für E-Mail-Meldungen nutzen. Häufig ist eine niedrige Performance eher ein Indikator für unzureichende Kenntnisse des Meldetools und weniger für die Phishing-Bedrohungen an sich.

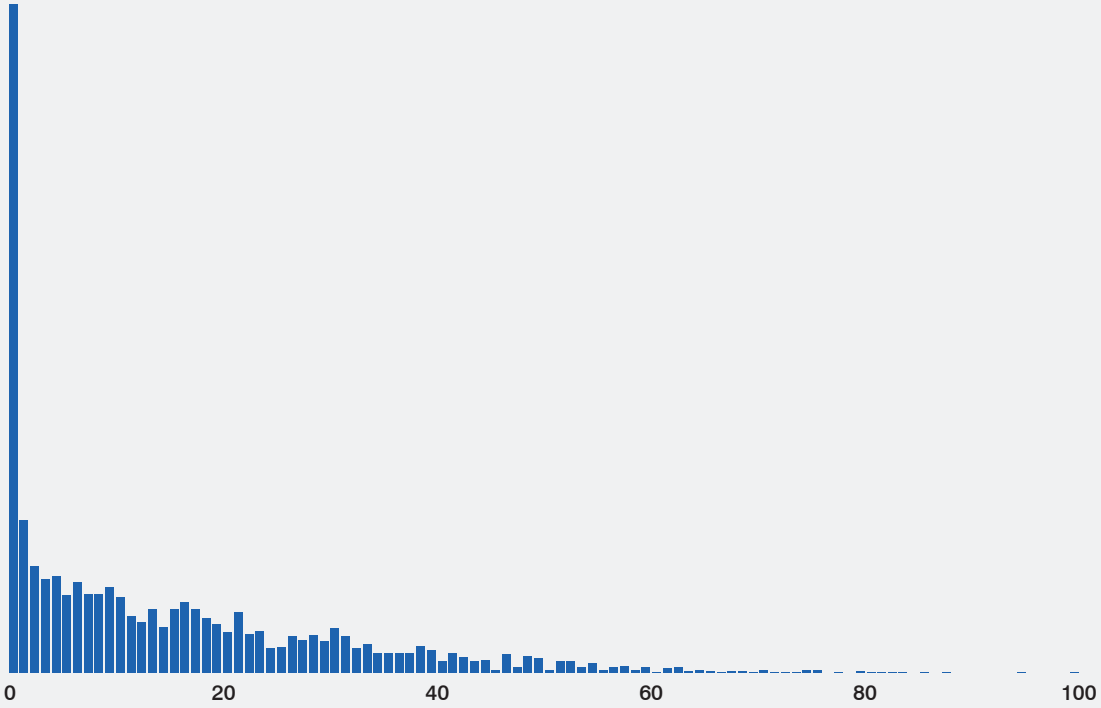


Abb. 5: Verteilung der Meldungsraten.

PERZENTIL	ANTEIL DER ANWENDER, DIE SIMULATIONEN MELDEN
25 %	1,4 %
50 %	8,5 %
75 %	19,9 %
Durchschnitt	13 %
BESTE LEISTUNG	83,6 %

Tabelle 3: Durchschnittliche Meldungsraten, aufgeschlüsselt nach Quartilen.

Bei geringen Meldungsraten haben wir häufig Folgendes festgestellt:

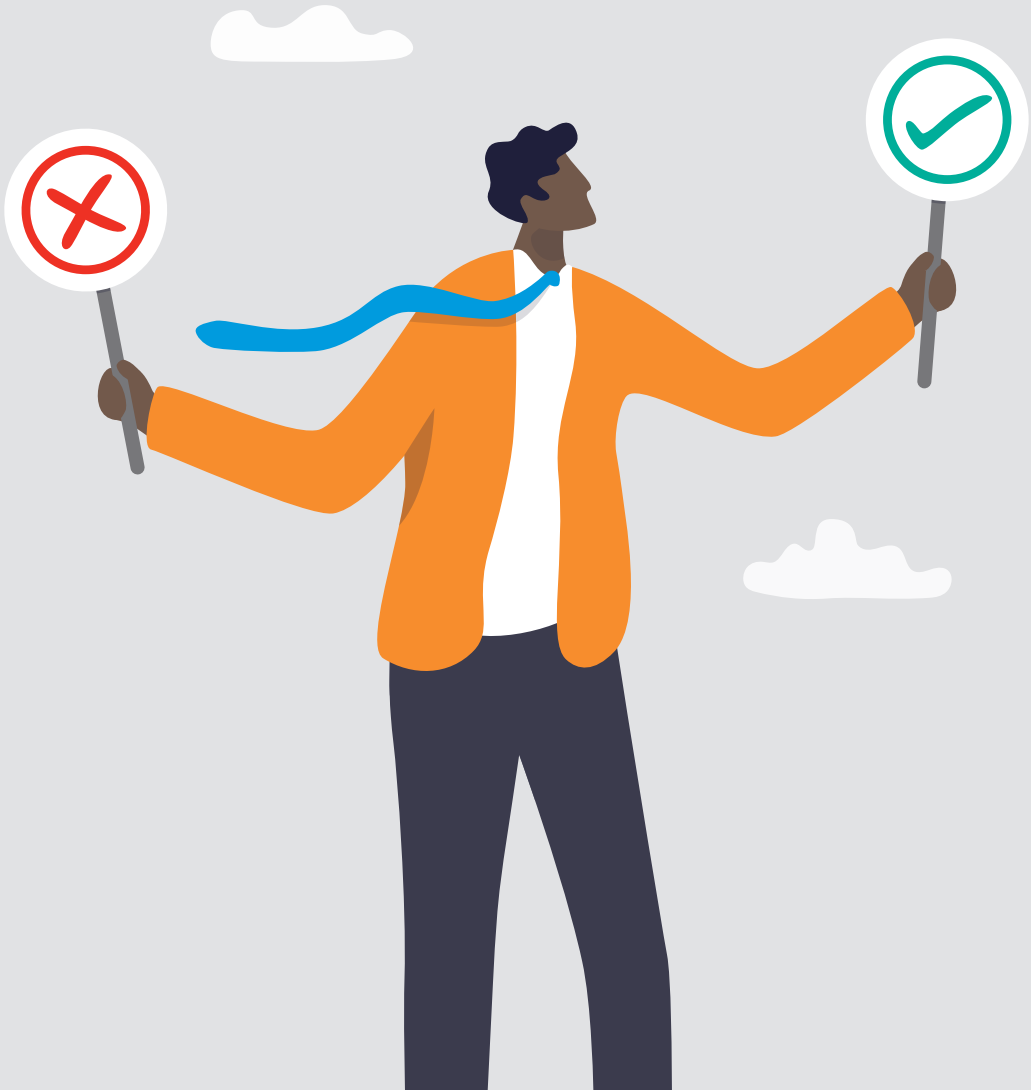
- Unternehmen haben die Add-ins für E-Mail-Meldungen gerade erst implementiert.
- Anwender haben mehrere Möglichkeiten zur Meldung von Nachrichten (z. B. eine Abuse-Postfach-Adresse), was in unseren Daten nicht ersichtlich wird.
- In Anwenderschulungen wird nicht darauf hingewiesen, wie sie mit dem Add-in verdächtige E-Mails melden können.
- Anwender löschen oder ignorieren Nachrichten, die für sie unerwartet eingegangen sind.

Die richtige Wissensvermittlung kann Ihrem Unternehmen enorm helfen, die Meldungsrate zu verbessern. Erläutern Sie daher im Rahmen Ihrer Schulungen zur Sensibilisierung für Sicherheit, wie das vorhandene Add-in für E-Mail-Meldungen genutzt wird. Erinnern Sie die Anwender regelmäßig an das Tool. Geben Sie außerdem Feedback, wenn Anwender simulierte Phishing-Nachrichten melden. Mit diesen Schritten können Sie die Meldungsrate verbessern – und so Ihr Unternehmen zu einem Top-Performer machen.

ABSCHNITT 2

Ein Blick auf die Realität: Anwender-Meldungsraten bei tatsächlichen Angriffen

Die Messung der Meldungsrate bei Phishing-Simulationen ist ganz klar unverzichtbar. Doch lässt sie sich auch in reale Ergebnisse umsetzen? Wenn eine wirklich schädliche oder verdächtige Nachricht im Postfach eingeht, wird sie dann von den Anwendern erkannt und gemeldet? Und wie zuverlässig sind solche Meldungen?



2,2 Milliarden

E-Mails werden täglich von uns analysiert.

Zur Beantwortung dieser Fragen analysierten wir Daten von Millionen von Anwendern, die Nachrichten als verdächtig eingestuft und daher über die Proofpoint PhishAlarm-Schaltfläche gemeldet hatten.[8] Wir prüften die Richtigkeit der Anwendermeldungen und verglichen dazu deren Berichte mit den von unserem E-Mail-Erkennungsmodul – dem Herzstück unserer Threat Protection-Plattform – klassifizierten E-Mails.

Hinweis: Für manche Leser stellt sich womöglich die Frage, wie E-Mails, die von unserem Erkennungsmodul als schädlich gekennzeichnet wurden, überhaupt in den Posteingang der Anwender gelangen konnten. Nicht jeder PhishAlarm-Kunde setzt auch unsere E-Mail-Sicherheitslösungen ein. Oft wissen wir, dass eine E-Mail schädlich ist, weil der Angriff bei einer der Milliarden anderen E-Mails aufgefallen ist, die wir jeden Tag analysieren.

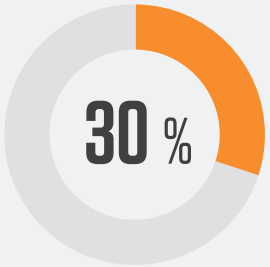
Erkennungskategorien:

- **Schädlich:** Diese E-Mails enthalten Malware, Phishing, Impostor-Elemente oder andere Bedrohungen.
- **Verdächtig:** Diese E-Mails sind wahrscheinlich schädlich und sollten von Ihnen unter Quarantäne gestellt werden. Prüfen Sie sie jedoch, um sicherzustellen, dass keine legitimen E-Mails verloren gehen.
- **Spam:** Diese E-Mails sind unerwünscht und könnten schädliche Inhalte aufweisen.
- **Massen-E-Mail:** Diese E-Mails haben eine geringe Priorität oder sind Werbe-E-Mails. Sie stellen keine Bedrohung dar.
- **Geringes Risiko:** Bei genauerer Analyse dieser E-Mails finden sich keine Anzeichen für schädliche Inhalte.
- **Wahrscheinlich keine Bedrohung:** Diese E-Mails lassen bei der Analyse in einer Sandbox und bei der Untersuchung durch unser Erkennungsmodul keine schädlichen Inhalte oder Aktivitäten erkennen.

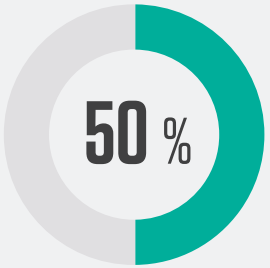
Wir haben Unternehmen in zwei unterschiedliche Gruppen unterteilt. Die erste Gruppe nutzt Proofpoint-Tools zum Melden von verdächtigen und schädlichen E-Mails, jedoch nicht von Spam. Die zweite Gruppe nutzt Proofpoint-Tools zum Melden von Spam sowie von verdächtigen und schädlichen E-Mails. Einige Unternehmen stufen Spam als „richtige“ Meldung ein, andere nicht. Dies ist der Grund, aus dem sie in diese beiden Gruppen unterteilt wurden.

8 Anteil an den verdächtigen E-Mails, die zwischen September 2019 und Oktober 2020 über unsere PhishAlarm-Funktion gemeldet wurden.

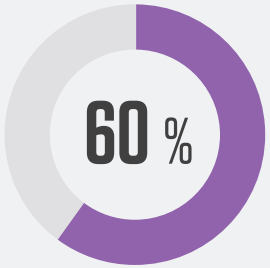
Schädliche und verdächtige Nachrichten



Bei den meisten Unternehmen sind etwa 30 % der gemeldeten Nachrichten tatsächlich schädlich oder verdächtig.



Spitzenreiter erreichen Werte über 50 %.



Bei vielen Unternehmen liegt die Richtigkeit bei über 60 %.

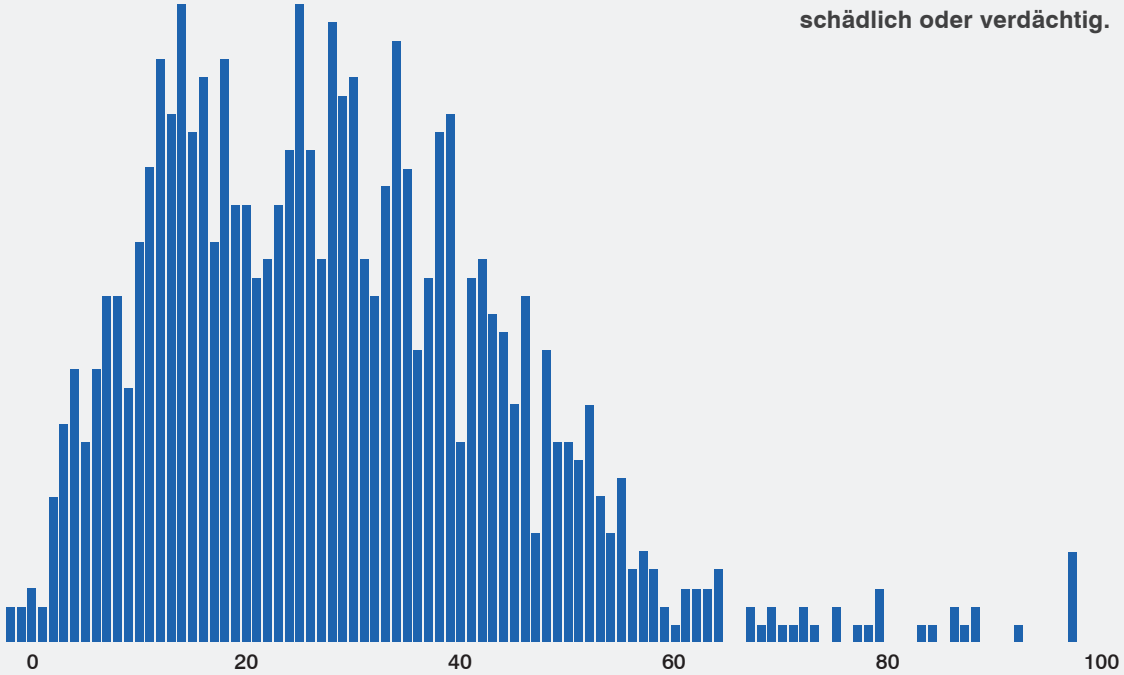


Abb. 6: Richtigkeit von E-Mail-Meldungen – Verteilung.

PERZENTIL	RICHTIGKEIT
25 %	18,1 %
50 %	29,6 %
75 %	41,1 %
Durchschnitt	31,0 %
BESTE LEISTUNG	**100 %**

Tabelle 4: Richtigkeit der Meldung von schädlichen und verdächtigen E-Mails – aufgeschlüsselt nach Quartilen.

Schädliche, verdächtige und Spam-Nachrichten

Nach Aufnahme von Spam-Nachrichten in die Meldungen stieg die Richtigkeit in allen Bereichen um durchschnittlich ein Drittel. Viele Anwender sind möglicherweise unsicher, was eine schädliche E-Mail ist, aber die meisten erkennen Spam-Nachrichten auf den ersten Blick.

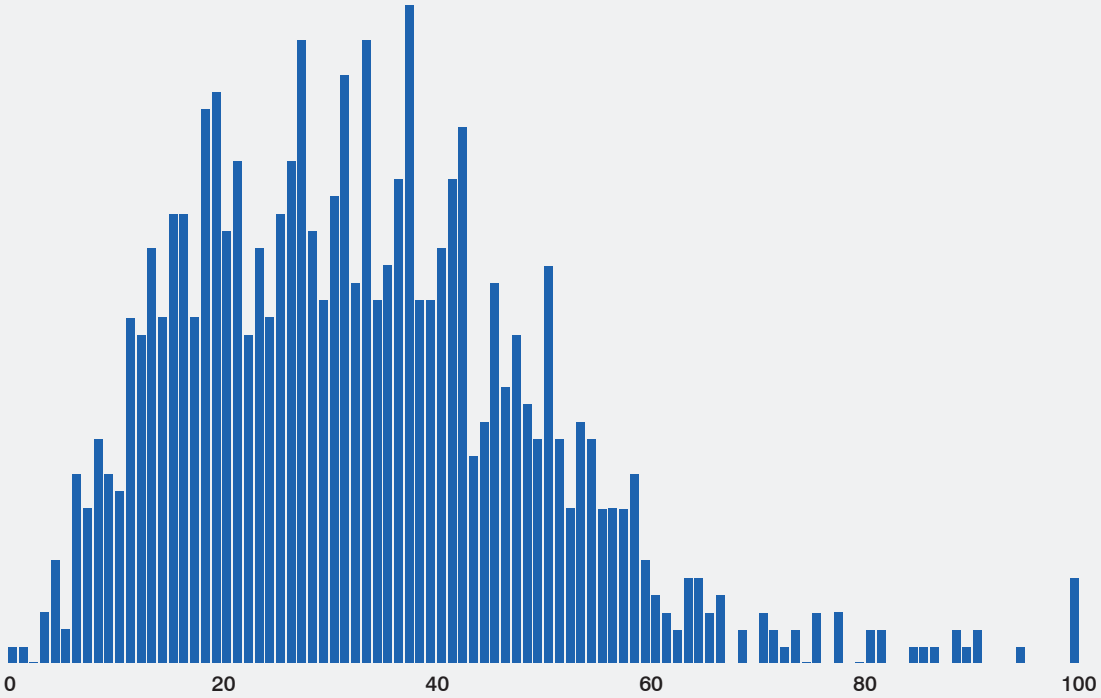
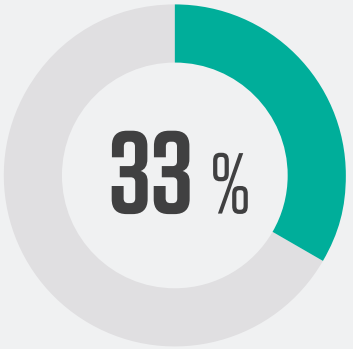


Abb. 7: Verteilung der Richtigkeit von E-Mail-Meldungen – einschließlich Spam.



Nach Aufnahme von Spam-Nachrichten in die Meldungen stieg die Richtigkeit um durchschnittlich ein Drittel.

PERZENTIL	RICHTIGKEIT
25 %	20,4 %
50 %	31,7 %
75 %	42,6 %
Durchschnitt	33,1 %
BESTE LEISTUNG	100 %

Tabelle 5: Richtigkeit der Meldung von schädlichen, verdächtigen und Spam-E-Mails – aufgeschlüsselt nach Quartilen.

ABSCHNITT 3

Neue Wege gehen – weg vom Abuse-Postfach

Das Abuse-Postfach kann IT-Sicherheitsteams vor große Probleme stellen. Unter Umständen müssen tausende Stunden investiert werden für:

- Untersuchung von Nachrichten
- Identifizierung der schädlichen Nachrichten
- Entfernung aller Kopien, bevor Bedrohungen von Anwendern aktiviert werden können

Und das gilt nur für echte Bedrohungen. Falsche Meldungen – dies sind bei einem durchschnittlichen Unternehmen mehr als zwei Drittel aller gemeldeten Nachrichten – ziehen sogar noch höhere Kosten nach sich. Die ohnehin schon ausgelasteten Sicherheits- und IT-Teams müssen False Positives auf den Grund gehen, während potenziell schwerwiegende Angriffe auf ihre Chance warten.

700.000 $

Allein die Reaktion auf Anmeldedaten-Phishing, eine der häufigsten Bedrohungen, kostet Unternehmen pro Jahr rund 700.000 US-Dollar.[9]

Ein durchschnittliches Unternehmen mit etwa 10.000 Mitarbeitern muss tausende Stunden in die Behebung von Bedrohungen wie Business Email Compromise (BEC, auch Chefmasche genannt), Malware-Infektionen, Ransomware und Anmeldedaten-Diebstahl investieren. Dies sind in der Regel die maßgeblichen Faktoren für E-Mail-basierte Bedrohungen. Allein die Reaktion auf Anmeldedaten-Phishing, eine der häufigsten Bedrohungen, kostet Unternehmen pro Jahr rund 700.000 US-Dollar.[10]

AUFGABEN	MALWARE-INFEKTIONEN	BUSINESS EMAIL COMPROMISE	RANSOMWARE	DIEBSTAHL VON ANMELDEDATEN
PLANUNG	1.248	1.019	967	885
ERFASSUNGSINTELLIGENZ	4.892	4.450	3.889	3.630
BEWERTUNGSINTELLIGENZ	4.282	5.001	4.200	5.411
UNTERSUCHUNG	12.045	12.336	11.901	12.884
BEREINIGUNG UND BEHEBUNG	12.215	14.395	13.415	11.950
DOKUMENTATION	951	1.075	913	1.002
STUNDEN GESAMT	**36.633**	**38.276**	**35.285**	**35.762**

Tabelle 6: Anzahl der Stunden, die IT-Teams für die Behebung unterschiedlicher Typen von Phishing-Angriffen benötigen (Quelle: *Ponemon-Studie zu Kosten durch Phishing 2021*).

9 Ponemon: „Studie zu Kosten durch Phishing 2021, August 2021.
10 ebd.

ABSCHNITT 4

Nächste Schritte: Vereinfachung und größere Überschaubarkeit von Meldungen

Ein Sicherheitsverantwortlicher, der vor einiger Zeit unsere PhishAlarm-Schaltfläche zur E-Mail-Meldung getestet hatte, erklärte uns, dass ihm die Idee der Meldung durch Anwender zwar gefiele, er sie aber noch nicht mit vollem Funktionsumfang bereitstellen wollte. Sein Team wäre besorgt, dass es mit von Anwendern gemeldeten False Positives nur so überschwemmt würde.

Damit hatte er nicht ganz Unrecht: Im Durchschnitt sind zwei Drittel der von Anwendern gemeldeten E-Mail-Nachrichten faktisch nicht schädlich. Hier gibt es also noch viel Verbesserungspotenzial.

Glücklicherweise können Sie die Anwender zu Meldungen ermutigen und das Risiko verringern, ohne gleich in blinden Alarmen zu ersticken. **Hier erfahren Sie, wie das funktioniert.**

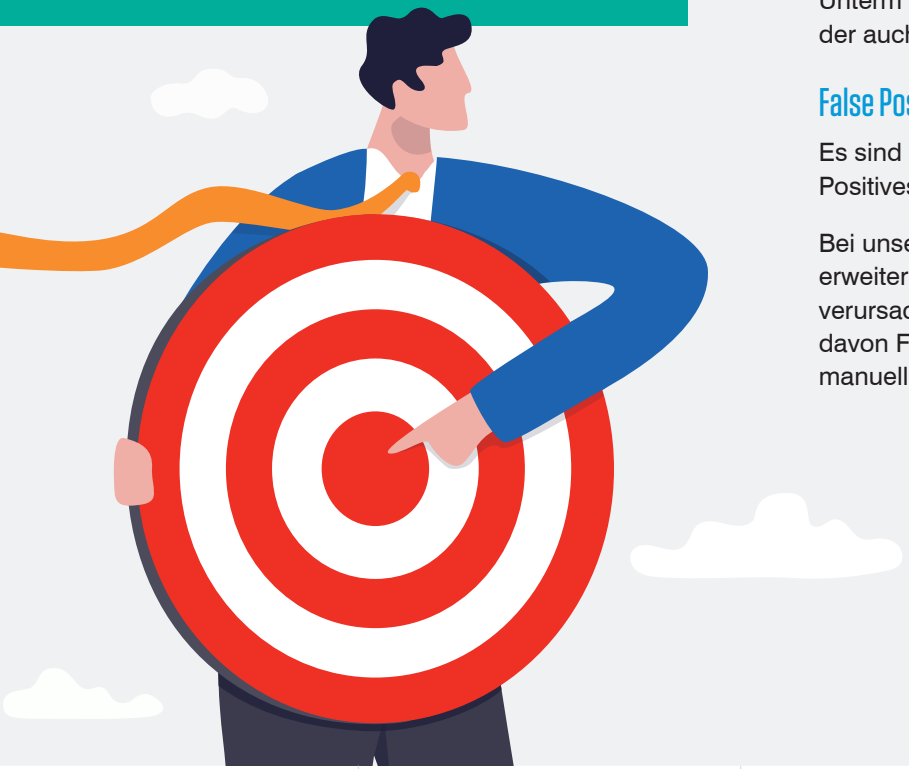
01 Beginnen Sie mit den Nachrichten in Ihrem Posteingang – den erwünschten, den schädlichen und den unerwünschten

Falls Ihr Abuse-Postfach bereits durch ein Schwemme an Spam-, Phishing- und anderen Nachrichten überquillt, ist es wichtig, an der Wurzel des Problems anzusetzen: dass **Nachrichten Ihren Anwendern zunächst einmal zugestellt werden**. Sie benötigen daher eine **ausgereifte E-Mail-Sicherheitslösung**, um die Anzahl schädlicher Nachrichten in Ihrem Posteingang zu verringern.

Wir empfehlen zwar dringend eine automatisierte Lösung für E-Mail-Meldungen und Behebungsmaßnahmen wie **Proofpoint Closed-Loop Email Analysis and Response (CLEAR)**, doch ist Automatisierung allein kein Allheilmittel. Ab einem gewissen Punkt bringt das Volumen eingehender – und dann gemeldeter – schädlicher E-Mails selbst die besten automatisierten Systeme an ihre Grenzen. Wenn weniger schädliche E-Mails in die Postfächer gelangen, werden auch weniger von den Anwendern gemeldet.

68 %

In einem Fall gab ein CESS an, dass 900 Nachrichten schädlich seien, obwohl tatsächlich 68 % davon False Positives waren.



Vorsicht ist besser als Nachsicht

Ein zuverlässig abgesichertes E-Mail-Postfach ist gewissermaßen eine Präventivmaßnahme. Es ist besser, das Problem bei seiner Entstehung anzugehen, als später die sich anschließenden, potenziell schlimmeren Auswirkungen beseitigen zu müssen. Dieser Ansatz spiegelt Frameworks wie MITRE ATT&CK und dessen „Linksverschiebung“ in der Angriffskette hin zum PRE-ATT&CK-Framework wider.

Mit diesem Problem in der E-Mail-Sicherheit haben wir es häufig bei unseren Bedrohungsbewertungen bei potenziellen Kunden zu tun. Vor kurzem führten wir gemeinsam mit Unternehmen eine Reihe von Proof-of-Concept-Projekten mithilfe von Microsoft-E-Mail-Gateways durch und **fanden dabei hunderttausende schwerwiegender Bedrohungen, die nicht abgefangen wurden, sondern unbemerkt „durchrutschten“**. Dazu zählten der Diebstahl von Anmeldedaten, schädliche Anhänge, unsichere URLs und BEC-Bedrohungen.

Unterm Strich kommt es zu einem höheren Zeit- und Ressourcenaufwand für die Reaktion auf Zwischenfälle, der auch später Auswirkungen nach sich zieht.

False Positives – ein großes Manko

Es sind nicht nur wirkliche Bedrohungen und Spam, die den Sicherheitsteams Probleme bereiten. Auch False Positives tragen zu einer unnötig großen Belastung bei der Reaktion auf Zwischenfälle bei.

Bei unseren Proofs of Concept haben wir festgestellt, dass viele API-basierte Cloud-E-Mail-Sicherheits-erweiterungen (CESS) bei potenziellen Kunden während ihrer Proofs of Concept eine hohe False-Positive-Rate verursachten. In einem Fall gab ein CESS an, dass 900 Nachrichten schädlich seien, obwohl tatsächlich 68 % davon False Positives waren. Das Team hätte in diesem Fall über 600 falsch gekennzeichnete Nachrichten manuell durchkämmen müssen, um sicherzustellen, dass sie zugestellt würden.

02 Helfen Sie Anwendern bei zuverlässigeren Meldungen

Eine größere Zuverlässigkeit der E-Mail-Meldungen von Anwendern kann Wunder wirken, wenn es darum geht, die Anzahl falsch positiver Meldungen zu verringern. (Ungeachtet dessen empfehlen wir weiterhin, dass Anwender alles melden sollen, bei dem sie unsicher sind. Für Ihr Team ist es besser, einen Überblick über alle potenziellen Bedrohungen zu erhalten, die in den Posteingängen der Anwender lauern.)

Einbindung und ständige Verstärkung

Ergänzen Sie Ihre Phishing-Schulungsinitiativen, indem Sie den Anwendern demonstrieren, wie sie ihre neuen Fähigkeiten nutzbringend anwenden können. Erläutern Sie die Schaltfläche zur E-Mail-Meldung und erklären Sie, welchen Zweck sie hat, wann sie zu nutzen ist und wie auf unterschiedlichen Geräten darauf zugegriffen werden kann. Auf diese Weise verbessern Sie die Zuverlässigkeit von Anwendermeldungen.

So rücken Sie das Add-in für E-Mail-Meldungen in das Bewusstsein der Anwender – einige Möglichkeiten:

- Vorstellung der Benutzeroberfläche in Unternehmens-Newslettern und Erläuterung ihrer Funktionsweise
- Erörterung des Add-ins bei Unternehmensveranstaltungen und Mitarbeiterversammlungen
- Integration von E-Mail-Meldungen in bestehende Programme zur Sensibilisierung für Sicherheit

Sie können die Zuverlässigkeit von Anwendermeldungen mit einem Startplan verbessern, der sich nahtlos in ein umfassendes Schulungsprogramm zur Sensibilisierung für Phishing integrieren lässt. Setzen Sie verschiedenste Medien und Formate ein, um die Anwender zu motivieren.

Feedback zu gemeldeten Nachrichten

Niemand möchte, dass seine Bemühungen um Wachsamkeit in einem schwarzen Loch verschwinden. Wenn die Anwender nicht das Gefühl haben, dass ihre Berichte ernst genommen werden, lassen sie es beim nächsten Mal sein. Eine unterbrochene Rückkopplungsschleife kann auch zu neuen Tickets führen, die Ihr Team bearbeiten muss, wenn Anwender wegen ihrer ursprünglichen Meldung nachfassen.

Es ist viel einfacher, die Rückkopplungsschleife zu automatisieren und die Anwender über den Status der von ihnen gemeldeten Nachricht auf dem Laufenden zu halten. Dieses Feedback verbessert die Kompetenzen der Anwender und erhöht die Zuverlässigkeit ihrer Meldungen.

Hinweise für Anwender durch Warnkennzeichnungen innerhalb von E-Mails

Durch HTML-basierte E-Mail-Warnhinweise werden Anwender kontextbezogen auf Bedrohungen aufmerksam gemacht, um die Anzahl und Zuverlässigkeit ihrer E-Mail-Meldungen zu verbessern. Wenn Anwender Kontext zu einer Nachricht erhalten – und zwar innerhalb der Nachricht –, können sie das Risiko leichter in Echtzeit prüfen.

Diese Hinweise können für unterschiedliche Typen potenziell schädlicher Nachrichten angepasst werden, um die Aufmerksamkeit der Anwender zu schärfen und ihnen die Möglichkeit zu geben, Phishing einfacher zu melden.

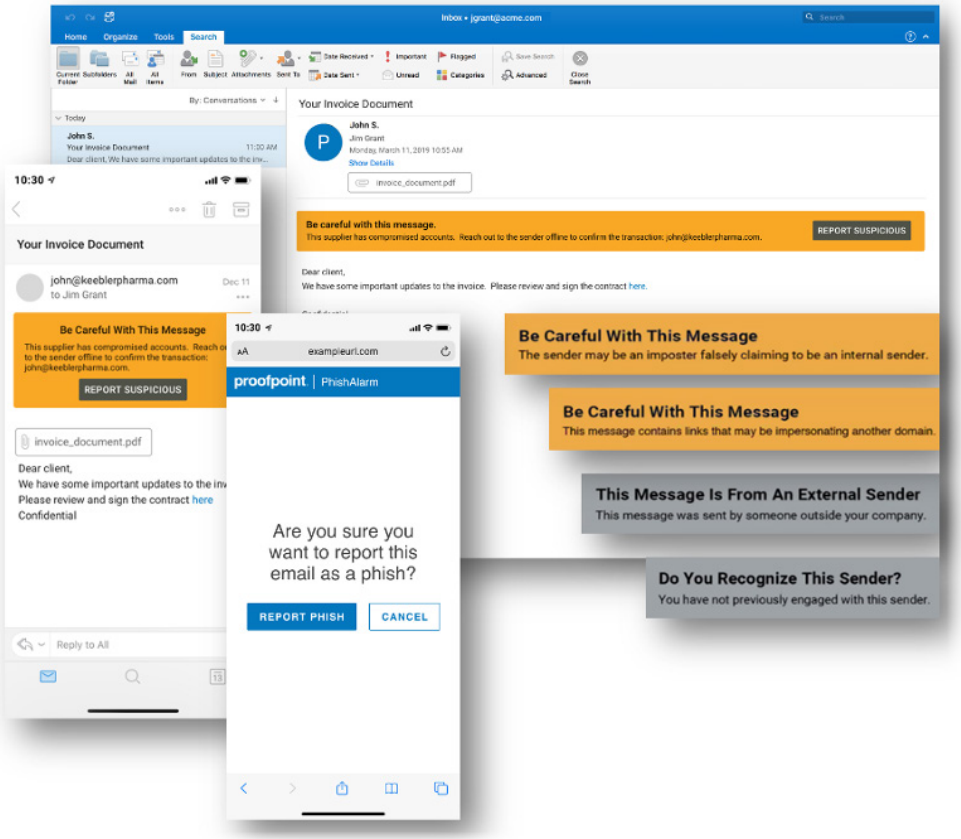


Abb. 8: Warnhinweise innerhalb von E-Mails können dazu beitragen, die Aufmerksamkeit der Anwender auf Nachrichten zu lenken, die ein erhöhtes Risiko darstellen könnten.

03 Nutzen Sie Automatisierung und erwägen Sie den Einsatz von Professional Services

Sie haben die allgemeine Sicherheitslage bereits verbessert und Anwendern die notwendigen Tools und Informationen in die Hand gegeben, mit denen sie die Meldung von Phishing-E-Mails verbessern können. Der letzte Schritt besteht nun darin, die Reaktion auf Zwischenfälle so weit wie möglich zu automatisieren.

Durch die Automatisierung des Abuse-Postfachs können Sie Workflows optimieren und den Zeitaufwand für manuelle Aufgaben reduzieren. Einige unserer Kunden haben ihre Arbeitslast um sage und schreibe 90 % verringert.

Doch Unternehmen stehen auch bei den Ressourcen zur Verwaltung der E-Mail-Sicherheit unter Druck. Falls dieser Aspekt auch für Sie problematisch ist, sollten Sie darüber nachdenken, einen erstklassigen Partner für **verwaltete E-Mail-Services** einzubinden, um die Belastung der IT-Abteilung zu verringern und Ihre E-Mail-Sicherheit zu verbessern.

Nicht alle Sicherheitsteams haben das Know-how und die Ressourcen, um Bedrohungsdaten und die Ergebnisse von Sandbox-Analysen zu einem Gesamtbild zusammenzufügen. Noch weniger verfügen über das Personal oder die Zeit zur ständigen Aktualisierung von YARA-Regeln und Playbooks, um auf dem neuesten Stand zu bleiben. (YARA ist ein Tool, das bei der Malware-Forschung für den Musterabgleich eingesetzt wird.)

Professional Services können dabei helfen, die Lücke zu füllen, damit Ihrem Team mehr Zeit bleibt, um sich auf strategische Sicherheitsaufgaben zu konzentrieren.

Fazit

E-Mail-Meldungen von Anwendern können einen wesentlichen Beitrag zu Ihrer Sicherheitsstrategie leisten. Doch ohne den richtigen Ansatz für Behebungsmaßnahmen können sie auch ein zweischneidiges Schwert sein.

Wenn Sie vermeiden möchten, dass Ihre Sicherheitsteams durch E-Mail-Meldungen – und eine Flut von False Positives – überlastet werden, müssen Sie das Aufkommen von schädlichen Spam-E-Mails verringern, die Zuverlässigkeit von Anwendermeldungen verbessern und Ihre Reaktion darauf automatisieren (oder auslagern).

Nutzen Sie die in diesem E-Book vorgestellten Strategien. Hierdurch können Sie die Sicherheitslage Ihres Unternehmens verbessern und ein optimiertes Abuse-Postfach implementieren.

Informieren Sie sich, wie Proofpoint Ihnen bei der Entwicklung von mehrstufigen Abwehrmaßnahmen gegen Phishing-Angriffe helfen kann.
Weitere Informationen finden Sie unter **proofpoint.com/de**.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **www.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 mehr als die Hälfte der Fortune-1000-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.

0504-005-01-01 04/22