proofpoint.

JAHRESBERICHT

State of the Phish 2021

Eine umfassende Bestandsaufnahme: Sicherheitsbewusstsein und Bedrohungsabwehr im Fokus

proofpoint.com/de

EINLEITUNG: EIN JAHR WIE KEIN ANDERES

Das Jahr 2020 stellte Menschen ebenso wie Unternehmen vor viele neue und bekannte Herausforderungen. Auch IT-Sicherheitsteams bekamen das zu spüren.

Neben „gewöhnlichen" Cybersicherheitsproblemen mussten sich die Sicherheitsexperten auch mit der rasanten Zunahme an Pandemie-bezogenen Betrugsversuchen sowie einer beständigen Flut von Ransomware-Angriffen herumschlagen. Gleichzeitig mussten die IT-Teams praktisch über Nacht viele Anwender beim Wechsel ins Home Office unterstützen.

Unser siebenter, jährlich erscheinender *State of the Phish*-Bericht beleuchtet diese und weitere Themen. Wir analysieren Umfragedaten, simulierte Phishing-Angriffe und reale Attacken, um Einblicke in Phishing und andere Bedrohungen zu geben sowie aufzuzeigen, wie Sie sich schützen können.

Der diesjährige Bericht umfasst Daten aus diesen Quellen:

Eine Drittanbieterumfrage unter

3.500

berufstätige Erwachsenen in sieben Ländern

(Australien, Deutschland, Frankreich, Großbritannien, Japan, Spanien und USA)

Eine Drittanbieterumfrage unter

600

IT-Sicherheitsexperten aus diesen sieben Ländern

Mehr als

60 Mio.

simulierte Phishing-Angriffe, die von unseren Kunden innerhalb von 12 Monaten gesendet wurden

Etwa

15 Mio.

E-Mails, die von Endnutzern unserer Kunden gemeldet wurden

„Phishing" kann für unterschiedliche Menschen unterschiedliche Bedeutungen haben. Wir bezeichnen damit alle E-Mail-Angriffe mit Social-Engineering-Elementen, unabhängig von der jeweiligen schädlichen Absicht (z. B. Umleitung von Anwendern zu gefährlichen Websites, Verteilung von Malware oder Erfassung von Anmeldedaten).

Inhaltsverzeichnis

4 **Die Herausforderungen von 2020:**
Unternehmensüberblick

12 **Benchmark-Analyse:**
Daten zu Branchen und Abteilungen

15 **Wichtige Zahlen:**
Anteil gemeldeter E-Mails
und Resilienzverhältnis

18 **Bedrohungsdaten:**
Identifizieren der Very Attacked People

20 **Personenzentrierte Sicherheit:**
Der aktuelle Stand bei Schulungen zur
Steigerung des Sicherheitsbewusstseins

29 **Fazit:**
Aufmerksamkeit und Entschlossenheit
sind gefragt

31 **Anhang**

ABSCHNITT 1

Die Herausforderungen von 2020: Unternehmensüberblick

57 %

der Teilnehmer einer Drittanbieter-Umfrage gaben an, ihr Unternehmen hätte 2020 einen erfolgreichen Phishing-Angriff erlebt. 2019 waren es mit **55 %** etwas weniger.

Für Phishing-Angriffe war 2020 ein Erfolgsjahr. Wir beobachteten Anmeldedaten-Phishing- und Social-Engineering-Techniken in großem Umfang (wobei einige raffinierter vorgingen als andere). Bei über der Hälfte unserer Email Protection-Kunden gingen mindestens 1.000 Phishing-Versuche ein. Bei einigen Kunden haben wir Millionen von Nachrichten blockiert. Die Angreifer nahmen zwar verschiedenste Branchen ins Visier, Fertigungsunternehmen verzeichneten jedoch im Durchschnitt das höchste Aufkommen an Phishing-E-Mails.

Allerdings ist kein technisches Tool absolut sicher. In unserer weltweiten, von einem unabhängigen Drittanbieter durchgeführten Umfrage unter IT-Sicherheitsexperten gaben 57 % der Befragten an, dass ihr Unternehmen 2020 von einem erfolgreichen Phishing-Angriff betroffen war. Das ist ein leichter Anstieg gegenüber unserer vorherigen Befragung.[1]

Diese Angriffe hatten schwerwiegende Auswirkungen auf die betroffenen Unternehmen. Im Vergleich zu unserer vorherigen Umfrage gaben 13 % mehr Befragte an, dass die Phishing-Angriffe zu Datenverlust führten. Außerdem berichteten 11 % mehr, dass durch diese Angriffe Anmeldedaten kompromittiert wurden.

Aber es gab auch ein paar Lichtblicke.

Die Zahl der Ransomware-Infektionen blieb im Jahresvergleich stabil. Gleichzeitig meldeten 17 % weniger Umfrageteilnehmer als in unserer vorherigen Umfrage Malware-Infektionen infolge von Phishing. Bei 47 % weniger Befragten kam es zu direkten finanziellen Schäden. Diese Ergebnisse könnten darauf hinweisen, dass Unternehmen stärkere Präventionsmaßnahmen gegen diese Art von Angriffen implementiert haben.

INTERNATIONAL

74 %

der US-Unternehmen verzeichneten im vergangenen Jahr einen erfolgreichen Phishing-Angriff. Die Zahl liegt **30 %** über dem weltweiten Durchschnitt und ist eine Steigerung von **14 %** im Vorjahresvergleich.

< 50 %

der französischen und deutschen Unternehmen waren von einem erfolgreichen Phishing-Angriff betroffen.

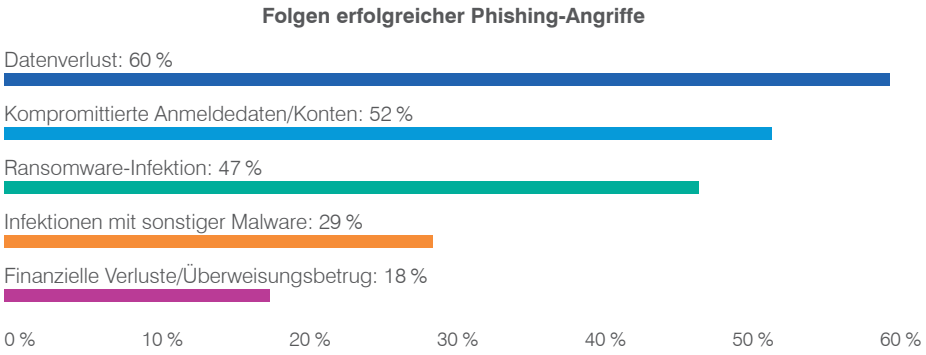


Abb. 1.

[1] Sofern nicht anders angegeben, handelt es sich bei den Umfrageergebnissen um weltweite Durchschnittswerte. Eine Aufschlüsselung der Umfrageergebnisse nach Ländern finden Sie im Anhang.

DIE FAKTEN

Die Bedeutung von Phishing-Angriffen unterschied sich von Region zu Region stark. Unabhängig davon, ob sich diese Unterschiede nun aus den kulturellen Einflüssen der Befragten oder der geografischen Diversität der Methoden der Angreifer ergeben – sie sind in jedem Fall erwähnenswert.

Nehmen wir zum Beispiel die enormen Mengen an betrügerischen Amazon-Meldungen in Japan im Jahr 2020. Das extreme Volumen dieser Anmeldedaten-Phishing-Angriffe kann zum überdurchschnittlichen Auftreten von Kontenkompromittierungen im Land beigetragen haben.[2]

Etwa **64 %** der japanischen Unternehmen hatten mit kompromittierten Anmeldedaten zu kämpfen. Das ist der größte prozentuale Anteil unter allen untersuchten Regionen. Dort kam es jedoch auch am seltensten zu direkten finanziellen Schäden (**11 %**).

Gleichzeitig verzeichneten **69 %** der spanischen Umfrageteilnehmer Datenverluste gegenüber nur **47 %** der australischen Kollegen.

Phishing-basierte Ransomware bedrohte **67 %** der australischen Unternehmen im Vergleich dazu nur **25 %** der französischen Umfrageteilnehmer.

In den USA kam es bei **35 %** der Befragten zu finanziellen Schäden und damit doppelt so häufig wie im weltweiten Durchschnitt.

Die Wandlungsfähigkeit gezielter Angriffe

Auf jeden erfolgreichen Angriff kommen viel mehr vereitelte Phishing-Angriffe. Über 75 % der Unternehmen gaben an, 2020 breit angelegten – sowohl erfolgreichen als auch erfolglosen – Phishing-Angriffen ausgesetzt gewesen zu sein. Diese Vorgehensweise, bei der die gleiche Phishing-E-Mail an zahlreiche Personen gesendet wird, kam in allen von uns untersuchten Regionen am häufigsten vor.

Das bedeutet jedoch nicht, dass Spearphishing, Whaling (gezielte Angriffe gegen Führungskräfte) und Business Email Compromise (BEC, auch als Chefmasche bekannt) gegenüber Massen-Kampagnen als „unbedeutendere" Bedrohungen angesehen werden sollten. Diese Arten von Angriffen richten sich zwar gegen weniger Menschen, doch durch die starke Fokussierung und Raffinesse sind sie für Anwender schlechter erkennbar und für technische Tools schwerer zu blockieren. Angreifer sind geschickt darin, Recherchen über bestimmte Rollen und Personen anzustellen und diese dann gezielt anzugreifen. Deshalb sollte jeder Phishing, Whaling und BEC fest im Auge behalten.

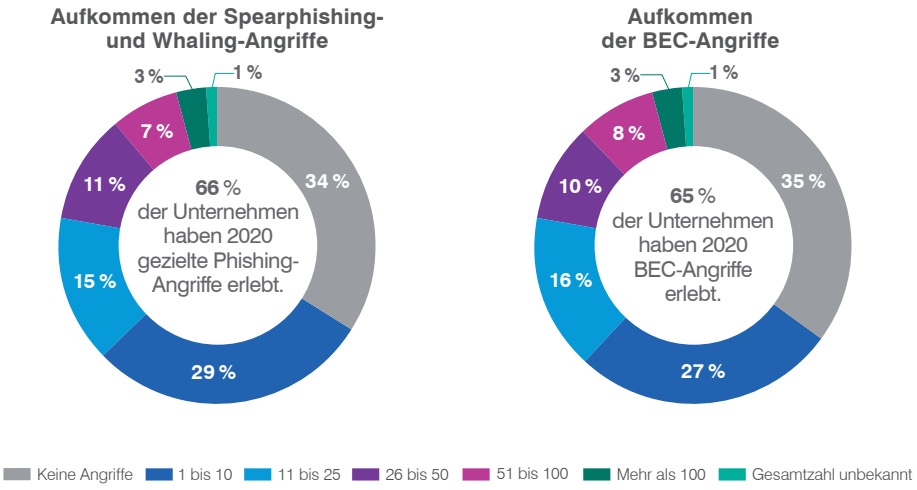


Abb. 2.

[2] Proofpoint: „Geofenced Amazon Japan Credential Phishing Volumes Rival Emotet" (Regionale Anmeldedaten-Phishing-Angriffe mit Amazon Japan machen Emotet Konkurrenz), Oktober 2020.

Unkonventionelle Social-Engineering-Angriffe jenseits von E-Mails

Social-Engineering-Angriffe treten in verschiedenen Formen auf, nicht nur als E-Mail. Die Angreifer verwenden soziale Netzwerke, Textnachrichten und sogar Voicemails, um Anwender hinters Licht zu führen. Hier sind einige der (erfolgreichen und erfolglosen) Angriffe ohne E-Mail-Beteiligung, die IT-Sicherheitsexperten 2020 beobachtet haben:

INTERNATIONAL

US-amerikanische und französische Unternehmen lagen 2020 bei Social-Engineering-Angriffen, die nicht auf E-Mails basierten, an den entgegengesetzten Enden des Spektrums:

US-Unternehmen

86 %
verzeichneten Social-Media-Angriffe wie Pretexting und Kontoübernahmen

81 %
verzeichneten SMS-/Text-Phishing-Angriffe (Smishing)

80 %
hatten mit manipulierten USB-Sticks zu tun

77 %
erlebten Phishing-Angriffe per Telefon (Vishing)

VS.

Französische Unternehmen

48 %
verzeichneten Smishing-Angriffe

33 %
verzeichneten Social-Media-Angriffe

31 %
hatten mit manipulierten USB-Sticks zu tun

29 %
verzeichneten Vishing-Angriffe

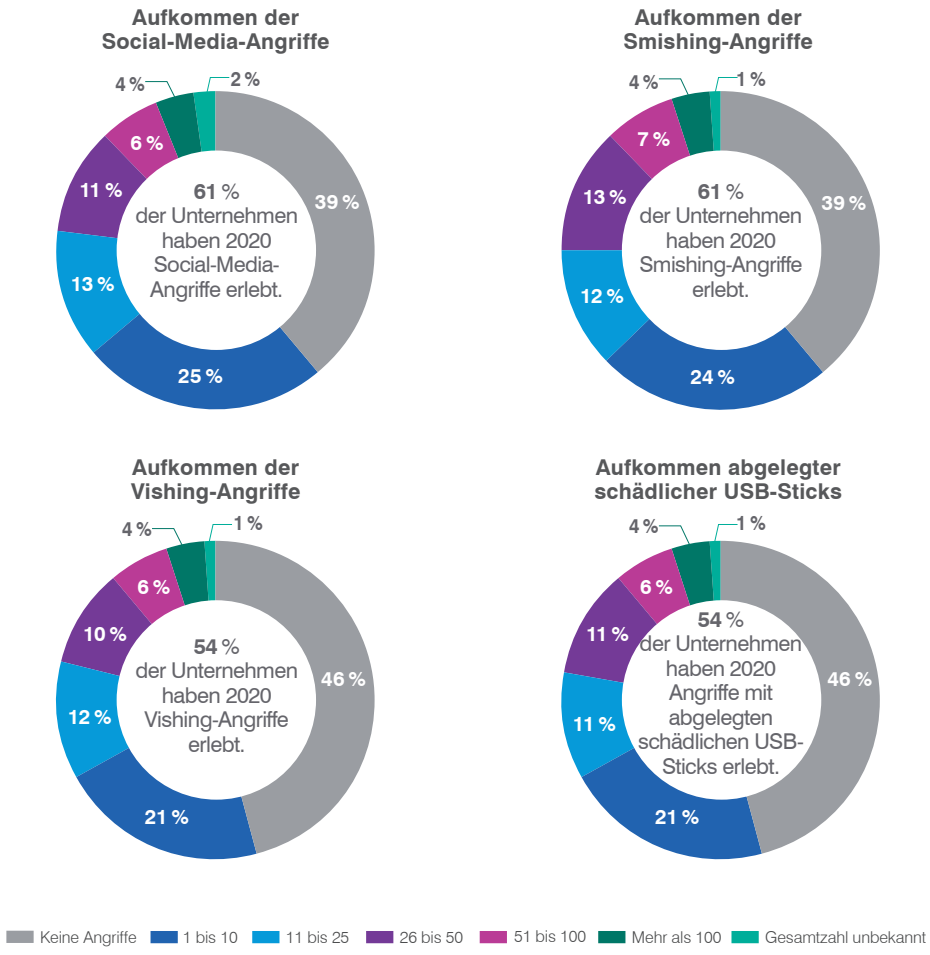


Abb. 3.

DIE FAKTEN

Bei französischen und japanischen Unternehmen kam es am seltensten zu Ransomware-Infektionen (**47 %** bzw. **46 %** gaben an, dass sie 2020 nicht von Ransomware-Angriffen betroffen waren). Sie zahlten nach einer Infektion auch am seltensten Lösegeld (jeweils **18 %**).

INTERNATIONAL

68 %

der US-Unternehmen gaben an, 2020 ein Lösegeld bezahlt zu haben (doppelt so viel wie der weltweite Durchschnitt).

41 %

der spanischen Unternehmen lehnte die Zahlung von Lösegeld nach einer Infektion ab und verhandelten am seltensten mit den Angreifern.

78 %

der französischen Unternehmen hatten nach der Zahlung eines einmaligen Lösegeldes das Glück, wieder Zugriff auf ihre Daten und Systeme zu erhalten. Das ist die höchste Zahl unter allen befragten Regionen (die USA lagen mit **76 %** auf Platz 2).

14 %

der deutschen Unternehmen lehnten die Zahlung eines Folgelösegeldes ab, der höchste Wert unter den untersuchten Regionen.

Ransomware: 2020 gingen mehr Unternehmen auf Lösegeldforderungen ein – mit gemischten Ergebnissen

Vielleicht kennen Sie den Spruch: „Diebe kennen keine Ehre.“ Zwei Drittel der Befragten gaben an, dass ihr Unternehmen 2020 mit Ransomware angegriffen wurde. Über die Hälfte von ihnen entschied sich für die Zahlung des geforderten Lösegeldes, um wieder auf die eigenen Systeme und Daten zugreifen zu können. Unsere Umfrageergebnisse zeigen jedoch, dass das oftmals nicht zu einer schnellen Lösung des Problems führte.

Wir befragten IT-Sicherheitsexperten zu ihren Erfahrungen mit Ransomware insgesamt (ob über Phishing-Angriffe oder andere Quellen). Daraus ergab sich Folgendes:

- 34 % der Unternehmen wurden infiziert und zahlten das Lösegeld (eine leichte Steigerung im Jahresvergleich).
- 32 % wurden infiziert, zahlten das Lösegeld jedoch nicht.
- 34 % gaben an, dass es bei ihnen 2020 nicht zu einer Ransomware-Infektion kam.

Bei vielen, die das Risiko einer Zahlung eingingen, bestätigte sich das Sprichwort und sie wurden im Ergebnis betrogen.

Auswirkungen von Ransomware-Zahlungen (2020 und 2019 im Vergleich)

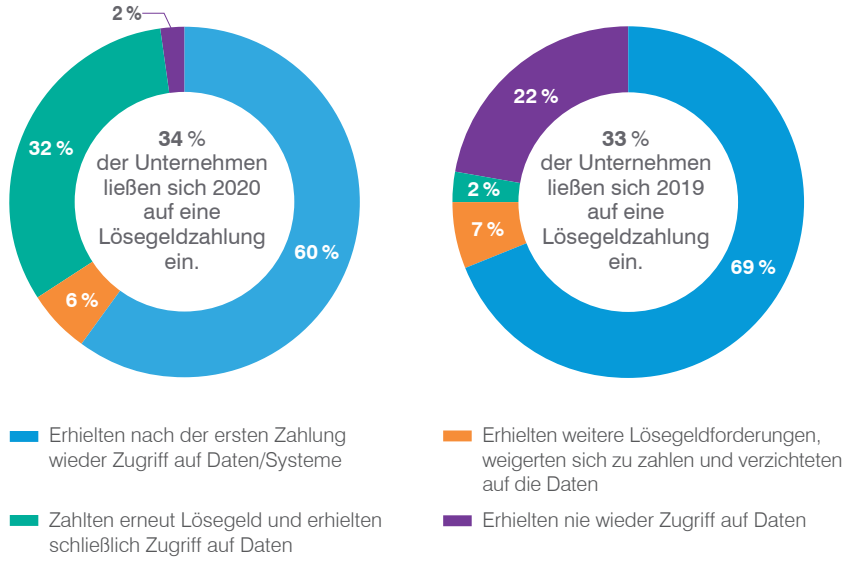


Abb. 4.

Wie im Jahresvergleich (Abb. 4) zu sehen ist, führte das Zahlen des Lösegeldes 2020 noch seltener zum gewünschten Ergebnis. Die Opfer, die 2020 zahlten, erhielten nach der ersten Zahlung seltener wieder Zugriff als im Jahr zuvor. Das ist an sich schon erschreckend. Noch erstaunlicher ist die Zunahme der Folge-Lösegeldforderungen und damit verbundener Aktionen:

- Die Zahl zusätzlicher Lösegeldforderungen nahm 2020 um 320 % zu.
- Im Jahr 2020 waren 32 % der Befragten bereit, zusätzliche Lösegelder zu bezahlen, im Vergleich zu 2 % im Jahr 2019 – was einer unglaublichen Steigerung von 1.500 % im Jahresvergleich entspricht.

Der einzige Lichtblick: Nur 8 % der Zahlenden standen nach den Verhandlungen mit den Angreifern mit leeren Händen da – das sind deutlich weniger die 29 % im letzten Jahr.

So schnitten die Anwender 2020 ab

11 %
durchschnittliche Fehlerquote bei Phishing-Tests 2020

33 %
durchschnittliche Anzeigerate aller simulierten Angriffe

Während des 12-monatigen Beobachtungszeitraums sendeten unsere Kunden ihren Anwendern über 60 Millionen Phishing-Tests und damit fast 15 Millionen mehr als 2019. Angesichts der heiklen Bedrohungslandschaft, mit der sowohl IT-Sicherheitsteams als auch die Anwender 2020 konfrontiert waren, stimmt es zuversichtlich, dass die Unternehmen ihren Aktivitäten für mehr Phishing-Sensibilisierung weiterhin Priorität einräumen.

Positiv ist außerdem, dass die durchschnittliche Fehlerquote in unserem aktuellsten Datensatz gesunken ist. Bei den Unternehmen kam es 2020 zu einer durchschnittlichen Fehlerquote von 11 % (verglichen mit 12 % im Jahr 2019).[3]

Der Durchschnittswert sagt jedoch nicht besonders viel über die Reaktion der Anwender bei verschiedenen Bedrohungsarten aus. Die Angreifer sind raffiniert und kreativ. Sie wechseln regelmäßig ihre Köder, um verschiedene Personen und Persönlichkeiten anzulocken. Deshalb ist es so wichtig, dass Unternehmen auf die gleiche Weise reagieren, d. h. sie müssen Tests und Schulungen so variieren, dass sie potenzielle Schwachstellen ermitteln und abbauen können.

Fehlerquoten nach Vorlagenart

Die meisten Tools für Phishing-Simulationen beinhalten anpassbare E-Mail-Vorlagen, mit denen Unternehmen verschiedene Phishing-Taktiken testen können. Unsere Kunden können aus einer Vielzahl von Themen und Ködern in drei Hauptvorlagenarten auswählen: Links, Dateneingaben und Anhänge. Wie schon in den zwei Jahren zuvor waren simulierte Angriffe mit URL-Hyperlinks auch 2020 mit Abstand am beliebtesten.

„Nicht bestandene" Dateneingabe-Tests beziehen sich auf Fälle, bei denen Anwender nach dem Klick auf einen Link im simulierten Angriff Daten übermittelten.

Arten der Phishing-Vorlagen: Häufigkeit der Nutzung

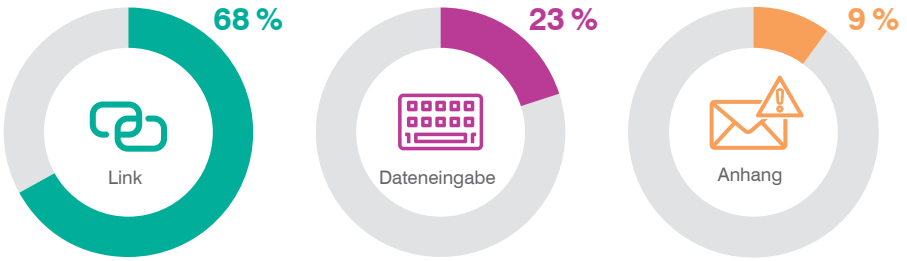


Abb. 5.

Arten der Phishing-Vorlagen: Durchschnittliche Fehlerquoten

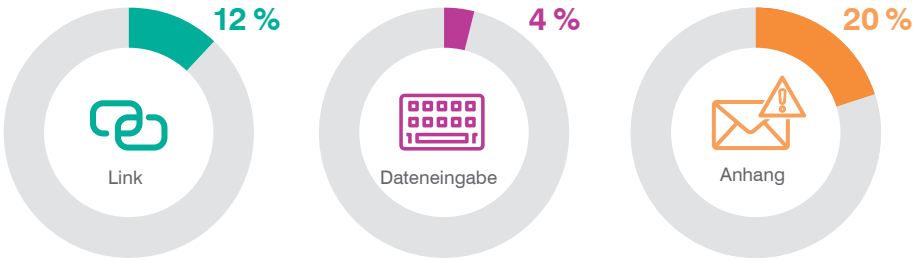


Abb. 6.

[3] Wir berechnen die durchschnittliche Fehlerquote auf Unternehmensebene und nicht auf Anwenderebene, wodurch die durchschnittliche Fehlerquote jedes einzelnen Unternehmens gewichtet wird, statt die Fehlerquote jedes Anwenders gleich zu gewichten. Dadurch können große Unternehmen und umfangreiche Programme die Ergebnisse nicht mehr verfälschen. Dies ermöglicht einen ausgewogeneren Blick auf die Fehlerdaten.

Dies steht im Einklang mit dem, was wir bei realen Angriffen beobachten. Link-basiertes Phishing ist deutlich stärker verbreitet als Anhang-basiertes Phishing. Zudem werden die Angreifer immer kreativer. Wir verzeichneten 2020 eine zunehmende Nutzung legitimer Dienste wie Microsoft 365, Google Drive, Constant Contact und SendGrid für Social-Engineering-Angriffe. Viele weit verbreitete und vertrauenswürdige Dienste generieren eigene URLs, die Anwender zum gehosteten Inhalt führen. Angreifer profitieren auf unterschiedliche Weise von diesem Ansatz:

- Diese Dienste gelten als legitime Geschäftsanwendung, sodass sich die URLs nur schwer (oder gar nicht) auf eine Blocklist verbannen lassen.
- Erkennungstechniken auf Basis der URL-/Domänen-Reputation können die URLs von Angreifern nicht eindeutig erkennen, sodass die Gefahr besteht, dass legitime Dienste blockieren werden.
- Mitarbeiter von Unternehmen sehen – und verwenden – diese Cloud-basierten Dienste oft. Durch diesen Bekanntheitsgrad entwickelt sich ein Vertrauen, das die Angreifer zu ihrem Vorteil ausnutzen können.

Wie jedoch in den Abbildungen 5 und 6 erkennbar ist, korrelieren positive Ergebnisse bei Link-basierten Tests nicht immer mit positiven Ergebnissen bei anderen Simulationsarten. Die Fehlerquote ist bei Anhang-basierten Tests beispielsweise sehr viel höher als bei URL-basierten Tests.

Fazit: Unternehmen sollten prüfen, ob sie in ausreichendem Maße testen, wie gut Anwender Anhang-basierte Phishing-Bedrohung erkennen und ihnen ausweichen. Zudem sollten sie berücksichtigen, dass ein Phishing-Test eben auch nur das ist: ein Test. Das chamäleonartige Wesen von Phishing-Angriffen erfordert eine flexible und aufgeschlossene Vorgehensweise beim Testen und Schulen der Anwender.

Ihren Anwendern werden wahrscheinlich verschiedenste Angriffe und Taktiken begegnen, sodass eine ausgewogene Vorgehensweise bei Phishing-Simulationen zu bevorzugen ist.

Die am meisten verwendeten und die raffiniertesten Themen der Kampagnenvorlagen

Unternehmen sollten Vorlagen für simulierte Phishing-Angriffe auswählen, die den echten Bedrohungen nachempfunden sind, mit denen ihre Anwender am ehesten konfrontiert sein werden. Beim Testen ihrer Anwender sollten sie die Elemente Kreativität und Überraschung jedoch nicht außer Acht lassen. Häufig sind es die „Sonderfälle“ unter den Themen, die am stärksten Aufschluss über Phishing-Aspekte geben, die Anwender noch nicht verstanden haben – sowie über Köder, bei denen die Verlockung zu groß ist, um sie zu ignorieren.

Deshalb folgt nun eine Liste der zehn am häufigsten verwendeten Themen und der Themen, die bei Phishing-Tests im Jahr 2020 am „erfolgreichsten“ waren. In beiden Kategorien wurden Vorlagen mit diesen Themen an mindestens 2.300 Anwender gesendet (und in manchen Fällen deutlich mehr).

Die meistverwendeten Themen

1. Neue Microsoft Teams-Anfragen
2. Coronavirus-Alarmmeldungen and Gesundheitswarnungen
3. Hinweis zum Ablaufen des Microsoft 365-Kennworts
4. Deaktivierung eines alten OneDrive-Kontos
5. Benachrichtigung über gemeinsamen OneDrive-Vertrag
6. Starbucks-Bonus
7. WHO-Sicherheitsinformationen zum Coronavirus
8. Hinweis auf neue Voicemail
9. Warnung über große Anzahl von Dateien, die vom OneDrive gelöscht werden
10. UPS-Versandbenachrichtigung

Die raffiniertesten Themen

1. Ein Monat kostenloses Netflix-Streaming für Mitarbeiter
2. Vertrag für Ferienvermietung
3. Starbucks Pumpkin Spice-Saison
4. Ticketvorverkauf für die Olympischen Sommerspiele 2020
5. Benachrichtigung über überfällige Rechnung
6. Aufforderung zur Aktualisierung des Spotify-Kennworts
7. Schuldschein
8. Verletzung der Kleiderordnung
9. Coronavirus-Maskenverfügbarkeit und Zahlungspläne für Unternehmen
10. Mitteilung über einen Verkehrsverstoß

Was ist mit den Fehlerquoten für diese Vorlagen? Die raffiniertesten Vorlagen hatten alle Fehlerquoten von fast 100 %. Dabei war der Köder mit dem Vertrag für die Ferienvermietung in mehreren Sprachen gleich erfolgreich. Im Vergleich dazu lag die höchste Fehlerquote unter den am häufigsten verwendeten Vorlagen bei 21 %.

Beachtenswert ist auch, dass sechs der raffiniertesten Vorlagen Anhang-basierte Tests waren. Bei den anderen vier handelte es sich um Link-basierte Tests. (Dateneingabe-Tests haben es nicht auf die Liste geschafft.)

Spotlight: Phishing mit Corona-Themen

Kein Bericht über das Jahr 2020 wäre vollständig, wenn er nicht Köder mit Coronavirus-Themen (und verwandten Themen) enthielte. Die Pandemie liefert eine lebende Fallstudie darüber, wie Angreifer thematisch aktuelle Angriffe ausführen, die sich aktuelle Probleme und Bedenken von Anwendern auf der ganzen Welt zu Nutze machen.

Von Januar bis Anfang Dezember 2020 blockierten wir Millionen von Phishing-E-Mails, die sich auf die Pandemie bezogen. Die Kombination aus sachbezogenen Botschaften und Massenverbreitung war beispiellos – ebenso wie das Jahr 2020 selbst.

Obwohl sich ihr Volumen seit einer Spitze im März/April 2020 verringert hat, profitieren die Angreifer weiterhin davon, dass die Menschen selbstverständlich Interesse an diesem Thema haben. Ende 2020 wechselten sie zu impfbezogenen E-Mail-basierten Ködern und Smishing-Angriffen (SMS-/Textnachrichten-Phishing), die sich auf Konjunkturpakete bezogen. Wir gehen davon aus, dass das Thema in künftigen Angriffen auffallend häufig vorkommen wird – und zwar so lange wie das Coronavirus weltweit die Schlagzeilen beherrscht.

Der anfängliche Anstieg der pandemiebezogenen Phishing-Angriffe fiel mit einem grundlegenden Wandel der Arbeitssituation zusammen, der sich bei enorm vielen Unternehmen weltweit vollzog. Diese Unternehmen – und ihre Anwender – betraten Neuland und bemühten sich dabei, den Geschäftsbetrieb in Umgebungen störungsfrei aufrechtzuerhalten, in denen es viele potenzielle Ablenkungen gab.

Einige unserer Kunden fragten zu diesem Zeitpunkt: Setzen wir die Schulungen zur Sensibilisierung für Sicherheit fort oder legen wir eine Pause ein? Unsere Antwort lautete: Angreifer kosten Veränderungen und Unsicherheiten voll aus. In Zeiten wie diesen sind Schulungen zur Sensibilisierung und Weiterbildung der Anwender unerlässlich – zudem bieten sie wichtige Einblicke in das Benutzerverhalten.

Die sich schnell ändernden Bedingungen bei Ausbruch der Pandemie zeigten nur noch einmal deutlich, wie wichtig Agilität ist. Um mit neuen Bedrohungen und den sich entwickelnden Ereignissen Schritt zu halten, bezogen Unternehmen schnell pandemiebezogene Tests und Schulungen ein. Dazu zählten Phishing-Simulationen mit Coronavirus-Bezug sowie Tipps für das sichere Arbeiten im Home Office.

Die Fehlerquote näherte sich für viele COVID-bezogene Tests den 100 %. Der Maskenköder in der Liste der raffiniertesten Themen auf Seite 10 war nur ein Beispiel. Andere Themen mit hohen Fehlerquoten nutzten die folgenden Betreffzeilen, die reale Betreffs von Phishing-Angriffen widerspiegeln:

- Singapur-Spezialist: Coronavirus-Sicherheitsmaßnahmen
- COVID-19-Krankenhausbesuch
- FBI-Warnung!!! Coronavirus-Betrug
- COVID-19 hat unsere Mitarbeiter infiziert

Insgesamt schnitten die Anwender jedoch bei Tests mit Coronavirus-Bezug gut ab. Angesichts der Tatsache, dass die meisten Köder mit Pandemiebezug mit weltweit verbreiteten Ängsten und Problemen spielten, ist das beeindruckend. Für Anwender, die mit den am häufigsten verwendeten COVID-bezogenen Vorlagen getestet wurden, reichten die durchschnittlichen Fehlerquoten von unter 1 % bis knapp über 20 %.

ABSCHNITT 2

Benchmark-Analyse: Daten zu Branchen und Abteilungen

DIE FAKTEN

Die Branchen mit den häufigsten Phishing-Tests waren im Jahr 2020 das Gesundheitswesen, der Finanzsektor, Fertigungsunternehmen, Energie- und Versorgungsunternehmen sowie der Technologiebereich.

Kunden fragen häufig nach Benchmark-Daten. Wir möchten, dass Unternehmen sich selbst und ihre Anwender noch detaillierter mit anderen Unternehmen und Anwendern vergleichen können. Deshalb bieten wir dieses Jahr eine größere Detailtiefe als je zuvor und haben Fehlerquoten für je 20 verschiedene Branchen und Abteilungen berücksichtigt.

Unter unseren Kunden waren es die Fertigungsunternehmen, bei denen das Durchschnittsvolumen an realen Phishing-Angriffen im Jahr 2020 am größten war. Andere Branchen mit großem Angriffsaufkommen waren Technologie-, Energie- und Versorgungsunternehmen, Einzelhändler und Finanzdienstleister. Zum Glück zählen vier dieser fünf Branchen zu denjenigen, die ihre Anwender am aktivsten testen. Die durchschnittliche Fehlerquote in jeder dieser Branchen entsprach dem Gesamtdurchschnitt von 11 %.

Jede in unserem Fehlerquotenvergleich aufgeführte Branche umfasst Daten von mindestens 15 Unternehmen sowie mindestens 150.000 simulierten Phishing-Angriffen.

Fehlerquoten nach Branche

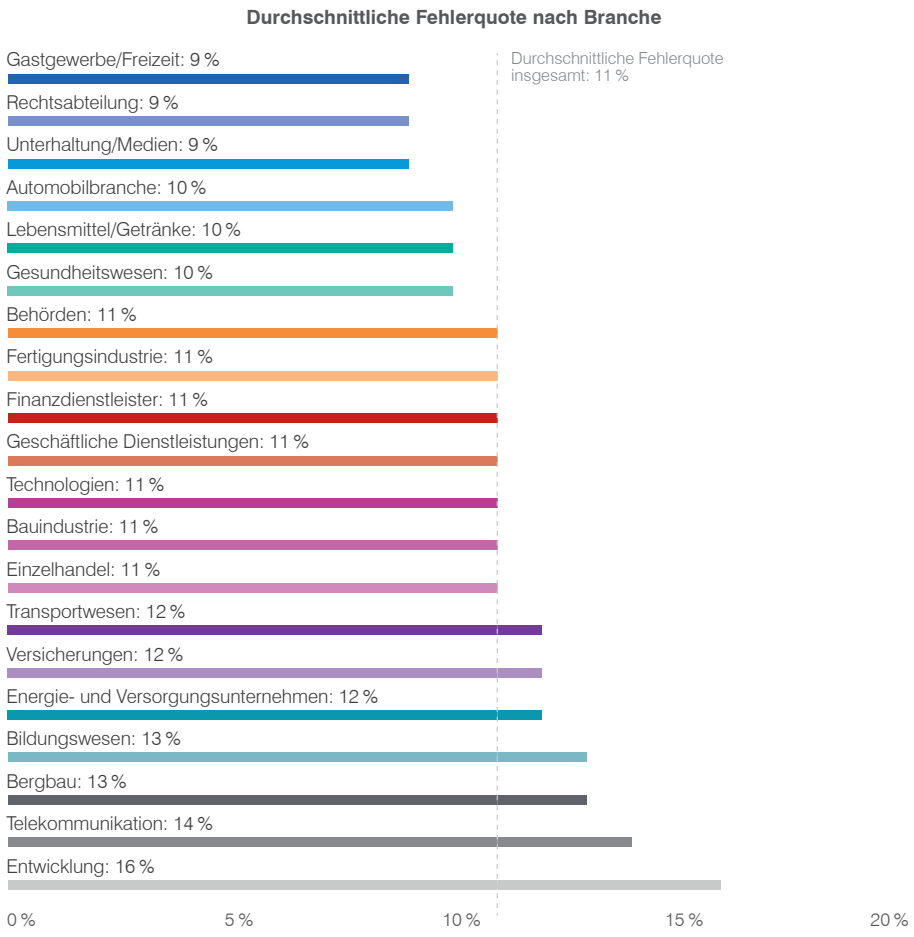


Abb. 7.

Beachtenswert: die weniger aktiven Branchen

Die aktivsten von uns analysierten Branchen sendeten ihren Anwendern im Jahr 2020 tausende Kampagnen und Millionen von Phishing-Tests. Natürlich ergeben sich einige dieser höheren Zahl aus einfacher Mathematik: mehr Unternehmen + mehr Anwender = mehr Tests.

Doch das ist nicht immer der Fall.

Im Durchschnitt sendete jedes Unternehmen in unserer Untersuchung im Jahr 2020 acht simulierte Phishing-Kampagnen. Die fünf aktivsten Branchen sendeten dabei sieben bis zehn Kampagnen.

Unternehmen in weniger aktiven Branchen – wie etwa Luft- und Raumfahrt, gemeinnützige Organisationen und die Immobilienbranche – sendeten hingegen nur vier oder fünf Kampagnen. Diese Branchen umfassten in unserer Probenzählung jeweils mindestens 15 Unternehmen, sendeten jedoch nicht genügend simulierte Phishing-Angriffe, um in unserem Vergleich der durchschnittlichen Fehlerquoten zu erscheinen.

Für die Beurteilung der Anfälligkeit von Anwendern für Phishing-Angriffe zählt die Anzahl der Touchpoints. Wenn Ihre Anwender mit nur wenigen simulierten Angriffen pro Jahr testen, erhalten Sie keine relevanten Ergebnisse. Angreifer sind rund um die Uhr auf der Jagd. Wir empfehlen Tests alle vier bis sechs Wochen mit einer Vielfalt an Ködern. So verschaffen Sie sich den besten Eindruck davon, wie Anwender auf verschiedene Arten von Phishing-Bedrohungen reagieren.

Fehlerquoten nach Abteilung

Die in unserem Fehlerquotenvergleich vertretenen Abteilungsbezeichnungen wurden von mindestens 40 Unternehmen verwendet und enthalten Daten zu mindestens 1.500 Anwendern.

Fehlerquoten auf Abteilungsebene bieten einen detaillierten Überblick über potenzielle Schwachstellen im Unternehmen. Angreifer nehmen häufig einzelne Posteingänge und E-Mail-Aliase ins Visier. Eine Fehlerquote auf Unternehmensebene allein legt nicht offen, bei welchen Rollen und Teams möglicherweise Probleme auftreten.

Leider gruppieren Unternehmen ihre Mitarbeiter in ihren Berichten nur selten nach Abteilungen. Ohne diese Einblicke können sie die Leistung (und Anfälligkeit) bezogen auf den Tätigkeitsbereich nicht schnell und regelmäßig beurteilen.

DIE FAKTEN

Im Bericht des vergangenen Jahres schnitt die Abteilung „Forschung und Entwicklung“ mit einer durchschnittlichen Fehlerquote von **20 %** am schlechtesten ab. Die diesjährige durchschnittliche Fehlerquote von **8 %** stellt eine Verbesserung von **60 %** im Jahresvergleich dar.

Mit **11 %** blieb die durchschnittliche Fehlerquote für den Vertrieb in diesem Jahr stabil und entspricht der übergreifenden durchschnittliche Fehlerquote. Diese Gruppe muss jedoch aufmerksam beobachtet werden, denn E-Mail-Aliase sind im Vertrieb häufig das Ziel von Angreifern.

In Abb. 8 sehen Sie einen Vergleich der durchschnittlichen Fehlerquoten von 20 verschiedenen Abteilungen in aufsteigender Reihenfolge.[4]

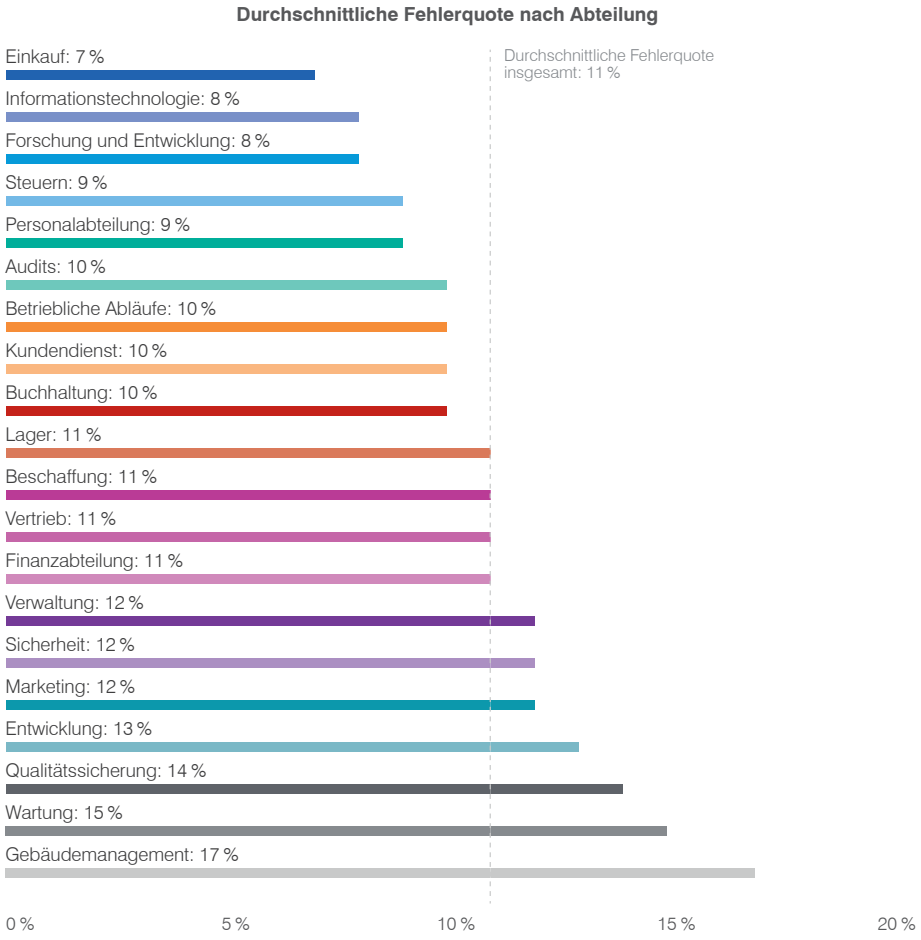


Abb. 8.

Es ist erfreulich, dass so viele Abteilungen bessere Werte erzielen als die 11 % der allgemeinen durchschnittlichen Fehlerquote. Es sind jedoch die schlechter abschneidenden Gruppen, die wirklich zeigen, wie wichtig der Einblick in die Phishing-Testergebnisse auf Abteilungsebene ist. Die allgemeine durchschnittliche Fehlerquote ist zwar nützlich, entscheidend ist jedoch die Erkenntnis, welche Rollen und Abteilungen das Ziel nicht erreichen – ganz besonders dann, wenn es deutlich verfehlt wird.

[4] Beachten Sie, dass unsere Kunden die Abteilungsbezeichnungen in ihren Daten selbst auswählen. Deshalb können ähnliche Bezeichnungen in verschiedenen Unternehmen etwas anderes bedeuten. So überschneiden sich beispielsweise „Gebäudemanagement“ und „Wartung“ in einem Unternehmen, haben aber in einem anderen unterschiedliche Bezeichnungen.

ABSCHNITT 3

Wichtige Zahlen: Anteil gemeldeter E-Mails und Resilienzverhältnis

PhishAlarm-Kunden verzeichneten eine durchschnittliche Meldungsrate von **13 %** bei Phishing-Tests.

Jeder PhishAlarm-Anwender meldete durchschnittlich **5** E-Mails.

Wenn Sie die *State of the Phish*-Berichte der letzten Jahre gelesen haben, wissen Sie, dass wir großen Wert auf E-Mail-Meldungen legen. Wir empfehlen allen unseren Kunden dringend, unser in den Client integriertes Meldetool PhishAlarm® einzusetzen, das folgende Vorteile bietet:

- Mitarbeiter können sichere Verhaltensweisen für E-Mails anwenden und sich aktiv an Ihren Sicherheitsbemühungen beteiligen.
- Mitarbeiter können die zuständigen Mitglieder des IT-Sicherheitsteams bei verdächtigen E-Mails schnell und einfach warnen.
- Ihre Sicherheitskultur wird verbessert, da eine engere Zusammenarbeit zwischen Anwendern und Sicherheitsteams gefördert wird.
- Fehlerquoten und Meldungsraten werden korreliert, sodass Sie die Resilienz (also die Widerstandsfähigkeit) quantitativ bestimmen können.
- Sie erhalten Einblicke darin, welche Arten von realen Bedrohungen Perimeter-Schutzmaßnahmen umgehen.
- Sie können Berichts- und Behebungsfunktionen integrieren, um aktive Bedrohungen im Netzwerk schnell zu erkennen und zu beseitigen.

Insgesamt ist unser neuester Meldedatensatz größer als je zuvor. Die Mitarbeiter unserer Kunden meldeten im Laufe unseres 12-monatigen Erfassungszeitraums über 15 Millionen E-Mails. Die allgemeine durchschnittliche Meldungsrate simulierter Phishing-Angriffe betrug 13 %. (Wir betrachten die Anwendermeldungen realer Bedrohungen weiter unten in diesem Abschnitt.)

Was bedeutet das Resilienzverhältnis?

PhishAlarm-Kunden erzielten einen durchschnittlichen Resilienzfaktor von 1,2.

Im vergangenen Jahr erörterten wir die 70/5-Regel als Fernziel für Unternehmen, die sowohl die Meldungsraten als auch die Fehlerquoten bei ihren simulierten Phishing-Angriffen verfolgen. Dieses angestrebte Resilienzverhältnis – eine Gesamtmeldungsrate von 70 % oder höher in Verbindung mit einer Fehlerquote von 5 % oder weniger – führt zu einem Resilienzfaktor von 14. Unternehmen, die dieses Resilienzniveau erzielen und – ganz wichtig – auch halten, erreichen einen traumhaften Zustand, in dem Anwender 14-mal häufiger eine Phishing-E-Mail melden als damit zu interagieren.

Unternehmen, die PhishAlarm verwenden, haben mit der Implementierung eines integrierten Meldemechanismus bereits den notwendigen ersten Schritt getan. Ihre durchschnittliche Meldungsrate übersteigt bereits die durchschnittliche Fehlerquote, sodass sich ein positiver Resilienzfaktor ergibt:

13 % durchschnittliche Meldungsrate ÷ 11 % durchschnittliche Fehlerquote = 1,2 Resilienzfaktor

Das ist nicht das ideale Resilienzverhältnis. Ein Resilienzfaktor von über 1 bedeutet jedoch, dass bereits mehr Anwender E-Mails melden als darauf hereinzufallen. Angesichts der Tatsache, dass Meldetools wie PhishAlarm noch neu sind, ist noch viel Verbesserungsspielraum vorhanden.

Benchmarking: branchenspezifische Resilienzfaktoren

Sie möchten nun möglicherweise den durchschnittlichen Resilienzfaktor Ihres Unternehmens mit anderen Unternehmen Ihrer Branche vergleichen. In Tabelle 1 sind die durchschnittlichen Meldungsraten, die durchschnittlichen Fehlerquoten und die Resilienzfaktoren für die in Abb. 7 dargestellten 20 Branchen aufgeführt.

Die durchschnittlichen Fehlerquoten in Tabelle 1 unterscheiden sich leicht von den Werten in Abb. 7. Die Quoten in diesem Abschnitt basieren auf Daten von Kunden, die sowohl unsere Tools für simulierte Phishing-Angriffe als auch unsere Melde-Schaltfläche verwenden. Somit beziehen sie sich auf eine Teilmenge der vorher genutzten Daten.

Durchschnittliche Fehlerquote, durchschnittliche Meldungsrate und durchschnittlicher Resilienzfaktor nach Branche

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
Entwicklung	16 %	16 %	1,0
Automobilbranche	15 %	8 %	1,9
Geschäftliche Dienstleistungen	14 %	11 %	1,3
Technologien	13 %	12 %	1,1
Behörden	13 %	10 %	1,3
Bergbau	13 %	13 %	1,0
Lebensmittel/Getränke	11 %	11 %	1,0
Fertigungsindustrie	10 %	10 %	1,0
Gesundheitswesen	10 %	10 %	1,0
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
Bildungswesen	6 %	12 %	-2,0
Gastgewerbe/Freizeit	5 %	10 %	-2,0

Tabelle 1.

Mehrere Branchen übertreffen den durchschnittlichen Resilienzfaktor von 1,2 deutlich. Die Rechts- und die Automobilbranche übernehmen mit etwa doppelt so vielen Meldungen wie Fehlern die Führung.

Wir sehen jedoch auch, dass mehrere Branchen deutlich unterhalb des Durchschnitts liegen, darunter sogar einige mit negativen Resilienzfaktoren (mehr Fehler als Meldungen). Dies kann verschiedene Gründe haben, darunter unausgereifte Programme, unzureichende kontinuierliche Weiterbildung oder die Fokussierung auf schwierige Phishing-Tests. Alle drei Aspekte können zu höheren Fehlerquoten und niedrigeren Resilienzfaktoren führen.

Die Zahlen veranschaulichen gut den Vorteil der Kombination aus starker Meldungsrate und geringer Fehlerquote bei allen Arten von Phishing-Tests. Dabei ist ein hoher Resilienzquotient (wie die 14, die wir als Fernziel empfehlen) nicht ausgeschlossen. Natürlich ist er bei Einzelkampagnen eher erreichbar, doch wir haben auch Kunden, die übergreifend über mehrere Kampagnen mit 40.000 bis nahezu 100.000 simulierten Phishing-E-Mails deutlich höhere Resilienzfaktoren von 24 und 60 erhalten.

Wenn andere das können, schaffen Sie es auch. Und wenn Sie es einmal können, dann können Sie es auch wieder (und wieder…).

Spotlight: Anwender meldeten im Jahr 2020 aktiv reale Angriffe

Unsere PhishAlarm-Schaltfläche funktioniert in Verbindung mit PhishAlarm Analyzer. Das Tool nutzt Proofpoint-Bedrohungsdaten zur Echtzeit-Identifizierung von Phishing-Angriffen. Die Inhalte der über PhishAlarm gemeldeten E-Mails werden von Proofpoint-Bewertungsmodulen gescannt und alle URLs und Anhänge werden in unserer Sandbox live ausgeführt. Dabei werden 60 bis 80 % der gemeldeten E-Mails automatisch einer finalen Klassifizierung als entweder schädlich/Spam oder Massenmail/harmlos zugeordnet.

Im Laufe unseres einjährigen Erfassungszeitraums ergab unsere Analyse Folgendes:

- Anwender meldeten über fünf Millionen reale verdächtige Nachrichten.
- Fast 800.000 der gemeldeten E-Mails wurden als „bekannt gefährlich“ (schädlich oder Spam) eingestuft.[5]
- Über 200.000 Nachrichten waren aktive Anmeldedaten-Phishing-Angriffe.
- Mehr als 35.000 gemeldete E-Mails enthielten Malware-Schaddaten.
- Fast zwei Millionen gemeldete Nachrichten wurden umgehend automatisch als Massenmails/E-Mails mit geringem Risiko klassifiziert, sodass Sicherheitsteams damit nicht ihre Zeit vergeuden mussten.

Diese Statistik zeigt den immensen Nutzen, der sich ergibt, wenn Mitarbeiter die IT-Sicherheitsteams über verdächtige Nachrichten informieren können. Anwender ermitteln und melden aktiv Anmeldedaten-Phishing-Angriffe und Malware. Die Malware kann in Form eines Anhangs oder einer URL versendet werden. Zu den so verbreiteten Schaddaten zählen Remote-Zugriffs-Trojaner (RATs), Keylogger, Downloader und sogar Schadcode von hochentwickelten permanenten Bedrohungen (Advanced Persistent Threats, APTs).

Viele Unternehmen sorgen sich möglicherweise wegen der Arbeitsbelastung für ihr IT-Sicherheitsteam, die eine Meldeschaltfläche verursachen kann. Wir empfehlen die Wahl eines Tools mit integrierten Melde-, Analyse- und Behebungsfunktionen wie unsere Lösung Closed-Loop Email Analysis and Response (CLEAR). Mit den richtigen Integrationen können als schädlich oder Spam gekennzeichnete E-Mails am E-Mail-Gateway automatisch unter Quarantäne gestellt, entschärft oder blockiert werden. Die Integration verringert zudem das Rauschen sicherer E-Mails, die Anwender eventuell fälschlicherweise melden.

Durch diesen Ansatz können Sie das Potenzial anwenderbasierter Meldungen voll ausschöpfen, ohne dadurch Ihre Behebungs- und Reaktionsteams zu überfordern. Sie erhalten zudem wertvolle Informationen zu Endnutzer- und Awareness-Schulungen, zum Beispiel:

- Welche Anwender setzen ihre Kenntnisse effektiv in die Praxis um, indem sie verdächtige und schädliche E-Mails melden?
- Welche Anwender können ihr Wissen nicht in der Praxis anwenden? Dazu können Anwender zählen, die zwar simulierte Phishing-E-Mails erkennen, aber nicht die richtigen. Oder es kann sich um Anwender handeln, die E-Mails wahllos als sicher oder unsicher kennzeichnen. Es können sogar Anwender sein, die scheinbar sorgfältiger sind, jedoch E-Mails melden, die keine Warnzeichen für schädliche Absichten aufweisen.
- Welche Arten von aktiven Angriffen umgehen die Perimeter-Schutzmaßnahmen? Mit dieser Information können Sie technischen Schutzmaßnahmen, Phishing-Tests und Schulungspläne noch detaillierter abstimmen.

[5] Der Prozentsatz der „bekannt gefährlichen“ gemeldeten Nachrichten variierte stark je nach eingesetztem sicherem E-Mail-Gateway. Im Durchschnitt verzeichneten Proofpoint-Kunden bessere Blockierraten als vor der Bereitstellung, sodass die Endnutzer weniger schädliche E-Mails melden mussten.

ABSCHNITT 4

Bedrohungsdaten: Identifizieren der Very Attacked People

Wir messen das Anwenderrisiko mit dem VAP-Modell, das Schwachstellen, Angriffe und Zugriffsrechte berücksichtigt. Das VAP-Modell bewertet nicht nur, wie Ihre Anwender angegriffen werden, sondern auch die Wahrscheinlichkeit, mit der diese Anwender auf einen Angriff hereinfallen, sowie die potenziellen Auswirkungen eines erfolgreichen Angriffs. Eine VAP-Ansicht des Anwenderrisikos kann dabei helfen, eine sehr kritische Lage zu erkennen, die sich unter der Oberfläche zusammenbraut: Anwender mit privilegiertem Zugriff, die für Angriffe anfällig sind und aktiv angegriffen werden. VAPs sind Risiken, die Sie kennen und auf die sie eingehen sollten.

Heutige Angriffe richten sich nicht mehr ausschließlich gegen Infrastruktur, sondern vor allem gegen Menschen. Deshalb setzen wir auf einen personenzentrierten Ansatz für Cybersicherheit und raten Unternehmen, dies ebenfalls zu tun.

Wenn Sie Ihre Mitarbeiter in den Mittelpunkt setzen, tragen Sie nicht nur der wichtigen Rolle Ihrer Mitarbeiter für Ihre Sicherheitslage Rechnung. Diese Erkenntnis hat sich inzwischen – wenn auch mit Verspätung – auf dem Markt für Cybersicherheit allgemein durchgesetzt. Es geht auch darum zu wissen, welche Anwender aufgrund der individuellen Faktorenkombination ein erhöhtes Risiko darstellen – und dieses Risiko zu verringern.

Wir analysieren eingehende Bedrohungen, um zu ermitteln, wer die Personen sind, die wir als Very Attacked People bzw. VAPs bezeichnen. Dazu gehören die Mitarbeiter und Alias-Posteingänge in Ihrem Unternehmen, die am aktivsten und intensivsten angegriffen werden. Unsere Analyse zeigt nicht nur, welche Anwender und Gruppen die Angreifer erreichen wollen, sondern auch die Methoden, Tools und Taktiken, die sie zu ihrer Kompromittierung anwenden.

Diese Art der Bedrohungsanalyse liefert sowohl auf der übergeordneten Ebene (unternehmensweit) als auch im Detailbereich (nach Abteilungen und pro Kampagne) umfangreiche Kontextinformationen für Fehlerquoten und Meldungsraten. Durch die Korrelation Ihrer Test- und Performance-Daten mit realen Angriffsdaten können Sie Ihren Plan für die Durchführung gezielter Schulungen für Personen erarbeiten, die Angreifer als sehr lohnenswerte Ziele ansehen.

Doch genau wie Tests und Schulungen ist auch die Ermittlung der VAPs keine einmalige Angelegenheit. Die VAPs ändern sich im Laufe der Zeit. In vielen Unternehmen verändert sich die Liste der Top-20-Angriffsziele jeden Monat.

Sie sollten sich also jegliche Mutmaßungen darüber sparen, wer wahrscheinlich ein VAP sein könnte. Die Ziele können sich nicht nur je nach Branche und Unternehmen unterscheiden. Manchmal sind Ihre hochkarätigen VIPs auch VAPs. Genauso häufig – unter Umständen sogar häufiger – werden aber auch Personen und E-Mail-Aliase das Ziel der Angreifer, die keine VIPs sind.

Unternehmen bestimmen ihre VIPs auf unseren Plattformen selbst. Einige markieren nur die Mitglieder der obersten Führungsebene als VIPs, während andere die Angelegenheit umfassender betrachten und Faktoren wie Sichtbarkeit, Zugriffsrechte und Zuständigkeiten und nicht nur Stellenbezeichnungen berücksichtigen.

Über einen Zeitraum von drei Monaten analysierten wir die Top 20 der VAPs bei einem großen Finanzdienstleister und einer großen regionalen Krankenhausgruppe. Unsere Ergebnisse zeigen, vor welchen Herausforderungen Unternehmen bei dem Versuch stehen, den Überblick über die sich verändernden Angriffsmethoden zu behalten:

Finanzdienstleister

- Im Laufe von drei Monaten wurde nur ein VIP Ziel eines Angriffs, aber diese Person (ein Manager der internationalen Finanzgruppe des Unternehmens) zählte durchgängig zu den drei am häufigsten angegriffenen Personen.
- Nur eine weitere Person – der CEO eines angeschlossenen globalen Zahlungsanbieters – war mehrfach in den Top 20 vertreten. Er war über zwei der drei Monate eine der am häufigsten angegriffenen Personen.
- Angreifer versuchten durchgängig, schädliche Nachrichten an Alias-Posteingänge zuzustellen. Eine allgemeine Kundendienstadresse war während aller drei untersuchten Monate das wichtigste Ziel.
- Über den CEO hinaus wurden E-Mail-Adressen, die zum angeschlossenen globalen Zahlungsanbieter gehörten, in allen drei Monaten häufig zum Angriffsziel. Im zweiten Monat des beobachteten Zeitraums waren 16 der Top-20-VAPs sogar Posteingänge dieses angeschlossenen Unternehmens. Angreifer versuchten, Phishing-E-Mails an Aliase und Einzelpersonen zuzustellen, darunter Personen im Bereich Business Development, im Point-of-Sales-Management und dem Compliance-Bereich für Finanzkriminalität.

Krankenhausgruppe

- Im ersten Beobachtungsmonat gehörte die Hälfte der 20 am häufigsten angegriffenen Personen der Organisation zu den VIPs. Im zweiten Monat verringerte sich diese Zahl auf sieben und im dritten Monat war nur noch ein VIP in den Top 20 vertreten.
- Nur der Finanzdirektor (ein VIP) blieb alle drei Monate in den Top 20.
- Die Angreifer versuchten in den beobachteten drei Monaten, VIPs über mehrere E-Mail-Konten zu erreichen. Im ersten Monat waren beispielsweise drei Adressen für den CEO unter den Top 20, gleichzeitig versuchten Angreifer, den Senior Vice President Operations über zwei verschiedene Adressen zu erreichen.
- Im dritten Monat wurden die Posteingänge mehrerer Personen angegriffen, die nicht mehr im Unternehmen beschäftigt waren. Dazu zählten zwei vorherige Mitglieder der Unternehmensführung und ein früherer Director of Business Development.
- Auch medizinisches Fachpersonal landete in den Top 20. Mehrere Krankenpfleger, Ärzte und Spezialpflegekräfte – darunter ein Spezialkrankenpfleger für Infektionskontrolle und eine Pflegekraft für Krisenfälle – wurden häufig genug angegriffen, um während des dreimonatigen Untersuchungszeitraums in den Top 20 zu erscheinen.

Der Vergleich der VAP-Indikatoren über den gesamten Dreimonatszeitraum verdeutlicht die individuelle Bedrohungslandschaft jeder Organisation. Darüber hinaus sind auch die Anwender der Organisationen bzw. Unternehmen einzigartig. Das gilt auch für den Wert, den sie für die Angreifer haben. Die Intensität und Vorgehensweise kann von Monat zu Monat – häufig sehr – unterschiedlich sein.

Der Einblick in diese Arten von Angriffsmerkmalen und die Trends und Ziele, die sie repräsentieren können, kann äußerst nützlich sein. Das gilt auch für Wissenstests und Schulungen, die speziell auf potenzielle Risiken zugeschnitten sind, die bestimmte VAPs mit sich bringen.

ABSCHNITT 5

Personenzentrierte Sicherheit: Der aktuelle Stand bei Schulungen zur Steigerung des Sicherheitsbewusstseins

Der *State of the Phish*-Bericht wäre ohne das Thema Schulungen zur Steigerung des Sicherheitsbewusstseins nicht vollständig. Diese Schulungen zur Sensibilisierung für Sicherheit sind ein unverzichtbarer Bestandteil mehrschichtiger Cybersicherheit. Wenn Unternehmen ihre Mitarbeiter nicht regelmäßig und gezielt in ihre Sicherheitsmaßnahmen einbeziehen, ignorieren sie damit die Zielgruppe der Angreifer.

Ansatzpunkt Terminologie

In den „Was ist"-Fragen unserer Umfrage konnten die Anwender zwischen drei Multiple-Choice-Antworten und einer „Weiß nicht"-Option wählen. Nutzer, die eine Antwort nicht kennen, stellen eine ebenso große Gefahr dar wie falsch antwortende.

Berufstätige Erwachsene wurden nach dem Multiple-Choice-Verfahren nach den Definitionen von Cybersicherheitsbegriffen gefragt. Die Herangehensweise mag trivial erscheinen, die Ergebnisse haben es jedoch in sich.

Die gute Nachricht: Außer bei Malware ist das Wissen um die auf Seite 21 aufgeführten Begriffe unter den Arbeitstätigen im Vergleich zum letzten Jahr gewachsen. Bei Malware hingegen ist das Wissen um 1 Prozent gesunken und blieb damit praktisch konstant.

Die Erkenntnisse dieses Jahres zeigen jedoch auch, dass Sie nie davon ausgehen sollten, dass Ihre Anwender die Cybersicherheitsbegriffe kennen, die Sie regelmäßig nutzen. Andernfalls kann das Ihre Sicherheitsschulungen ernstlich behindern.

In gewisser Weise lässt sich das Problem mit einem Arztbesuch vergleichen. Der durchschnittliche Patient ist nicht besonders bewandert mit medizinischen Fachbegriffen. Wenn ein Arzt Testergebnisse in einem Jargon vorstellt, den der Patient nicht kennt, wird dieser weniger wahrscheinlich die richtige Behandlung suchen oder notwendige Veränderungen angehen – selbst wenn sich das Problem eigentlich leicht beheben lässt.

Stellen Sie sich Ihre Anwender als Ihre Patienten vor. Viele der Schutzmaßnahmen, die sie anwenden sollen, sind nicht kompliziert. Doch wenn Sie von Anfang an die Aufmerksamkeit Ihrer Anwender verlieren, weil Sie eine ganz andere Sprache sprechen, werden diese sich wohl kaum die richtigen Verhaltensweisen angewöhnen.

Was ist
PHISHING?

Richtig **63 %**

Falsch **22 %**

Weiß nicht **15 %**

Mit 52 % haben US-Angestellte am wenigsten richtig geantwortet (wobei sich die Zahl gegenüber 49 % im Jahr 2019 verbessert hat).

69 % der Angestellten in Großbritannien kannten den Begriff. Keine andere von uns untersuchte Region kam auf einen so hohen Wert.

Was ist
RANSOMWARE?

Richtig **33 %**

Falsch **36 %**

Weiß nicht **31 %**

Die Zahl der richtigen Antworten ist im Vergleich zu den 31 % des letzten Jahres gestiegen – die der falschen Antworten aber auch (ebenfalls 31 % in unserer letzten Umfrage).

Nur 26 % der deutschen Angestellten beantworteten diese Frage richtig. Im Vergleich dazu haben 42 % der australischen Teilnehmer die richtige Antwort ausgewählt.

Was ist
MALWARE?

Richtig **65 %**

Falsch **21 %**

Weiß nicht **14 %**

Mit 75 % richtigen Antworten lagen spanische Angestellte vor allen anderen Regionen (obwohl das ein Rückgang im Vergleich zu den 80 % des letzten Jahres ist).

US-Teilnehmer lagen unter dem weltweiten Durchschnitt: Nur 54 % antworteten richtig, während fast 40 % die falsche Antwort wählten.

Was ist
SMISHING?

Richtig **31 %**

Falsch **25 %**

Weiß nicht **44 %**

Mit 60 % richtigen Antworten haben Angestellte in Frankreich wieder einmal die beste Leistung abgeliefert und den Wert des Vorjahres (54 %) deutlich übertroffen.

Japanische Angestellte lieferten im Vergleich zum weltweiten Durchschnitt einen sehr schlechten Wert ab: Nur 19 % beantworteten die Frage richtig – und 56 % waren sich nicht sicher.

Was ist
VISHING?

Richtig **30 %**

Falsch **22 %**

Weiß nicht **48 %**

Im vergangenen Jahr konnten nur 25 % der Angestellten in aller Welt diese Frage richtig beantworten. Seit unserer Umfrage des Jahres 2018 ist das Wissen um fast 70 % gestiegen.

Französische Angestellte verbesserten ihren Wert erneut. Mit 54 % richtigen Antworten lagen sie dreimal so hoch wie Angestellte in Deutschland (18 %).

INTERNATIONAL

Beste Ergebnisse

92 %
der japanischen Angestellten wissen, dass private E-Mail-Anbieter nicht alle gefährlichen Nachrichten blockieren können.

90 %
der Angestellten in Japan wissen, dass bekannte Logos in E-Mails kein Hinweis auf ihre Sicherheit sind.

65 %
der deutschen Angestellten verstehen, dass die E-Mail-Absenderdaten gefälscht sein können.

64 %
der Teilnehmer aus Spanien wissen, dass Anhänge mit Malware infiziert sein können.

60 %
der Angestellten in Spanien und Australien wissen, dass sie bei allen unerwarteten E-Mails vorsichtig sein sollen.

VS.

Schlechteste Ergebnisse

34 %
der US-Teilnehmer glauben, E-Mails mit bekannten Logos wären sicher.

30 %
der japanischen Angestellten wissen, dass der Absender einer E-Mail gefälscht sein kann.

22 %
der Umfrageteilnehmer in Australien und Spanien gehen davon aus, dass ihr Unternehmen alle gefährlichen E-Mails automatisch blockieren wird.

15 %
der Befragten in Japan konnten nicht sicher sagen, ob eine dieser Aussagen wahr oder falsch ist.

Knackpunkt E-Mail

In diesem Jahr setzten wir unseren Umfrageteilnehmern einen neuen Fragenkomplex vor: Was wissen sie über E-Mails? Wir wollten nicht nur wissen, ob sie Phishing definieren können, sondern auch, ob sie die Funktionsweise von E-Mail kennen und verstehen, wie sie in ihrem E-Mail-Client dargestellt wird. Dabei haben wir vielversprechende Ergebnisse gefunden.

Ergebnisse der Umfrage zu E-Mails

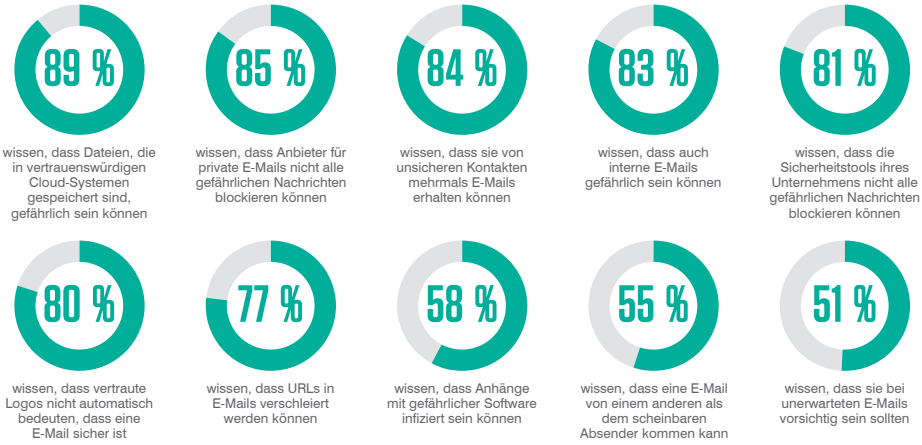


Abb. 9.

Nur 8 % der weltweiten Umfrageteilnehmer trauten sich nicht zu, mindestens eine Auswahl aus unserer Liste zu treffen. Wir freuen uns, dass mehr als drei Viertel der Befragten viele Gefahrenanzeichen richtig erkennen.

Natürlich gibt es Verbesserungsmöglichkeiten, insbesondere beim Erkennen von Spoofing und beim Umgang mit Anhängen und unerwünschten Nachrichten. Letztendlich sollten idealerweise 100 % der Anwender wissen, dass technische E-Mail-Schutzmaßnahmen niemals absolut sicher sind. Diejenigen, die das nicht wissen, stellen für Ihr Unternehmen ein großes Risiko dar.

Wer nutzt die Geräte Ihres Unternehmens?

Wir befragten Anwender über ihre privaten Gewohnheiten und Verhaltensweisen bei der Nutzung von Computern und Smartphones, die ihnen von ihrem Arbeitgeber gestellt werden. Dieser Fragenkomplex war im Jahr 2020 wichtiger als je zuvor.

Mehr als 80 % der von uns befragten IT-Sicherheitsexperten erklärten, dass ihre Unternehmen im vergangenen Jahr von mindestens der Hälfte ihrer Angestellten wünschten oder forderten, im Home Office zu arbeiten. Bei einigen Unternehmen erfolgte dieser Wechsel abrupt – und sorgte dafür, dass Geräte in potenziell unsicheren Umgebungen genutzt wurden.

Da so viele Angestellte – und ihre Mitbewohner und Familienmitglieder – an ihre Wohnung gefesselt sind, wollten wir wissen: Hat das Auswirkungen auf die private und gemeinsame Nutzung vom Unternehmen gestellter Geräte?

DIE FAKTEN

Mehr als **50 %** der Arbeitnehmer mit vom Unternehmen gestellten Geräten stellen diese Freunden und Familienmitgliedern zur Verfügung.

INTERNATIONAL

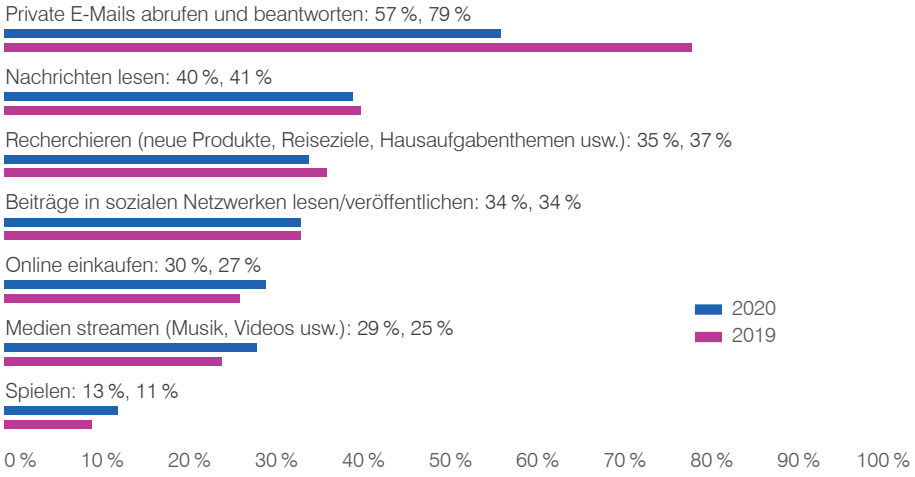
75 %

der US-Teilnehmer gewähren Freunden und Familienmitgliedern Zugang zu Geräten des Arbeitgebers. Dies ist erheblich mehr als in anderen Regionen und stellt einen Anstieg gegenüber 2019 (**71 %**) dar.

Bei Angestellten waren die Ergebnisse gemischt: Einige Verhaltensweisen (z. B. Abrufen privater E-Mails, Lesen von Nachrichten und Recherche) sind im Vorjahresvergleich zurückgegangen, während andere (wie Online-Shopping, Medien-Streaming und Online-Spiele) zugenommen haben.

Die Ergebnisse der Geräteweitergabe waren erheblich weniger gemischt. Im Jahr 2020 haben Angestellte ihren Freunden und Familienmitgliedern erheblich seltener gestattet, mit Unternehmensgeräten private E-Mails abzurufen. Bei allen anderen Aktivitäten gab es jedoch im Vorjahresvergleich Zuwächse (zum Teil bis zu 50 %).

Auf unternehmenseigenen Geräten durchgeführte private Aktivitäten



Auf unternehmenseigenen Geräten durchgeführte Aktivitäten von Freunden und Familienmitgliedern

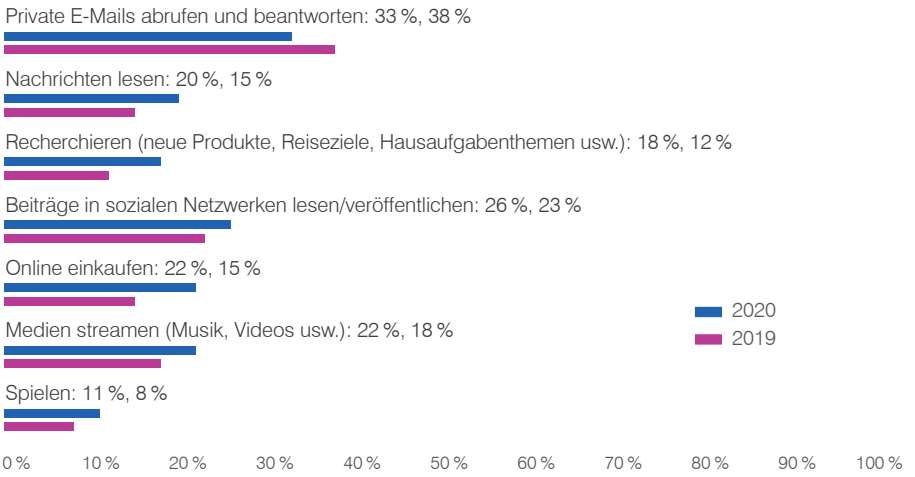


Abb. 10.

Schulungen zu Cybersicherheit: Sind Unternehmen engagiert genug?

98 %
der Unternehmen haben ein Schulungsprogramm zur Sensibilisierung für Sicherheit implementiert.

ABER

Nur **64 %**
führen formelle Schulungen durch (Präsenz- oder Online-Kurse).

Die Zahlen zeigen zweifelsfrei, dass Unternehmen in den letzten Jahren die Bedeutung von Cybersicherheitsschulungen erkannt haben. In der diesjährigen Umfrage sagten fast alle IT-Sicherheitsexperten, dass ihr Unternehmen ein Schulungsprogramm zur Sensibilisierung für Sicherheit betreibt.

Doch die Implementierung eines Programms ist nur der erste Schritt – seine effektive Nutzung der nächste.

Dies zeigt sich dadurch, dass von den Unternehmen mit einem solchen Programm nur etwas mehr als die Hälfte (52 %) unternehmensweite Schulungen durchführt. Etwas mehr als ein Drittel (36 %) schult lediglich bestimmte Abteilungen und Rollen, während 11 % erklärten, dass ihr Schulungsansatz „sehr gezielt" sei und sich auf Einzelpersonen anstatt Gruppen konzentrieren würde. (Etwa 1 % konnte keine Angaben zu Schulungen im eigenen Unternehmen machen.)

Noch größere Sorgen bereitet uns, dass nur bei etwa 60 % der Umfrageteilnehmer formelle Schulungen im Rahmen ihres Programms durchführt werden (als Präsenz- oder Online-Sitzungen). Fast 30 % setzen ausschließlich auf simulierte Phishing-Angriffe, um ihre Anwender zu informieren – ein Ansatz, der viele Probleme bereitet. Obwohl simulierte Phishing-Angriffe durchaus ein wertvolles Hilfsmittel sind, sind sie allein nicht ausreichend. Phishing-Tests sind genau das: Tests. Sie bewerten die Reaktionen der Anwender auf ein konkretes Thema sowie konkrete Köder zu einem konkreten Zeitpunkt. Wenn Nutzer auf eine der vielen und vielfältigen Angreifertaktiken beim E-Mail-Phishing (und andere Social-Engineering-Betrugsversuche) hereinfallen, werden sie jedoch nicht geschult.

Gleichzeitig erhalten Anwender, die nicht geklickt haben, überhaupt keine Schulungen – unabhängig davon, ob sie sie benötigen oder nicht. Einige Nutzer (vielleicht sogar die meisten) werden einen simulierten Angriff als verdächtig erkennen und der Anweisung folgen, die Nachricht zu melden bzw. zu löschen. Andere jedoch könnten den gleichen Test ignorieren, weil sie zu beschäftigt sind oder das Thema sie einfach nicht anspricht. Die Gründe können vielfältig sein. In jedem Fall sollten alle Anwender formelle Schulungen zu diesem Thema erhalten.

Solche unbekannten Faktoren zeigen, dass Unternehmen gut daran tun, die Aussagekraft von Daten zu hinterfragen. Wenn wir die ursprüngliche Zahl von 98 % nicht hinterfragen, scheinen die meisten Unternehmen bei Awareness-Schulungen auf dem richtigen Kurs zu sein. Ein Blick hinter die Kulissen zeigt jedoch, dass die reale Situation weniger eindeutig ist.

Auf die Frage, wie häufig ihr Unternehmen formelle Schulungen für die Angestellten veranstaltet, antworteten die Umfrageteilnehmer wie folgt:

INTERNATIONAL

53 %
der US-Unternehmen nutzen bei Awareness-Schulungen für Endnutzer ausschließlich simulierte Phishing-Angriffe – der höchste Wert unter allen untersuchten Regionen.

81 %
der spanischen Unternehmen binden in ihre Programme formelle Schulungssitzungen ein. Keine andere Region erreicht diesen Wert.

Häufigkeit formeller Schulungen

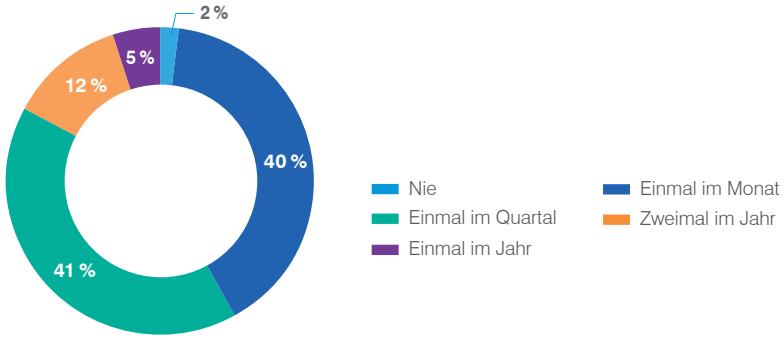


Abb. 11.

INTERNATIONAL

37 %

der Unternehmen in Japan veranstalten jedes Jahr weniger als eine Stunde an formellen Schulungen.

28 %

der deutschen Unternehmen führen ein- bis zweimal jährlich Schulungen zur Verbesserung des Endnutzerverhaltens durch.

Pro Jahr für formelle Schulungen vorgesehene Zeit

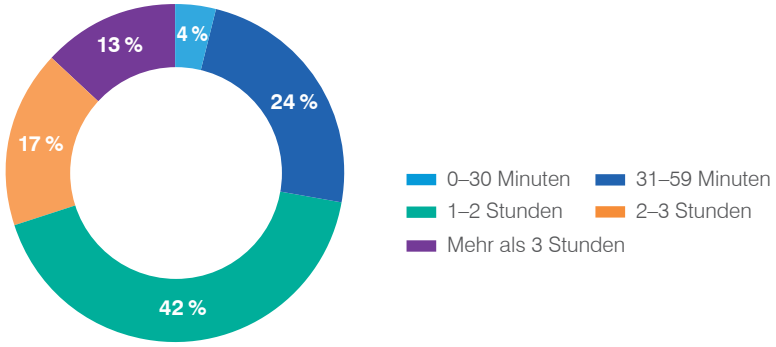


Abb. 12.

Wenn Sie überschlagen, wie häufig Sie formelle Schulungen durchführen und wie viel Zeit Sie dafür einplanen, stellt sich die Frage: Sind Ihre personenzentrierten Schutzmaßnahmen so flexibel wie die Angriffsmethoden Ihrer Gegenspieler? Wenn Sie nur wenige Schulungen im Jahr veranstalten und nicht bereit sind, dem Thema Cybersicherheit mehr Zeit zu widmen, ist die Antwort ein klares „Nein“.

Wir kennen die Schwierigkeiten, die Unternehmensführung und die Anwender an Bord zu holen: Sie müssen die Anwender motivieren und gleichzeitig weitere Schulungsaspekte berücksichtigen.

Doch wenn Ihre Interaktionen nur selten stattfinden und Sie die am stärksten gefährdeten Nutzer nicht erkennen und schulen können, legt sich Ihr Unternehmen weniger ins Zeug als die Angreifer – zum Nachteil für Sie.

Themen der Cybersicherheit: Sind sie umfassend genug?

Weiter oben in diesem Bericht sprechen wir von „jenseits des Posteingangs“. Ein ähnliches Schlagwort lautet „jenseits von Phishing“ („Beyond the Phish“). Diese drei Merksätze kennzeichnen die Philosophie hinter Schulungen zur Sensibilisierung für Sicherheit:

- Simulierte Phishing-Angriffe allein genügen nicht.
- Die Schulungen sollten sich nicht auf E-Mail-Phishing beschränken.
- Social-Engineering-Angriffe dürfen nicht das einzige Thema sein.

DIE FAKTEN

71 % der Unternehmen gaben an, dass sie ein automatisiertes Tool für E-Mail-Meldungen einsetzen, doch **nur 28 %** nutzen E-Mail-Berichte für ihr Schulungsprogramm zur Sensibilisierung für Sicherheit.

INTERNATIONAL

Nur **63 %** der britischen Unternehmen veranstalten für ihre Anwender Schulungen zu E-Mail-Phishing. Dies ist der geringste Wert unter allen untersuchten Regionen.

Nur **15 %** der deutschen Unternehmen schulen ihre Anwender zu Compliance-bezogenen Themen wie die DSGVO.

Im Jahr 2020 wünschten oder forderten **90 %** der Unternehmen in den USA von ihren Angestellten, im Home Office zu arbeiten. Dabei schulen jedoch nur **29 %** ihre Anwender in empfohlenen Vorgehensweisen zur Arbeit im Home Office.

Leider beschränken viele Unternehmen ihre Schulungen zur Sensibilisierung für Sicherheit auf wenige Themen, wie die folgende Abbildung beweist:

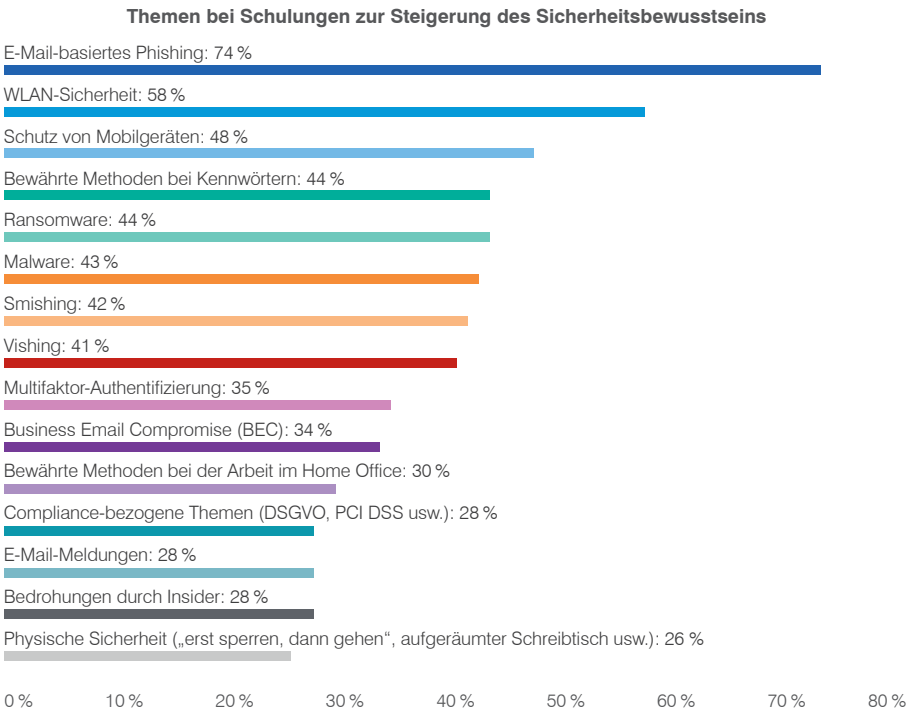


Abb. 13.

Natürlich sollten alle Angestellten eine klare Vorstellung von E-Mail-Sicherheit haben, da die Angreifer noch lange (vielleicht für immer) auf Phishing setzen werden. Da E-Mails am Arbeitsplatz und im Privatleben ein fester Bestandteil des Alltags sind, muss E-Mail-Hygiene statt als Spezialwissen im Bereich Cybersicherheit vielmehr als grundlegende Alltagskompetenz betrachtet werden.

Deshalb sollten Unternehmen bei ihren Schulungen ihrer Anwender Social-Engineering-Bedrohungen umfassender betrachten. Social-Engineering-Techniken kommen nicht nur bei E-Mails, sondern auch bei vielen anderen Angriffsvektoren zum Einsatz. Wenn Nutzer die emotionalen Manipulationsversuche unabhängig von ihrer Quelle erkennen können, erhöht das die Sicherheit auf allen Kommunikationskanälen.

Unternehmen sollten es damit nicht bewenden lassen. Viele Verhaltensweisen bei der Cybersicherheit betreffen die Unternehmenssicherheit als Ganzes. Ständige Ärgernisse für die IT sind beispielsweise einfache sowie wiederverwendete Kennwörter. Gleichzeitig schulen weniger als 50 % der Unternehmen ihre Mitarbeiter zu empfohlenen Vorgehensweisen bei der Kennwortverwendung und weniger als ein Drittel behandeln in ihren Programmen die mehrstufige Authentifizierung. Erfolgreiche Angriffe nutzen häufig eine Kette von Fehlern aus, die von mehreren Menschen – innerhalb und außerhalb des Postfachs – begangen werden.

Daher wollen viele IT-Sicherheitsexperten die Verhaltensweisen der Anwender ändern. Wenn Sie dazugehören, sollten Sie sich die Frage stellen: Habe ich alles in meiner Macht stehende getan, um die gewünschten Veränderungen zu erreichen?

Konsequenzmodelle: Schwierige Antworten

Viele unserer Kunden möchten von uns wissen, wie das Konsequenzmodell in ihrem Unternehmen strukturiert werden sollte. Darauf haben wir keine wirkliche Antwort, dafür aber einen Ratschlag: Anwender sollten für unabsichtliche Fehler nicht bestraft werden. Unserer Meinung nach sollten Schulungen stets als Chance und nicht als Konsequenz betrachtet werden.

Wir verstehen jedoch, dass manche Firmen ein Konsequenzmodell für „Wiederholungstäter" einführen möchten. Gleichzeitig wollten wir mehr über die Eskalationspfade dieser Unternehmen jenseits von Folgeschulungen wissen.

In diesem Jahr nahmen wir Schulungen von der Liste der Strafmaßnahmen und konzentrierten uns auf die Konsequenzen. Außerdem fragten wir die IT-Sicherheitsexperten, welche Zeitrahmen vorgegeben werden und wie die Reaktionen der Angestellten auf Konsequenzmodelle ausfallen.

DIE FAKTEN

55 % der Unternehmen bestrafen Anwender, die regelmäßig auf (reale bzw. simulierte) Phishing-Angriffe hereinfallen.

82 % der Unternehmen mit einem Konsequenzmodell erklärten, dieses hätte die Sensibilisierung für Sicherheitsthemen verbessert.

INTERNATIONAL

82 %
der US-Unternehmen und damit mehr als jede andere untersuchte Region nutzen ein Konsequenzmodell.

72 %
der australischen Unternehmen beziehen bei der Disziplinierung von Wiederholungstätern die Personalabteilung ein.

35 %
der spanischen Unternehmen und damit weniger als alle anderen untersuchten Regionen nutzen ein Konsequenzmodell.

32 %
der Unternehmen in Großbritannien gaben an, dass ihr Konsequenzmodell keinen Einfluss auf das Sicherheitsbewusstsein der Angestellten hat.

30 %
der US-Unternehmen und damit mehr als jede andere untersuchte Region drohen als Konsequenz mit Kündigung.

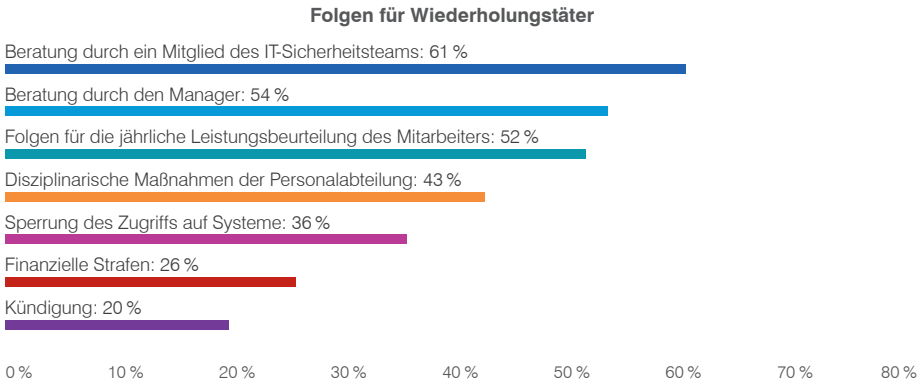


Abb. 14.

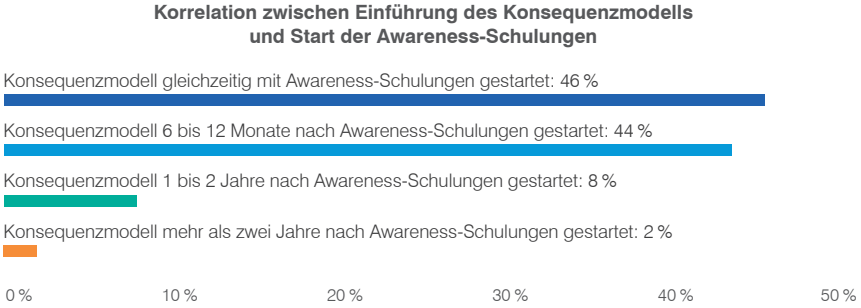


Abb. 15.

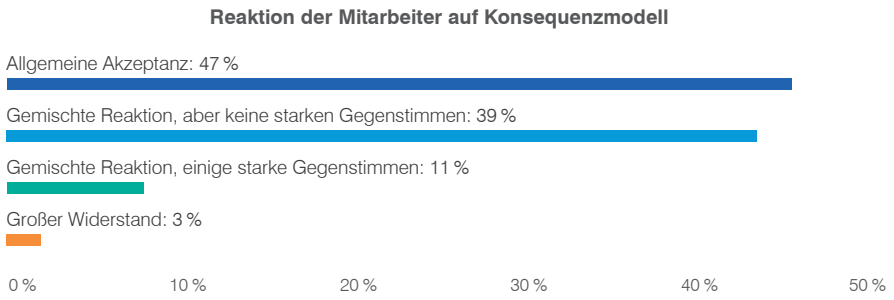


Abb. 16.

Fast die Hälfte der Unternehmen gab an, dass ihr Konsequenzmodell weithin akzeptiert wäre. Bei der anderen Hälfte sind die Anwender jedoch unsicher (oder verärgert) über die Konsequenzen von Cybersicherheitsverstößen.

Die Umfrageteilnehmer, in deren Unternehmen großer Widerstand existiert, versuchen, den Sorgen der Nutzer Rechnung zu tragen. Bei der Einführung eines Konsequenzmodells ist die Wahrnehmung der Anwender jedoch ein wichtiger Faktor. Wenn Strafmaßnahmen Teil der Awareness-Schulungen sind, können einige (oder sogar viele) Anwender das gesamte Programm ablehnend betrachten.

ABSCHNITT 6

Fazit: Aufmerksamkeit und Entschlossenheit sind gefragt

80 %

der Unternehmen geben an, dass Schulungen zur Sensibilisierung für Sicherheit die Anfälligkeit für Phishing verringert haben.

Wir wissen, dass Unternehmen viel für den Schutz ihrer Ressourcen vor Cyberangreifern tun. Deshalb freuen wir uns, dass mehr als zwei Drittel der befragten IT-Sicherheitsexperten der Meinung sind, ihre Schulungsmaßnahmen zur Sensibilisierung für Sicherheit hätten die Anfälligkeit ihrer Anwender für Phishing merklich verringert.

Aber tun die Unternehmen wirklich so viel, wie sie könnten? Und was ist mit Ihnen?

Im diesjährigen Bericht haben wir die Cybersicherheit sowohl aus Sicht der IT-Sicherheit als auch der Anwender betrachtet. Unsere Benchmark-Daten, Brancheneinblicke und Empfehlungen sollen Sie beim Erarbeiten eines Aktionsplans unterstützen. Dabei sollten Sie die folgenden Punkte berücksichtigen:

Machen Sie Anwender zu Verantwortlichen

Führungskräfte und andere Entscheidungsträger sind wichtige Verantwortliche in Ihrem Unternehmen. Bei Schulungen zur Sensibilisierung für Sicherheit sind die wichtigsten Verantwortlichen die Anwender. Der Erfolg eines Programms hängt vom Erfolg der Anwender ab. Die Akzeptanz bei den Angestellten bleibt jedoch vielfach unberücksichtigt. Wenn Sie Sicherheit zu einem Kernaspekt Ihrer Unternehmenskultur machen möchten, müssen Sie die Nutzer für sich gewinnen.

Beachten Sie dazu die folgenden Tipps:

- Gehen Sie nicht automatisch davon aus, dass die Anwender alle Cybersicherheits-begriffe kennen. Wenn sie Ihre Sprache nicht kennen, besteht die Gefahr, sie gleich am Anfang zu verlieren.
- Sprechen Sie die Anwender persönlich an. Cybersicherheit ist nicht ausschließlich auf die Arbeit bezogen – und die Nutzer sollten das verstehen. Zeigen Sie ihnen, wie wichtig die Sicherheitsmaßnahmen sowohl auf Arbeit als auch zu Hause sind.
- Legen Sie Ihre Erwartungen klar und deutlich dar und kommunizieren Sie regelmäßig mit den Nutzern, damit sie die Ziele Ihres Programms sowie die geplanten Aktivitäten kennen. (Natürlich sollten Sie den genauen Zeitplan der Phishing-Tests für sich behalten.)
- Geben Sie den Anwendern das Gefühl, unterstützt zu werden. Häufig genug sind es die Nutzer, die zwischen dem Erfolg oder Misserfolg eines Angriffs stehen. Geben Sie Ihren Anwendern die notwendigen Tools in die Hand und führen Sie Schulungen zu ihrer Nutzung durch.
- Schaffen Sie den Nutzern eine sichere Umgebung, in der sie lernen, Fehler machen, üben und sich weiterbilden können. Wenn Sie der Meinung sind, ein Konsequenzmodell einführen zu müssen, schulen Sie zuvor die Angestellten darin, unzulässige Verhaltensweisen zu vermeiden.
- Weisen Sie auf die Vorteile des Programms hin und zeigen Sie, wie besseres Verhalten die Sicherheit des Unternehmens stärkt. In den meisten Fällen sind die negativen Aspekte längst klar und dennoch liegt der Schwerpunkt auf den Fehlern der Anwender – und nicht darauf, was sie richtig machen. Kehren Sie das Prinzip um und geben Sie den Nutzern Gelegenheit, sich auf die konstruktiven Aspekte der Cybersicherheit zu konzentrieren. Die Angestellten sollten klar verstehen, was Sie von ihnen warum erwarten, damit die Sicherheit an erster Stelle steht.

Betrachten Sie Benchmark-Daten mit Augenmaß

Wir haben es in diesem Bericht mehrfach erwähnt, möchten es hier jedoch noch einmal wiederholen: Benchmark-Ergebnisse wie die oben genannten zu den durchschnittlichen Fehlerquoten und Meldungsraten sind für Vergleiche sinnvoll. Doch wenn Sie hinter den Durchschnittswerten zurückbleiben, heißt das noch lange nicht, dass Ihr Unternehmen „versagt". Ebenso gilt: Wenn Ihre Werte besser sind, ist das noch kein Grund zur Entspannung.

Verknüpfen Sie Bedrohungsdaten und Schulungen zur Sensibilisierung für Sicherheit

90 %

der Unternehmen berücksichtigen Bedrohungsdaten bei der Planung ihrer Awareness-Schulungen.

Verwendung von Bedrohungsdaten in Unternehmen

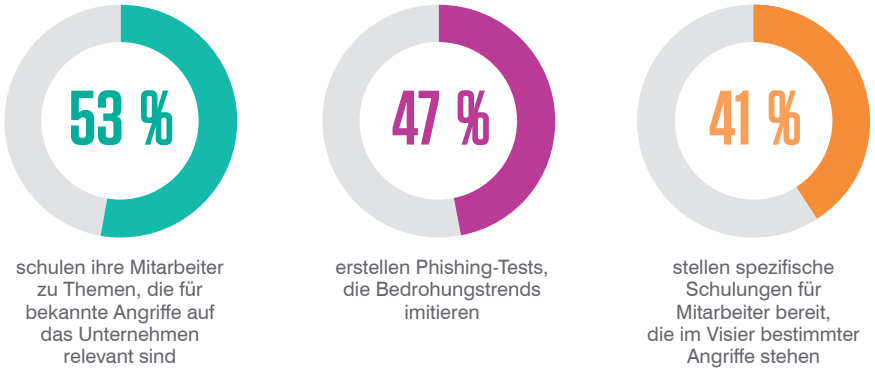


Abb. 17.

Wir freuen uns, dass fast alle Unternehmen auf Bedrohungsdaten setzen, um ihre Schulungen gezielt anzupassen. Es gibt aber noch viele Verbesserungsmöglichkeiten. Im Idealfall sollten Unternehmen alle drei in Abb. 17 vorgestellten Aktivitäten durchführen, um die Bedrohungsdaten bestmöglich zu nutzen.

Verbinden Sie Sensibilisierungs- und Schulungsaktivitäten mit anderen Sicherheitsfunktionen

Wir erleben häufig, dass Awareness-Schulungsprogramme isoliert von anderen Sicherheitsprogrammen betrieben werden. Im Idealfall sollten sich alle anwenderbezogenen Sicherheitsmaßnahmen überschneiden und aufeinander Bezug nehmen. So sind E-Mail-Meldungen ein gutes Beispiel dafür, wie zwei Seiten der Unternehmenssicherheit verknüpft werden können.

Und es warten noch viele weitere Möglichkeiten. Beispielsweise können Sie Kennwortschulungen mit der Anzahl von Anfragen zur Kennwortzurücksetzung verknüpfen oder damit, wie viele Versuche ein Anwender nach Aufforderung zur Erstellung eines neuen Kennworts benötigt. Eine weitere Möglichkeit ist die Überwachung von Verstößen gegen Richtlinien zur Datenverlustprävention (DLP) in Verbindung mit Schulungen zu Datensicherheit.

Die Verknüpfung von Schulungen und weiteren Sicherheitsinitiativen bietet viele potenzielle Vorteile:

- Insgesamt einheitlicherer und stärker ergebnisorientierter Sicherheitsansatz
- Klarere Verbindung für Anwender und besseres Verständnis der Auswirkungen ihrer Handlungen auf die Sicherheit
- Messbare und umsetzbare Informationen über die Wirkung Ihres Programms auf die allgemeine Sicherheitslage des Unternehmens, die Sie an Ihren CISO und das gesamte Sicherheitsteam weitergeben können

ANHANG

A. Umfrage zu IT-Sicherheit: Aufschlüsselung nach Ländern

	Australien	Frankreich	Deutschland	Japan	Spanien	Groß-britannien	USA	Weltweiter Durchschnitt
Hat Ihr Unternehmen im Jahr 2020 einen erfolgreichen Phishing-Angriff verzeichnet?								
Ja	60 %	48 %	47 %	56 %	51 %	66 %	74 %	57 %
Nein	38 %	49 %	49 %	42 %	45 %	29 %	25 %	40 %
Weiß nicht	2 %	3 %	4 %	2 %	4 %	5 %	1 %	3 %
Welches der folgenden Ereignisse hat Ihr Unternehmen nach einem erfolgreichen Phishing-Angriff im Jahr 2020 verzeichnet? (Mehrere Antworten zulässig.)								
Datenverlust	47 %	63 %	62 %	61 %	69 %	59 %	58 %	60 %
Kompromittierte Anmeldedaten/Konten	47 %	42 %	60 %	64 %	37 %	58 %	55 %	52 %
Ransomware-Infektion	67 %	25 %	49 %	32 %	49 %	50 %	55 %	47 %
Infektionen mit sonstiger Malware	30 %	42 %	28 %	25 %	18 %	32 %	31 %	29 %
Finanzielle Verluste/ Überweisungsbetrug	23 %	13 %	13 %	11 %	12 %	17 %	35 %	18 %
Wie viele dieser (erfolgreichen oder erfolglosen) Social-Engineering-Angriffe hat Ihr Unternehmen im Jahr 2020 verzeichnet?								
Umfangreicher Phishing-Angriff (gleiche E-Mail an mehrere Personen gesendet)								
0	26 %	34 %	29 %	26 %	17 %	18 %	16 %	23 %
1 bis 10	30 %	33 %	27 %	36 %	48 %	38 %	29 %	34 %
11 bis 25	14 %	16 %	20 %	14 %	16 %	22 %	16 %	17 %
26 bis 50	22 %	8 %	15 %	2 %	9 %	5 %	14 %	11 %
51 bis 100	2 %	6 %	7 %	6 %	5 %	6 %	15 %	7 %
Mehr als 100	6 %	1 %	1 %	12 %	5 %	9 %	8 %	6 %
Weiß nicht	0 %	2 %	1 %	4 %	0 %	2 %	2 %	2 %

	Australien	Frankreich	Deutschland	Japan	Spanien	Groß-britannien	USA	Weltweiter Durchschnitt
Spearphishing/Whaling (gezielter Angriff)								
0	26 %	43 %	38 %	46 %	35 %	32 %	19 %	34 %
1 bis 10	32 %	30 %	26 %	20 %	34 %	32 %	25 %	29 %
11 bis 25	20 %	12 %	18 %	12 %	11 %	14 %	18 %	15 %
26 bis 50	14 %	10 %	11 %	8 %	11 %	9 %	15 %	11 %
51 bis 100	4 %	2 %	5 %	12 %	5 %	10 %	13 %	7 %
Mehr als 100	4 %	2 %	1 %	2 %	3 %	3 %	8 %	3 %
Weiß nicht	0 %	1 %	1 %	0 %	1 %	0 %	2 %	1 %
Business Email Compromise (z. B. Überweisungs- oder Rechnungsbetrug)								
0	34 %	52 %	32 %	48 %	22 %	39 %	20 %	35 %
1 bis 10	30 %	28 %	21 %	28 %	37 %	28 %	15 %	27 %
11 bis 25	16 %	13 %	21 %	8 %	17 %	13 %	21 %	16 %
26 bis 50	10 %	3 %	15 %	10 %	7 %	9 %	19 %	10 %
51 bis 100	8 %	1 %	8 %	2 %	12 %	5 %	18 %	8 %
Mehr als 100	2 %	1 %	1 %	4 %	5 %	6 %	5 %	3 %
Weiß nicht	0 %	2 %	2 %	0 %	0 %	0 %	2 %	1 %
Smishing (SMS-/Textnachrichten-Phishing)								
0	36 %	52 %	44 %	42 %	40 %	38 %	19 %	39 %
1 bis 10	26 %	21 %	22 %	26 %	32 %	25 %	19 %	24 %
11 bis 25	12 %	10 %	16 %	8 %	12 %	16 %	11 %	12 %
26 bis 50	18 %	9 %	11 %	14 %	9 %	8 %	21 %	13 %
51 bis 100	4 %	3 %	3 %	6 %	4 %	10 %	18 %	7 %
Mehr als 100	4 %	4 %	2 %	2 %	2 %	3 %	9 %	4 %
Weiß nicht	0 %	1 %	2 %	2 %	1 %	0 %	3 %	1 %

	Australien	Frankreich	Deutschland	Japan	Spanien	Groß-britannien	USA	Weltweiter Durchschnitt
Vishing (Voice Phishing per Telefonanruf)								
0	32 %	71 %	36 %	62 %	54 %	44 %	23 %	46 %
1 bis 10	28 %	15 %	26 %	20 %	22 %	21 %	16 %	21 %
11 bis 25	14 %	6 %	17 %	4 %	12 %	14 %	13 %	12 %
26 bis 50	18 %	4 %	8 %	8 %	7 %	5 %	18 %	10 %
51 bis 100	6 %	3 %	8 %	0 %	2 %	10 %	16 %	6 %
Mehr als 100	2 %	0 %	3 %	6 %	2 %	6 %	10 %	4 %
Weiß nicht	0 %	1 %	2 %	0 %	1 %	0 %	4 %	1 %
Abgelegte USB-Sticks (manipulierte USB-Laufwerke mit schädlicher Software oder Code)								
0	38 %	69 %	37 %	58 %	48 %	49 %	20 %	46 %
1 bis 10	20 %	15 %	28 %	22 %	26 %	20 %	16 %	21 %
11 bis 25	14 %	5 %	15 %	8 %	11 %	9 %	16 %	11 %
26 bis 50	20 %	5 %	9 %	4 %	10 %	6 %	21 %	11 %
51 bis 100	4 %	4 %	5 %	6 %	2 %	12 %	14 %	6 %
Mehr als 100	4 %	1 %	4 %	2 %	2 %	3 %	11 %	4 %
Weiß nicht	0 %	1 %	2 %	0 %	1 %	1 %	2 %	1 %
Social-Media-Angriffe (z. B. Pretexting oder Kontoübernahmen)								
0	28 %	67 %	38 %	46 %	42 %	39 %	14 %	39 %
1 bis 10	32 %	9 %	21 %	34 %	32 %	27 %	21 %	25 %
11 bis 25	16 %	12 %	20 %	6 %	8 %	9 %	18 %	13 %
26 bis 50	12 %	6 %	7 %	8 %	11 %	13 %	18 %	11 %
51 bis 100	6 %	4 %	8 %	2 %	2 %	5 %	18 %	6 %
Mehr als 100	4 %	0 %	3 %	4 %	3 %	7 %	9 %	4 %
Weiß nicht	2 %	2 %	3 %	0 %	2 %	0 %	2 %	2 %

	Australien	Frankreich	Deutschland	Japan	Spanien	Groß-britannien	USA	Weltweiter Durchschnitt
Hat Ihr Unternehmen 2020 einen Ransomware-Angriff verzeichnet und das Lösegeld gezahlt?								
Ja	28 %	18 %	36 %	18 %	25 %	44 %	68 %	34 %
Nein, wir wurden infiziert, zahlten jedoch nicht	38 %	35 %	31 %	36 %	41 %	31 %	10 %	32 %
Nein, wir wurden nicht infiziert	34 %	47 %	33 %	46 %	34 %	25 %	22 %	34 %
Was ist passiert, nachdem Sie das Lösegeld gezahlt haben? (Eine Antwort zulässig.)								
Erhielten nach der ersten Zahlung wieder Zugriff auf Daten/Systeme	50 %	78 %	56 %	45 %	56 %	59 %	76 %	60 %
Erhielten anschließend weitere Ransomware-Forderungen; zahlten erneut und erhielten schließlich Zugriff auf Daten	43 %	17 %	25 %	44 %	40 %	39 %	19 %	32 %
Erhielten anschließend weitere Ransomware-Forderungen; verweigerten die Zahlung und verloren die Daten	7 %	0 %	14 %	11 %	4 %	2 %	3 %	6 %
Erhielten niemals Zugang zu Daten, selbst nachdem das Lösegeld gezahlt wurde	0 %	5 %	5 %	0 %	0 %	0 %	2 %	2 %
Betreibt Ihr Unternehmen ein Schulungsprogramm zur Sensibilisierung für Sicherheit?								
Ja	100 %	95 %	97 %	98 %	100 %	96 %	100 %	98 %
Nein	0 %	5 %	3 %	2 %	0 %	4 %	0 %	2 %
Welche der folgenden Themen werden in Ihrem Schulungsprogramm zur Sensibilisierung für Sicherheit behandelt? (Mehrere Antworten zulässig.)								
E-Mail-basiertes Phishing	80 %	75 %	68 %	88 %	75 %	63 %	70 %	74 %
Smishing	52 %	29 %	32 %	37 %	50 %	44 %	47 %	42 %
Vishing	56 %	26 %	40 %	37 %	40 %	48 %	43 %	41 %
WLAN-Sicherheit	58 %	53 %	55 %	49 %	64 %	61 %	67 %	58 %
Schutz von Mobilgeräten	52 %	44 %	45 %	49 %	48 %	47 %	48 %	48 %
Bewährte Methoden bei Kennwörtern	58 %	51 %	26 %	39 %	51 %	43 %	42 %	44 %
Mehrfaktor-Authentifizierung	40 %	29 %	32 %	33 %	40 %	36 %	33 %	35 %
Bedrohungen durch Insider	34 %	32 %	23 %	16 %	35 %	22 %	32 %	28 %
Ransomware	48 %	44 %	38 %	39 %	52 %	47 %	39 %	44 %
Malware	50 %	46 %	34 %	41 %	57 %	41 %	35 %	43 %

	Australien	Frankreich	Deutschland	Japan	Spanien	Groß-britannien	USA	Weltweiter Durchschnitt
Business Email Compromise (BEC)	46 %	25 %	31 %	39 %	39 %	28 %	27 %	34 %
E-Mail-Meldungen	36 %	22 %	29 %	24 %	25 %	31 %	28 %	28 %
Compliance-bezogene Themen (z. B. DSGVO und PCI DSS)	36 %	23 %	15 %	27 %	38 %	31 %	26 %	28 %
Empfohlene Vorgehensweisen für die Arbeit im Home Office	32 %	38 %	14 %	22 %	36 %	36 %	29 %	30 %
Physische Sicherheitsmaßnahmen (z. B. „erst sperren, dann gehen“)	32 %	28 %	19 %	27 %	23 %	31 %	25 %	26 %
Wer nimmt in Ihrem Unternehmen am Schulungsprogramm zur Sensibilisierung für Sicherheit teil?								
Alle/unternehmensweite Schulungen	48 %	49 %	52 %	59 %	42 %	56 %	63 %	52 %
Bestimmte Abteilungen/Rollen	38 %	37 %	34 %	35 %	49 %	36 %	22 %	36 %
Bestimmte Personen	12 %	12 %	14 %	4 %	9 %	8 %	15 %	11 %
Weiß nicht	2 %	2 %	0 %	2 %	0 %	0 %	0 %	1 %
Welchen Ansatz verfolgen Sie bei Ihren Schulungen zur Sensibilisierung für Sicherheit?								
Ausschließlich simulierte Phishing-Tests	26 %	24 %	30 %	26 %	11 %	28 %	53 %	29 %
Ausschließlich formelle Schulungen (Präsenz- oder Online-Kurse)	42 %	46 %	39 %	33 %	44 %	52 %	30 %	41 %
Ausschließlich informative Inhalte (wie E-Mails und Newsletter)	6 %	8 %	7 %	10 %	8 %	7 %	6 %	7 %
Kombination aus verschiedenen Inhaltstypen	26 %	22 %	24 %	31 %	37 %	13 %	11 %	23 %
Wie häufig führt Ihr Unternehmen formelle Schulungen oder weist sie zu (Präsenz- oder Online-Kurse)?								
Nie	3 %	5 %	0 %	3 %	0 %	0 %	0 %	2 %
Einmal im Monat	53 %	29 %	36 %	42 %	40 %	29 %	56 %	40 %
Einmal im Quartal	41 %	49 %	36 %	32 %	44 %	52 %	34 %	41 %
Zweimal im Jahr	3 %	14 %	21 %	16 %	9 %	14 %	5 %	12 %
Einmal im Jahr	0 %	3 %	7 %	7 %	7 %	5 %	5 %	5 %

	Australien	Frankreich	Deutschland	Japan	Spanien	Groß-britannien	USA	Weltweiter Durchschnitt
Wie viel Zeit widmet Ihr Unternehmen formellen Schulungen (Präsenz- oder Online-Kurse) in einem Kalenderjahr?								
0–30 Minuten	6 %	2 %	8 %	10 %	3 %	0 %	2 %	4 %
31–59 Minuten	27 %	19 %	21 %	27 %	16 %	29 %	24 %	24 %
1–2 Stunden	46 %	34 %	36 %	40 %	44 %	48 %	44 %	42 %
2–3 Stunden	6 %	34 %	25 %	10 %	17 %	15 %	15 %	17 %
Mehr als 3 Stunden	15 %	11 %	10 %	13 %	20 %	8 %	15 %	13 %
Konnte Ihr Unternehmen nach Schulungen zur Sensibilisierung für Sicherheit eine reduzierte Anfälligkeit für Phishing feststellen?								
Ja	86 %	79 %	70 %	72 %	80 %	83 %	90 %	80 %
Nein	9 %	15 %	28 %	19 %	19 %	11 %	5 %	15 %
Weiß nicht	5 %	6 %	2 %	9 %	1 %	6 %	5 %	5 %
Nutzt Ihr Unternehmen ein automatisiertes Tool für E-Mail-Meldungen?								
Ja	74 %	62 %	61 %	80 %	63 %	71 %	89 %	71 %
Nein	16 %	25 %	30 %	14 %	17 %	19 %	9 %	19 %
Noch nicht, wir haben es aber vor	10 %	13 %	9 %	6 %	20 %	10 %	2 %	10 %
Haben bei Ihrem Unternehmen Bedrohungsdaten Einfluss auf Ihre Schulungen zur Sensibilisierung für Sicherheit? (Mehrere Antworten zulässig.)								
Ja, wir nutzen Phishing-Tests, die wachsende Bedrohungen imitieren	52 %	45 %	38 %	56 %	40 %	33 %	67 %	47 %
Ja, wir schulen zu konkreten Themen, die sich auf reale Angriffe beziehen	50 %	39 %	62 %	52 %	55 %	65 %	47 %	53 %
Ja, wir schulen konkrete Personen, von denen wir wissen, dass sie angegriffen werden	64 %	35 %	40 %	38 %	35 %	33 %	41 %	41 %
Nein, wir passen unsere Schulungen nicht an Bedrohungsdaten an	6 %	4 %	7 %	14 %	13 %	7 %	5 %	8 %
Nicht zutreffend (ich habe keinen Zugriff auf die Bedrohungsdaten meines Unternehmens)	2 %	3 %	1 %	0 %	1 %	3 %	2 %	2 %

	Australien	Frankreich	Deutschland	Japan	Spanien	Groß-britannien	USA	Weltweiter Durchschnitt
Hat Ihr Unternehmen im Laufe des Jahres 2020 von mehr als 50 % der Angestellten gewünscht oder gefordert, ins Home Office zu wechseln?								
Ja, wir haben das gewünscht	48 %	46 %	43 %	64 %	54 %	47 %	69 %	53 %
Ja, wir haben das gefordert	32 %	31 %	25 %	20 %	33 %	45 %	21 %	29 %
Nein	20 %	21 %	28 %	14 %	12 %	7 %	8 %	16 %
Nicht zutreffend (mehr als 50 % unserer Angestellten arbeiten immer extern)	0 %	2 %	4 %	2 %	1 %	1 %	2 %	2 %
Bestraft Ihr Unternehmen Mitarbeiter, die regelmäßig auf (reale bzw. simulierte) Phishing-Angriffe hereinfallen? Mit anderen Worten: Gibt es Konsequenzen (außer zusätzlichen Schulungen) für „Wiederholungstäter“?								
Ja	50 %	43 %	46 %	66 %	35 %	60 %	82 %	55 %
Nein	50 %	47 %	49 %	30 %	62 %	36 %	16 %	41 %
Weiß nicht	0 %	10 %	5 %	4 %	3 %	4 %	2 %	4 %
Welche Strafen (außer zusätzlichen Schulungen) drohen Angestellten? (Mehrere Antworten zulässig.)								
Beratung durch den Manager	52 %	65 %	52 %	64 %	37 %	35 %	71 %	54 %
Beratung durch das IT-Sicherheitsteam	76 %	60 %	57 %	58 %	60 %	63 %	56 %	61 %
Auswirkungen auf jährliche Leistungsbeurteilungen	64 %	42 %	54 %	58 %	37 %	48 %	61 %	52 %
Disziplinarmaßnahmen (wie eine schriftliche Verwarnung) durch die Personalabteilung	72 %	30 %	30 %	33 %	51 %	40 %	45 %	43 %
Entfernung des Zugriffs auf Systeme	36 %	30 %	30 %	45 %	43 %	33 %	34 %	36 %
Finanzielle Strafen	24 %	16 %	22 %	36 %	34 %	18 %	34 %	26 %
Kündigung	12 %	26 %	15 %	15 %	14 %	27 %	30 %	20 %
Weiß nicht	0 %	0 %	0 %	3 %	0 %	0 %	0 %	<1 %
Wie korrelierte die Implementierung eines Konsequenzmodells mit dem Start Ihres Schulungsprogramms zur Sensibilisierung für Sicherheit?								
Konsequenzmodell gleichzeitig mit Awareness-Schulungen gestartet	44 %	44 %	50 %	49 %	34 %	35 %	67 %	46 %
Konsequenzmodell 6 bis 12 Monate nach Awareness-Schulungen gestartet	40 %	44 %	43 %	39 %	63 %	50 %	29 %	44 %
Konsequenzmodell 1 bis 2 Jahre nach Awareness-Schulungen gestartet	12 %	5 %	7 %	12 %	3 %	15 %	4 %	8 %
Konsequenzmodell mehr als zwei Jahre nach Awareness-Schulungen gestartet	4 %	7 %	0 %	0 %	0 %	0 %	0 %	2 %

	Australien	Frankreich	Deutschland	Japan	Spanien	Groß-britannien	USA	Weltweiter Durchschnitt
Hat die Nutzung eines Konsequenzmodells zu einer Verbesserung der Mitarbeiter-Sensibilisierung geführt?								
Ja, es hat einen Unterschied gemacht	88 %	84 %	72 %	85 %	80 %	68 %	95 %	82 %
Nein, es hat keinen Unterschied gemacht	12 %	14 %	22 %	9 %	20 %	32 %	4 %	16 %
Nicht sicher, wir haben das nicht ausgewertet	0 %	0 %	6 %	6 %	0 %	0 %	1 %	2 %
Weiß nicht	0 %	2 %	0 %	0 %	0 %	0 %	0 %	0 %
Wie haben die Angestellten auf die Implementierung Ihres Konsequenzmodells reagiert?								
In den meisten Fällen scheinen die Angestellten den Ansatz zu verstehen und zu akzeptieren	48 %	42 %	48 %	42 %	46 %	40 %	60 %	47 %
Gemischte Reaktionen, aber keine starken Gegenstimmen	44 %	35 %	28 %	55 %	43 %	39 %	27 %	39 %
Gemischte Reaktionen, einige starke Gegenstimmen	8 %	19 %	20 %	0 %	8 %	18 %	7 %	11 %
Großer Widerstand bei den Angestellten	0 %	2 %	4 %	3 %	3 %	3 %	6 %	3 %
Weiß nicht	0 %	2 %	0 %	0 %	0 %	0 %	0 %	0 %

B. Umfrage unter berufstätigen Erwachsenen: Aufschlüsselung nach Ländern

	Australien	Frankreich	Deutschland	Japan	Spanien	Groß-britannien	USA	Weltweiter Durchschnitt
Was ist Phishing?								
Richtige Antwort	66 %	63 %	64 %	66 %	63 %	69 %	52 %	63 %
Falsche Antwort	17 %	20 %	23 %	21 %	17 %	20 %	37 %	22 %
Weiß nicht	17 %	17 %	13 %	13 %	20 %	11 %	11 %	15 %
Was ist Ransomware?								
Richtige Antwort	42 %	30 %	26 %	40 %	28 %	37 %	29 %	33 %
Falsche Antwort	35 %	36 %	31 %	27 %	30 %	38 %	55 %	36 %
Weiß nicht	23 %	34 %	43 %	33 %	42 %	25 %	16 %	31 %
Was ist Malware?								
Richtige Antwort	72 %	72 %	58 %	60 %	75 %	66 %	54 %	65 %
Falsche Antwort	17 %	16 %	24 %	12 %	13 %	24 %	38 %	21 %
Weiß nicht	11 %	12 %	18 %	28 %	12 %	10 %	8 %	14 %
Was ist Smishing?								
Richtige Antwort	25 %	60 %	21 %	19 %	29 %	27 %	35 %	31 %
Falsche Antwort	24 %	16 %	27 %	25 %	20 %	32 %	36 %	25 %
Weiß nicht	51 %	24 %	52 %	56 %	51 %	41 %	29 %	44 %
Was ist Vishing?								
Richtige Antwort	22 %	54 %	18 %	20 %	26 %	30 %	35 %	30 %
Falsche Antwort	18 %	19 %	28 %	20 %	18 %	21 %	32 %	22 %
Weiß nicht	60 %	27 %	54 %	60 %	56 %	49 %	33 %	48 %

	Australien	Frankreich	Deutschland	Japan	Spanien	Groß-britannien	USA	Weltweiter Durchschnitt
Ich weiß, dass die folgenden Aussagen für E-Mails gelten. (Wählen Sie alle zutreffenden Antworten aus.)								
Eine E-Mail kann scheinbar von einer anderen Person bzw. einem anderen Unternehmen als dem realen Absender stammen.	62 %	55 %	65 %	30 %	55 %	58 %	57 %	55 %
Wenn eine E-Mail Logos und Kontaktinformationen von einem bekannten Unternehmen enthält, ist sie sicher.	22 %	17 %	17 %	10 %	20 %	22 %	34 %	20 %
Wenn ich auf einen Link in einer E-Mail klicke, werde ich auf die Website geleitet, die mit der URL in der E-Mail übereinstimmt.	21 %	21 %	21 %	21 %	23 %	24 %	30 %	23 %
E-Mail-Anhänge können mit gefährlicher Software infiziert sein, die meinen Computer beschädigen kann.	63 %	54 %	63 %	51 %	64 %	58 %	52 %	58 %
Alle internen E-Mails (z. B. von meinen Kollegen) sind sicher.	19 %	22 %	14 %	6 %	18 %	15 %	23 %	17 %
Wenn mich ein Link in einer E-Mail zu einer Datei führt, die sich in einem legitimen Cloud-Dienst wie Microsoft 365, Google Drive oder Dropbox befindet, weiß ich, dass die Datei sicher ist.	11 %	10 %	8 %	7 %	13 %	9 %	15 %	11 %
Wenn ich mit einer anderen Person mehrfach E-Mails ausgetauscht habe, weiß ich, dass dieser Kontakt sicher ist.	21 %	13 %	16 %	8 %	19 %	16 %	21 %	16 %
Ich sollte bei allen unerwünschten E-Mail-Nachrichten sofort misstrauisch sein.	59 %	47 %	53 %	47 %	60 %	47 %	41 %	51 %
Auf Arbeit halten die Sicherheits-tools meines Unternehmens alle gefährlichen E-Mails von meinem Posteingang fern.	22 %	15 %	20 %	19 %	22 %	20 %	18 %	19 %
Zu Hause hält mein E-Mail-Anbieter alle gefährlichen E-Mails von meinem Posteingang fern.	16 %	13 %	20 %	8 %	15 %	17 %	16 %	15 %
Ich kann mich nicht sicher für eine dieser Optionen entscheiden.	7 %	10 %	7 %	15 %	5 %	5 %	4 %	8 %

	Australien	Frankreich	Deutschland	Japan	Spanien	Groß-britannien	USA	Weltweiter Durchschnitt
Für welche dieser privaten Aktivitäten nutzen Sie Ihr vom Arbeitgeber gestelltes Notebook bzw. Smartphone? (Mehrere Antworten zulässig.)								
Private E-Mails abrufen und beantworten	61 %	59 %	50 %	53 %	54 %	51 %	70 %	57 %
Beiträge in sozialen Netzwerken lesen/veröffentlichen	33 %	28 %	29 %	29 %	30 %	42 %	45 %	34 %
Medien streamen (Musik, Videos)	27 %	20 %	26 %	19 %	29 %	35 %	47 %	29 %
Online einkaufen	36 %	19 %	31 %	15 %	28 %	37 %	46 %	30 %
Nachrichten lesen	47 %	29 %	35 %	53 %	42 %	35 %	42 %	40 %
Recherchieren (neue Produkte, Reiseziele)	38 %	24 %	29 %	52 %	36 %	28 %	38 %	35 %
Spielen	13 %	9 %	10 %	8 %	11 %	15 %	27 %	13 %
Nichts davon	18 %	19 %	26 %	15 %	23 %	23 %	11 %	19 %
Welche dieser Aktivitäten gestatten Sie Freunden/Familienmitgliedern auf Ihrem vom Arbeitgeber gestellten Notebook bzw. Smartphone? (Mehrere Antworten zulässig.)								
E-Mails abrufen und beantworten	27 %	32 %	31 %	37 %	27 %	27 %	52 %	33 %
Beiträge in sozialen Netzwerken lesen/veröffentlichen	23 %	19 %	28 %	21 %	24 %	29 %	39 %	26 %
Medien streamen (Musik, Videos)	17 %	16 %	24 %	14 %	20 %	24 %	40 %	22 %
Online einkaufen	19 %	18 %	19 %	16 %	19 %	23 %	38 %	22 %
Nachrichten lesen	18 %	12 %	23 %	24 %	19 %	16 %	28 %	20 %
Hausaufgaben recherchieren/ erledigen	16 %	12 %	15 %	26 %	17 %	14 %	24 %	18 %
Spielen	6 %	9 %	11 %	8 %	9 %	10 %	23 %	11 %
Nichts davon	58 %	51 %	48 %	49 %	55 %	48 %	25 %	48 %

C. Fehlerquoten nach Branchen bei simulierten Phishing-Vorlagenstilen

Unterschiedliche Ansichten von Daten können neue Erkenntnisse bringen. Dieser detaillierte Blick auf die branchenspezifischen Fehlerquoten (nach Vorlagenstil, verglichen mit Gesamtfehlerquoten) zeigt, dass es sehr vielen Anwendern schwer fällt, Anhang-basierte Phishing-Tests zu erkennen und zu vermeiden. Diese sehr hohen durchschnittlichen Fehlerquoten (die zum Teil bis auf 26 % oder 32 % gehen) haben normalerweise keinen Einfluss auf die allgemeinen Fehlerquoten, weisen aber auf etwas anderes hin: Anhang-basierte Tests werden in vielen Unternehmen nicht oft eingesetzt.

Wie im Hauptartikel bereits angesprochen, kann eine insgesamt durchschnittliche Fehlerquote potenzielle Risikobereiche verschleiern. Unsere Daten zeigen, dass die Anfälligkeit für Anhang-basierte Phishing-Angriffe für viele Unternehmen ein schlummerndes Problem darstellen kann. Aus diesem Grund können sich regelmäßige Tests und Schulungen zu diesen Bedrohungstypen als sehr nützlich erweisen.

	Durchschnittliche Fehlerquote			
Branche	**Link-basierte Tests**	**Anhang-basierte Tests**	**Dateneingabe-basierte Tests**	**Gesamt**
Automobilbranche	11 %	14 %	4 %	10 %
Bauindustrie	13 %	20 %	6 %	11 %
Behörden	11 %	15 %	3 %	11 %
Bergbau	18 %	22 %	5 %	13 %
Bildungswesen	13 %	32 %	4 %	13 %
Einzelhandel	12 %	26 %	4 %	11 %
Energie- und Versorgungs-unternehmen	11 %	22 %	4 %	12 %
Entwicklung	20 %	24 %	2 %	16 %
Fertigungsindustrie	12 %	24 %	4 %	11 %
Finanzdienstleister	12 %	17 %	3 %	11 %
Gastgewerbe/Freizeit	11 %	10 %	4 %	9 %
Geschäftliche Dienstleistungen	12 %	21 %	3 %	11 %
Gesundheitswesen	11 %	19 %	4 %	10 %
Lebensmittel/Getränke	11 %	17 %	4 %	10 %
Rechtsbranche	11 %	10 %	2 %	9 %
Technologien	13 %	22 %	4 %	11 %
Telekommunikation	16 %	21 %	5 %	14 %
Transportwesen	11 %	28 %	4 %	12 %
Unterhaltung/Medien	11 %	16 %	3 %	9 %
Versicherungen	14 %	23 %	3 %	12 %

WEITERE INFORMATIONEN

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

INFORMATIONEN ZU PROOFPOINT

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

proofpoint.

0400-004-01-01 1/21