proofpoint.

JAHRESBERICHT

2020 State of the Phish

Eine umfassende Bestandsaufnahme: Sicherheitsbewusstsein und Bedrohungsabwehr im Fokus

proofpoint.com/de

EINFÜHRUNG

Wissen Sie, wie gut Ihre Anwender mit Begriffen zur Cybersicherheit vertraut sind? Und wie sie mit einer Phishing-E-Mail konfrontiert in der Praxis tatsächlich handeln würden? Kennen Sie die größten Probleme, die IT-Sicherheitsteams durch Phishing-Angriffe entstehen? Und wie steht es um die Methoden, um Social-Engineering-Angriffe abzuwehren? Den Erfolgen und Hindernissen?

Unser sechster jährlicher *State of the Phish*-Bericht bietet erneut umfangreiche Einblicke in den aktuellen Stand der Phishing-Bedrohung. **Sie erfahren mehr über folgende Themen:**

- Wie bewusst sind sich Mitarbeiter der Bedrohung und welche Wissenslücken bestehen, die Ihre Cybersicherheit gefährden könnten
- Mit welchen Folgen von Phishing-Angriffen sehen sich IT-Sicherheitsexperten in Unternehmen konfrontiert und welche Möglichkeiten zur Abwehr dieser Bedrohungen bestehen
- Die Umsetzung von Schulungen zur Steigerung des Sicherheitsbewusstseins bei Proofpoint-Kunden sowie die Möglichkeiten, die Erfolge der Trainings zu ermitteln und zu messen

Der Bericht dieses Jahres umfasst die Analysen von Daten aus unterschiedlichen Quellen, beispielsweise:

Eine Umfrage unter mehr als

3.500

berufstätigen Erwachsenen aus sieben Ländern (USA, Australien, Frankreich, Deutschland, Japan, Spanien und Großbritannien)

Eine Umfrage unter mehr als

600

IT-Sicherheitsexperten aus diesen sieben Ländern

Fast

50 Mio.

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

Mehr als

9 Mio.

verdächtige E-Mails, die von den Endnutzern unserer Kunden gemeldet wurden

Der Begriff „Phishing“ kann unterschiedliche Bedeutungen haben, wir verwenden ihn jedoch allgemein. Im Kontext dieses Berichts umfasst Phishing alle Social-Engineering-E-Mails unabhängig von der jeweiligen böswilligen Absicht (z. B. Umleitung von Anwendern zu gefährlichen Websites, Verteilung von Malware oder Erfassung von Anmeldedaten).

Inhaltsverzeichnis

1 **Im Kopf der Endnutzer:** Wie ist es um das Sicherheitsbewusstsein rund um den Globus bestellt?

2 **Umfrage:** Der Alltag von IT-Sicherheitsexperten

3 **Phishing-Fehlerquoten:** Ein frischer Blick auf frische Daten

4 **Aufgeschlüsselt:** Sensibilisierung von Mitarbeitern für Phishing-Angriffe in der Praxis Aus

5 **Endnutzer-Berichte:** Der Weg zum Nirvana

6 **Der Schlüssel zum Wissen:** Vorteile detaillierter Daten

7 **Fazit:** Nutzen Sie Ihre Daten

8 **Anhang**

ABSCHNITT 1

Im Kopf der Endnutzer: Wie ist es um das Sicherheitsbewusstsein rund um den Globus bestellt?

Wir beginnen den *State of the Phish*-Bericht stets mit einem Blick auf die Sensibilisierung der weltweiten Endnutzer im Bereich Cybersicherheit. In der diesjährigen Umfrage, die wir mithilfe eines Drittanbieters durchgeführt haben, wurden mehr als 3.500 berufstätige Erwachsene aus sieben Ländern (USA, Australien, Frankreich, Deutschland, Japan, Spanien und Großbritannien) befragt.

Wie in vergangenen Jahren bewerteten wir Folgendes:

- Kenntnis typischer Cybersicherheits-Begriffe: Phishing, Ransomware, Malware, Smishing (SMS/Textnachrichten-Phishing) und Vishing (Voice-Phishing)
- Verständnis der Grenzen technischer Schutzmaßnahmen bei der Identifizierung (und Behebung) Malware-bezogener Zwischenfälle
- Möglicher Vorsprung jüngerer Mitarbeiter gegenüber ihren älteren Kollegen bei den Cybersicherheits-Kenntnissen

In diesem Jahr haben wir Fragen zu weiteren Verhaltensweisen und Annahmen in den Katalog aufgenommen. Unsere Beobachtung war, dass viele Mitarbeiter auch weiterhin keine Ahnung haben, was zu tun ist, wenn eine mögliche Phishing-E-Mail im Postfach ankommt. Diese Wissenslücken verschärfen die Phishing-Bedrohung und schwächen die allgemeine Sicherheit in Ihrem Unternehmen.

Dieser Abschnitt umfasst folgende Themen:

- Smartphone- und WLAN-Nutzung
- Kennwort-Management
- VPN-Verwendung (Virtual Private Network)
- Verwendung unternehmenseigener Geräte für private Aktivitäten

Wir stellen weltweite Durchschnittswerte vor und weisen auf regionale Abweichungen und andere nennenswerte Auffälligkeiten hin. Im Anhang finden Sie eine Aufschlüsselung nach Ländern für alle Fragen.

Typische Begriffe: Verstehen Ihre Anwender, worüber Sie sprechen?

Mitarbeiter in der IT und Informationssicherheit fragen sich immer wieder: Wer weiß eigentlich *nicht*, was Phishing ist? Die Antwort ist (leider) immer wieder: sehr viele Menschen.

Viele Anwender haben zumindest eine vage Vorstellung von den Bedrohungen durch schädliche Software, E-Mails, Textnachrichten und Telefonanrufe. Ihnen fehlt jedoch das Wissen um die jeweiligen „offiziellen" Begriffe, sodass Sie und Ihre Anwender bei kritischen Sicherheitsproblemen häufig nicht die gleiche Sprache sprechen. Wenn Sie Sicherheitsschulungen in Ihrem Unternehmen einführen wollen, vorher aber die Kenntnisse oder Wissenslücken Ihrer Anwender nicht kennen, ist der Erfolg Glücksache.

In unserer Umfrage sollten Anwender wichtige Begriffe rund um das Thema Cybersicherheit definieren und konnten dazu zwischen drei Multiple-Choice-Antworten plus einer „Weiß nicht"-Option wählen. Falsche bzw. „Weiß nicht"-Antworten zeigen deutlich, dass die Anwender im Unternehmen die wichtigsten Begriffe rund um das Thema Cybersicherheit nicht kennen.

Was ist
PHISHING?

Richtig	Falsch	Weiß nicht
61 %	24 %	15 %

Nur 49 % der Angestellten in den USA beantworteten diese Frage richtig.

Deutsche Angestellte lagen mit 66 % am häufigsten richtig.

Was ist
RANSOMWARE?

Richtig	Falsch	Weiß nicht
31 %	31 %	38 %

Im vergangenen Jahr konnten 45 % der Angestellten in aller Welt diese Frage richtig beantworten. Dieser Rückgang beim Wissen könnte daraus resultieren, dass Ransomware-Angriffe im Jahr 2018 erheblich zurückgingen. Möglicherweise haben IT-Sicherheitsteams dieses Thema deshalb seltener gegenüber den Anwendern thematisiert.

Was ist
MALWARE?

Richtig	Falsch	Weiß nicht
66 %	17 %	17 %

Fast 80 % der Angestellten in Spanien beantworteten diese Frage richtig.

Fast 30 % der Angestellten in den USA glauben, dass Malware eine Art von Hardware wäre, die WLAN-Signale verstärkt.

Was ist
SMISHING?

Richtig	Falsch	Weiß nicht
30 %	21 %	49 %

Die Bekanntheit dieses Begriffs ist im Jahresvergleich gestiegen. In unserer vorherigen Umfrage konnten nur 25 % der Teilnehmer diese Frage richtig beantworten.

Französische Angestellte erzielten die besten Ergebnisse: 54 % beantworteten die Frage richtig.

Was ist
VISHING?

Richtig	Falsch	Weiß nicht
25 %	22 %	53 %

Im vergangenen Jahr konnten nur 18 % der Angestellten in aller Welt diese Frage richtig beantworten.

Mit 48 % kannten französische Angestellte diesen Begriff etwa doppelt so häufig wie der weltweite Durchschnitt.

INTERNATIONAL

14 %

der britischen Angestellten sperren niemals ihre Smartphones.

45 %

der US-amerikanischen Angestellten glauben, dass öffentliche WLAN-Netzwerke an vertrauenswürdigen Orten immer sicher sind.

21 %

der britischen Angestellten wissen nicht, wie sie ihre WLAN-Netzwerke zu Hause vollständig absichern können.

Cybersicherheit am Arbeitsplatz: Wie stark gefährden Angestellte ihre Arbeitgeber?

E-Mail-Sicherheit sollte für Privatpersonen und Unternehmen gleichermaßen an höchster Stelle stehen. Anwender müssen jedoch verstehen, dass auch Entscheidungen, die sie außerhalb ihres E-Mail-Posteingangs treffen, das Risiko von Phishing-Angriffen und anderen Attacken auf sie selbst (und Ihr Unternehmen) erhöhen.

Smartphones und WLAN: Potenzielle Schwachstellen

Fast alle Umfrageteilnehmer (95 %) nutzen ein Smartphone und 41 % verwenden ihre Geräte für private und berufliche Aktivitäten. So schützen sie diese Geräte (weitere Einzelheiten im Anhang):

- 42 % der Smartphone-Besitzer nutzen eine biometrische Sperre (z. B. einen Fingerabdruckleser).
- 24 % entsperren ihr Gerät mit einer vierstelligen PIN.
- 10 % nutzen keine Sperre auf ihrem Gerät.

WLAN-Netzwerke sind ebenfalls problematisch. Offene Netzwerke sind praktisch überall zu finden und werden sowohl für private als auch berufliche Zwecke bereitwillig genutzt (oftmals, um Gebühren für Datenübertragungen zu vermeiden). Die Normalität der Nutzung suggeriert fälschlicherweise, dass öffentliche WLAN-Netze vertrauenswürdig wären.

- 26 % der weltweiten Umfrageteilnehmer glauben so auch, dass die Nutzung öffentlicher WLAN-Netzwerke an vertrauenswürdigen Orten sicher ist, z. B. in örtlichen Cafés oder an internationalen Flughäfen.
- 17 % sind sich nicht sicher, ob sie offenen WLANs an bekannten Orten vertrauen können.

Doch öffentliche Hotspots sind nicht die einzige Gefahrenquelle im Zusammenhang mit WLANs. Das Arbeiten per Remote-Zugriff nimmt immer mehr zu, sodass die Sicherheit des WLANs der Mitarbeiter zu Hause direkte Auswirkungen auf die Sicherheit Ihrer Unternehmensdaten und -systeme haben kann.

Laut unserer Umfrage nutzen 95 % der Mitarbeiter ihr WLAN zu Hause für berufliche Zwecke. Aber sind diese Netzwerke auch ausreichend geschützt? Urteilen Sie selbst:

- 49 % schützen ihr Netzwerk mit einem Kennwort.
- 45 % der Umfrageteilnehmer haben den Namen ihres WLAN-Netzwerks personalisiert.
- 31 % haben das Standardkennwort ihres WLAN-Routers geändert.
- 19 % haben die Firmware ihres WLAN-Routers überprüft bzw. aktualisiert.
- 14 % wissen nicht, wie sie WLAN-Sicherheitsmaßnahmen umsetzen können.
- 11 % finden die Implementierung von WLAN-Sicherheitsmaßnahmen zu zeitaufwändig bzw. zu unbequem.

DIE FAKTEN

Fast 90 % der Umfrageteilnehmer sichern wichtige Dateien in Cloud-Speichern, auf externen Laufwerken oder in unterschiedlichen Datenspeichern. Das ist zwar eine begrüßenswerte Maßnahme zum Schutz vor Ransomware, doch Unternehmen müssen stets wissen, wo ihre Daten gespeichert werden.

INTERNATIONAL

44 %

der US-amerikanischen Teilnehmer nutzen einen Kennwort-Manager. Das ist deutlich mehr als der weltweite Durchschnitt.

15 %

der französischen Umfrageteilnehmer nutzen einen Kennwort-Manager – im weltweiten Vergleich ist das der niedrigste Wert.

US-Teilnehmer nutzen VPNs am häufigsten:

Bei **51 %** ist mindestens ein VPN installiert. **63 %** der Befragten, die ein VPN besitzen, nutzen es immer.

VS.

Französische Teilnehmer nutzen VPN am seltensten: Nur bei **35 %** ist ein VPN installiert.

Japanische Angestellte kennen sich am wenigsten mit VPNs aus: Nur **37 %** wissen, was ein VPN überhaupt ist.

Technische Schutzmaßnahmen: Fehlgeleitetes Vertrauen

Mitarbeiter gehen häufig von falschen Annahmen aus. Dies ist einer der Hauptgründe für riskantes Verhalten und hat negative Auswirkungen auf die Cybersicherheit. Wie wir festgestellt haben, gehen Arbeitnehmer häufig fälschlicherweise davon aus, dass technische Schutzmaßnahmen auf privaten und unternehmenseigenen Geräten absolut sicher sind:

- 66 % der Umfrageteilnehmer glauben, dass sie mit einer aktuellen Virenschutzlösung Zugriffe von Cyberkriminellen auf ihre Geräte verhindern können.
- 51 % sind der Meinung, dass ihre IT-Teams automatisch benachrichtigt werden, wenn die Anwender versehentlich einen Virus oder eine andere schädliche Software auf ihrem beruflich genutzten Computer installieren.

Kennwörter und VPNs: Falsch verstanden und falsch genutzt

Kennwörter sind für IT- und Sicherheitsteams eine weitere Quelle für Ärgernisse. Das größte Problem ist dabei die Neigung vieler Anwender, ihre Kennwörter mehrfach zu verwenden. Glücklicherweise haben wir festgestellt, dass die Hälfte der Umfrageteilnehmer diese gefürchtete Praxis vermeidet – allerdings nur eine sehr knappe Hälfte.

Kennwort-Gewohnheiten

nutzen einen Kennwort-Manager.

geben bei jeder Anmeldung manuell ein anderes Kennwort ein.

wechseln zwischen fünf bis zehn unterschiedlichen Kennwörtern.

verwenden die gleichen ein oder zwei Kennwörter für alle Konten.

VPNs bieten eine einfache Möglichkeit, vertrauliche Daten und Konten zu schützen. Leider ist das vielen Anwendern – und anscheinend auch deren Arbeitgebern – bisher entgangen.

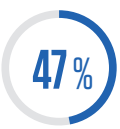
VPN-Nutzung auf unternehmenseigenen und privaten Geräten

nutzen ein VPN für ein oder mehrere Geräte.

glauben nicht, dass sie ein VPN nutzen müssen.

wissen nicht, was ein VPN ist.

VPN-Nutzung nach der Installation



nutzen ihr VPN immer.

nutzen ihr VPN häufig.

nutzen ihr VPN nur bei Bedarf.

nutzen ihr VPN nie.

DIE FAKTEN

ca. 50 %

der Umfrageteilnehmer lassen zu, dass Freunde und Familie auf ihre vom Arbeitgeber gestellten Geräte zugreifen.

INTERNATIONAL

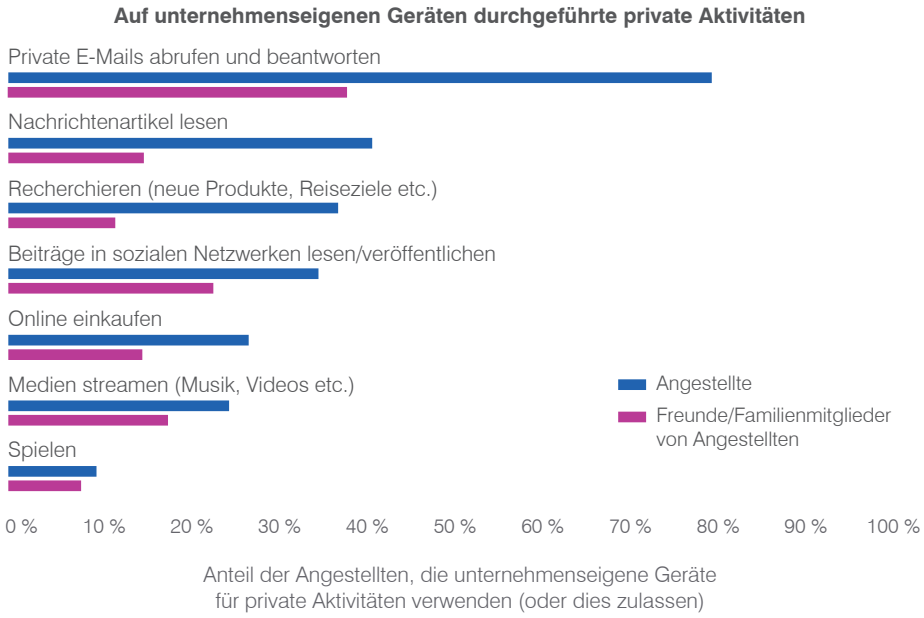
61 %

der US-amerikanischen Angestellten lassen Freunde und Familie ihre unternehmenseigenen Geräte nutzen – und damit doppelt so häufig wie Umfrageteilnehmer in Japan und Deutschland.

Unternehmenseigene Geräte: Wissen Sie, wo sie waren?

Die meisten Unternehmen legen für unternehmenseigene Geräte verbindliche Richtlinien für die zulässige Nutzung fest. Doch sofern der Zugriff nicht vollständig gesperrt ist, gibt es keine Möglichkeit zu erkennen, ob die Angestellten diese Richtlinien wirklich befolgen. Und wie das Diagramm zeigt, nutzen Arbeitnehmer ihre Geräte für private Aktivitäten. Wenn Ihre Mitarbeiter nicht ausreichend darüber geschult wurden, wie sie auf sichere Weise mit E-Mails, Websites und sozialen Netzwerken interagieren, können ihre Aktionen Sicherheitsrisiken nach sich ziehen.

Gleichzeitig ist es sicherlich besonders besorgniserregend, dass die Freunde und Familie von Mitarbeitern Zugriff auf die PCs und Smartphones Ihres Unternehmens haben. Obwohl 51 % der Umfrageteilnehmer mit unternehmenseigenen Geräten angaben, keine externen Zugriffe zuzulassen, gestatten viele Menschen ihren Nächsten (einschließlich Kindern) die Nutzung der Geräte für verschiedenste Aktivitäten.



Generationenwandel in der Belegschaft: Führen jüngere Mitarbeiter zu mehr Cybersicherheit im Unternehmen?

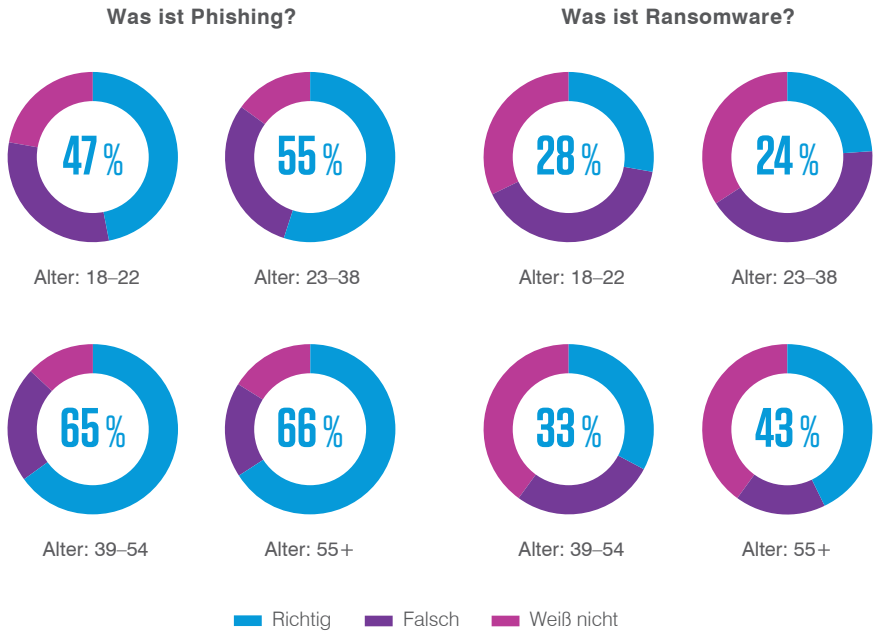
Für heutige jüngere Mitarbeiter sind intelligente Geräte und Anwendungen nicht aus dem Alltag wegzudenken. Da immer mehr technikaffine Menschen auf den Arbeitsmarkt strömen, könnte man annehmen, dass jüngere Angestellte ein tieferes Verständnis für Cybersicherheit mitbringen.

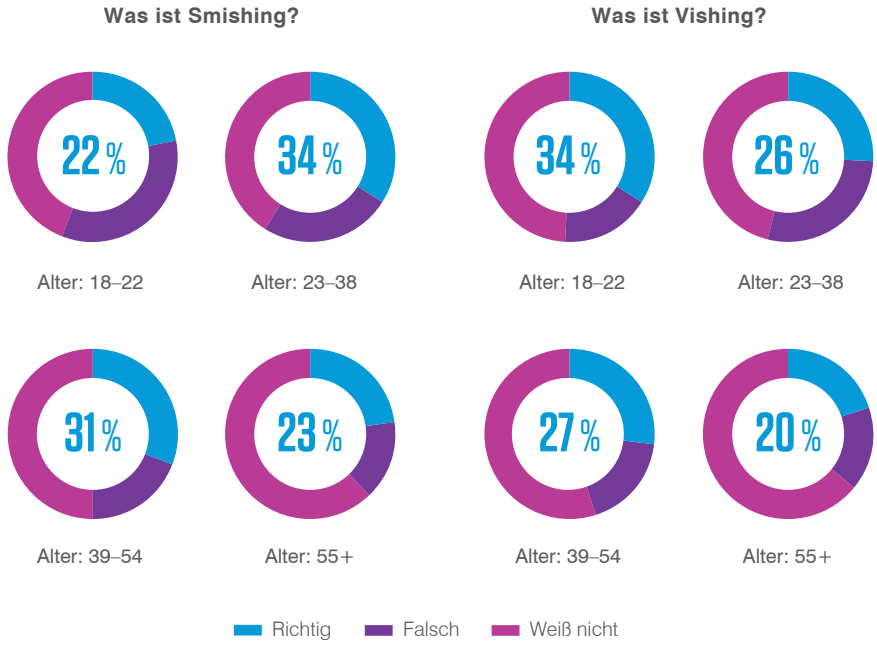
Das ist jedoch nicht immer der Fall. So schneiden jüngere Arbeitnehmer und die viel diskutierte Millenial-Generation gegenüber älteren Mitarbeitern (einschließlich den Baby-Boomern) bei sechs wichtigen Fragen ab.[1]

[1] Laut Pew Research sind Millennials 23 bis 38 Jahre alt, während Baby-Boomer im Jahr 2019 – als unsere Umfrage durchgeführt wurde – mindestens 55 Jahre alt sind.

DIE FAKTEN

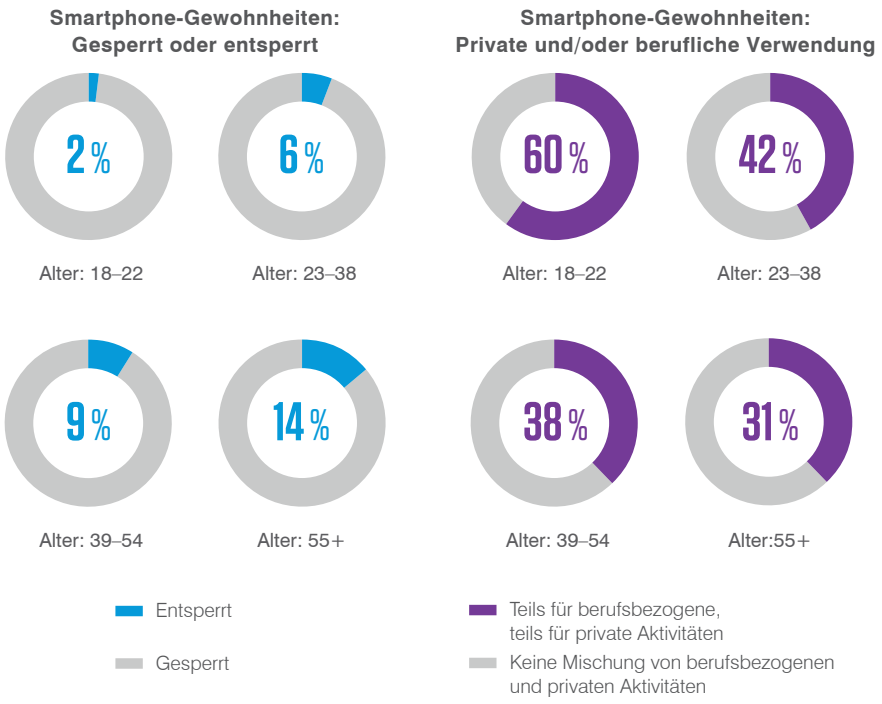
Bei der Erkennung der Phishing- und Ransomware-Begriffe lagen Baby-Boomer an der Spitze. Millennials waren lediglich bei einem einzigen Begriff führend: *Smishing.*





DIE FAKTEN

Alle Umfrageteilnehmer in der Altersgruppe 18 bis 22 Jahre nutzen ein Smartphone – und für die meisten Befragten gibt es keine klare Linie zwischen privater und beruflicher Nutzung ihrer Geräte. Da diese Menschen auf dem weltweiten Arbeitsmarkt eine immer größere Rolle spielen, werden Sicherheitsmaßnahmen für Mobilgeräte wichtiger als je zuvor sein.



Wichtigster Punkt: Keine falschen Vorurteile

Die Ergebnisse solcher Umfragen können sich von Jahr zu Jahr unterscheiden. Der Grund dafür ist einfach: In jedem Jahr werden unterschiedliche Teilnehmer befragt, was zu unterschiedlichen Antworten führt.

Das Gleiche geschieht auch am Arbeitsplatz.

Die meisten Unternehmen verzeichnen von Jahr zu Jahr zumindest ein gewisses Maß an Mitarbeiterfluktuation. Das bedeutet auch, dass es stets sicherheitstechnisch affine sowie weniger gut geschulte Angestellte geben wird. Wir sehen an unseren Umfrageergebnissen, dass jüngere Mitarbeiter nicht immer über die für Ihr Unternehmen wichtigsten Cybersicherheitskenntnisse verfügen. Gleichzeitig sollten Sie erst dann davon ausgehen, dass *irgendjemand* gut informiert ist, wenn Sie dessen Kompetenzen geprüft und Wissenslücken geschlossen haben.

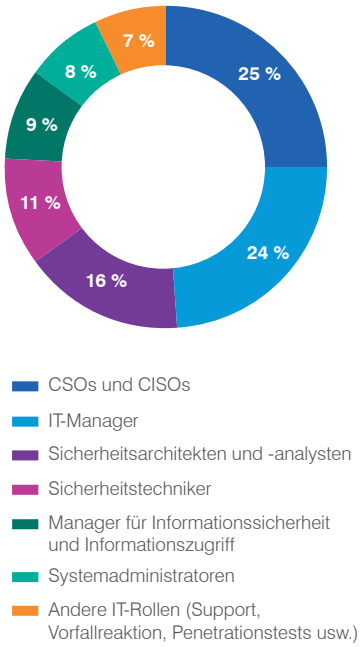
Deshalb ist auch die Einbindung von Sicherheitsschulungen in das Onboarding Ihrer Mitarbeiter unverzichtbar. Damit wird auch klargestellt, dass Cybersicherheit auf allen Unternehmensebenen wichtig ist. Sie sollten kontinuierlich Cybersicherheitsschulungen durchführen, anstatt die Kenntnisse über Monate (oder gar ein ganzes Jahr) verkümmern zu lassen. Wenn Sie der Cybersicherheit keine Priorität einräumen, werden Ihre Mitarbeiter das auch nicht tun.

ABSCHNITT 2

Umfrage: Der Alltag von IT-Sicherheitsexperten

Sie können die Bedrohungslandschaft nur dann wirklich verstehen, wenn Sie die Probleme von IT-Sicherheitsexperten im Zusammenhang mit Phishing kennen. Verwertbare Bedrohungsdaten sind wichtig, existieren jedoch nicht im luftleeren Raum. Auch Bedrohungsdaten zum Faktor Mensch sind unverzichtbar – und diese beziehen sich nicht nur auf das Endnutzerverhalten.

Umfrageteilnehmer



Dabei geht es auch darum, was die Mitarbeiter an der vordersten Front der Cybersicherheit im Unternehmen erleben, wie sie auf Angriffe reagieren und mit welchen Schritten sie ihre Sicherheitslage verbessern.

In diesem Jahr befragten wir mehr als 600 IT-Sicherheitsexperten aus sieben Ländern: USA, Australien, Frankreich, Deutschland, Japan, Spanien und Großbritannien. Dabei wurde eine repräsentative Gruppe unterschiedlicher IT-Sicherheitsrollen aus mehr als 20 Branchen angesprochen.

Die sich daraus ergebenden unterschiedlichen Sichtweisen sind wichtig. Die Verantwortung für Cybersicherheitsschulungen kann auf mehrere Mitarbeiter in einem Unternehmen verteilt sein und verschiedene Sicherheitsrollen umfassen. Wir befragten alle Umfrageteilnehmer zu den folgenden Phishing- und Social-Engineering-Problemen:

- Die Raten erfolgreicher Phishing-Angriffe und die sich daraus ergebenden Auswirkungen
- Das Aufkommen von Spearphishing-Angriffen (die sich gegen ausgewählte Ziele richten) sowie Business Email Compromise-Attacken (BEC) im Jahr 2019
- Auftreten von Ransomware-Infektionen im Jahr 2019 sowie der Umgang mit Lösegeldforderungen
- Das Aufkommen „alternativer“ Social-Engineering-Versuche (Smishing, Vishing, ausgelegte infizierte USB-Sticks und Angriffe über soziale Netzwerke) im Jahr 2019
- Berechnungsmethode für die Kosten von Phishing-Angriffen
- Maßnahmen für Schulungen zur Steigerung des Sicherheitsbewusstseins
- Einsatz von Konsequenzmodellen bei Endnutzern, die regelmäßig auf Phishing-Angriffe hereinfallen

Wie im vorherigen Abschnitt werden auch hier weltweite Durchschnittswerte und regionale Besonderheiten herausgestellt. Im Anhang finden Sie eine Aufschlüsselung nach Ländern für alle Fragen.

INTERNATIONAL

65 %

der US-amerikanischen Unternehmen verzeichneten im vergangenen Jahr mindestens einen erfolgreichen Phishing-Angriff, was deutlich über dem weltweiten Durchschnitt von 55 % liegt.

42 %

der japanischen Unternehmen verzeichneten 2019 einen erfolgreichen Phishing-Angriff. Das ist die geringste Rate unter allen untersuchten Regionen.

54 %

der US-amerikanischen Unternehmen verzeichneten erfolgreiche Anmeldedaten-Phishing-Angriffe, was über dem weltweiten Durchschnitt von 47 % liegt.

DIE FAKTEN

Japanische Unternehmen stellten nach einem erfolgreichen Phishing-Angriff am häufigsten Datenverluste und finanzielle Schäden fest. Das stimmt auch mit unseren Bedrohungsdaten überein, laut denen japanische Unternehmen am häufigsten mit Bank-Trojanern angegriffen werden, die Datenexfiltration ermöglichen.

59 % der japanischen Unternehmen stellten nach einem Phishing-Angriff Datenverluste fest.

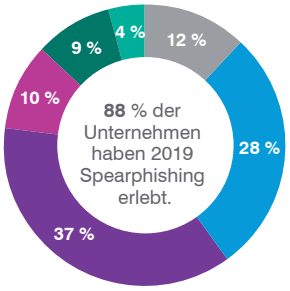
45 % erlitten finanzielle Verluste.

Zwischenfälle und Auswirkungen: Das war Phishing im Jahr 2019

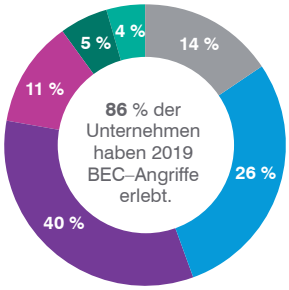
Mehr als die Hälfte (ca. 60 %) der weltweiten Umfrageteilnehmer verzeichneten im Jahr 2019 genauso viele oder weniger Phishing-Angriffe als 2018. Das passt zu einer Entwicklung, die wir (und andere) schon seit einer Weile beobachten: Die Angreifer konzentrieren sich auf Qualität statt Quantität.

Cyberkriminelle wählen immer häufiger gezielte und personalisierte Angriffe statt Massen-Kampagnen, was sich auch in der Zahl gezielter Attacken auf die Unternehmen unserer Umfrageteilnehmer im Jahr 2019 widerspiegelt:

Aufkommen der Spearphishing-Angriffe



Aufkommen der BEC-Angriffe

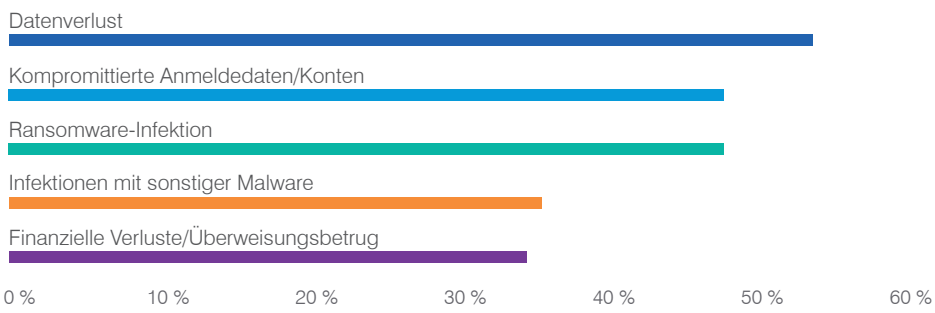


Angriffsversuche sind jedoch nicht das Gleiche wie erfolgreiche Angriffe. Mehr als die Hälfte (55 %) der Umfrageteilnehmer berichtete, dass ihr Unternehmen im Jahr 2019 mindestens einen – für den Cyberkriminellen – erfolgreichen Phishing-Angriff verzeichnete.

Auswirkungen von Phishing auf Unternehmen

Phishing-Angriffe erfolgen gezielt und die Cyberkriminellen verfolgen bei ihrem Angriff ein ganz konkretes Ziel. Die Umfrageteilnehmer erlebten durch erfolgreiche Phishing-Angriffe im Jahr 2019 folgende Auswirkungen. (Mehrere Antworten waren zulässig.)

Folgen erfolgreicher Phishing-Angriffe



Ransomware: Griff nach den Schlagzeilen (und Bankkonten) im Jahr 2019

INTERNATIONAL

60 %

der australischen Unternehmen verzeichneten durch Phishing ausgelöste Ransomware-Infektionen – der höchste Wert unter allen untersuchten Regionen.

55 %

der spanischen Unternehmen verzeichneten Malware-Infektionen aufgrund von Phishing-Angriffen, was deutlich über dem weltweiten Durchschnittswert von 35 % lag.

Obwohl das Aufkommen E-Mail-basierter Ransomware-Angriffe in den letzten Jahren deutlich zurückging, überrascht es nicht, dass IT-Sicherheitsexperten für 2019 einen starken Anstieg bei Infektionen durch Phishing feststellten.

Im vergangenen Jahr erwies sich vor allem das Ransomware-as-a-Service-Angebot GandCrab für viele Unternehmen als Plage. Berichten zufolge soll die Malware 2 Milliarden US-Dollar an Lösegeld eingebracht haben, bevor sie stillgelegt wurde, nachdem ihre Schöpfer sich angeblich „zur Ruhe setzten“.[2]

Abgesehen von GandCrab scheint es sich bei vielen aktuell bekannt gewordenen Ransomware-Angriffen um Sekundärinfektionen von Unternehmen zu handeln, die zuvor bereits mit anderer Malware infiziert wurden. Obwohl also durch E-Mails verursachte Ransomware-Infektionen zurückgingen, bleibt das Problem für viele IT-Sicherheitsexperten auch weiterhin aktuell.

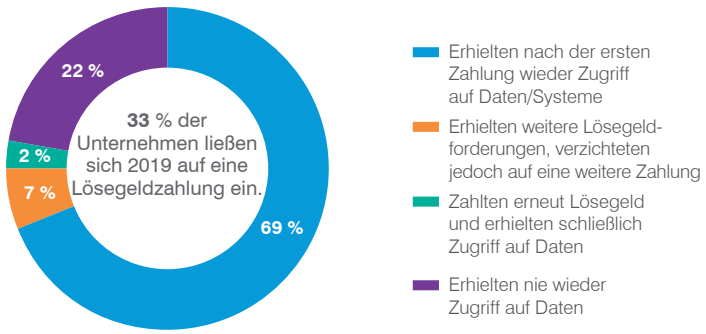
Aus Sicht der Angreifer besteht der Vorteil einer erfolgreichen Ransomware-Infektion darin, dass sie die Opfer unter Zeitdruck setzt. Unternehmen aus dem Gesundheitswesen sowie staatliche und lokale Behörden wurden 2019 besonders hart getroffen. Ransomware kann kritische Infrastrukturen lahmlegen und wichtige (oder sogar lebenswichtige) Dienste können nicht mehr aufrechterhalten werden. In einer solchen Situation kann ein Unternehmen schnell zu dem Schluss gelangen, dass die Zahlung des Lösegeldes die zweckmäßigste – und preiswerteste – Methode ist, den Betrieb wieder aufzunehmen.

Wir fragten unsere Umfrageteilnehmer nach ihren allgemeinen Erfahrungen mit Ransomware im Jahr 2019. Das sind die Ergebnisse:

- 33 % der Unternehmen wurden mit Ransomware infiziert und zahlten das Lösegeld.
- 32 % wurden infiziert, zahlten das Lösegeld jedoch nicht.

Von den Unternehmen, die das Lösegeld zahlten, lernten viele sehr schnell eine alte Lektion: Es gibt keine Ehre unter Dieben.

Auswirkungen von Ransomware-Zahlungen



[2] Catalin Cimpanu (*ZDNet*): „GandCrab ransomware operation says it's shutting down“ (GandCrab-Ransomware-Operation will sich angeblich selbst beenden), Juni 2019.

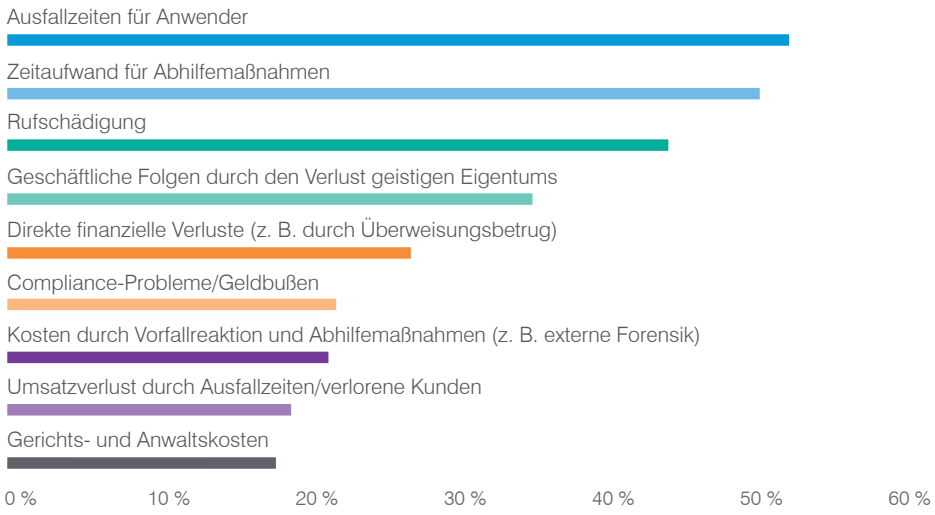
Aufgrund von Datenschutzvorschriften kann es Vorgaben dahingehend geben, was Unternehmen auf Ebene einzelner Mitarbeiter ermitteln dürfen. Unternehmen weltweit können jedoch die finanziellen Folgen von Phishing-Angriffen insgesamt abschätzen. Das Gleiche gilt auch für den Mehrwert von Schulungen zur Steigerung des Sicherheitsbewusstseins.

93 %
der Unternehmen berechnen die Kosten von Phishing-Angriffen.

Erfolgreiche Phishing-Angriffe: Die Kosten

Abgesehen von all ihren unmittelbaren Auswirkungen führen erfolgreiche Phishing-Angriffe stets auch zu finanziellen Einbußen. Der größte Teil (93 %) der Umfrageteilnehmer gab an, dass ihr Unternehmen diese Kosten in einem gewissen Maße erfasst. Wie Sie im Diagramm sehen können, lassen sich finanzielle Schäden auf eine Reihe von Ursachen zurückführen – von beeinträchtigter Produktivität bis hin zu unerwarteten (und unbeabsichtigten) Ausgaben. (Mehrere Antworten waren zulässig.)

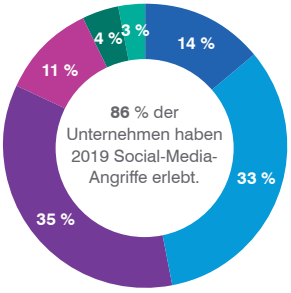
So berechnen Unternehmen die Kosten von Phishing-Angriffen



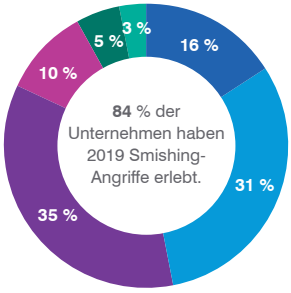
Social Engineering jenseits des Posteingangs

Für Cyberkriminelle sind und bleiben E-Mails der wichtigste Angriffsvektor. Doch die Angreifer nutzen die gleichen Social-Engineering-Techniken auch für andere Ansätze, mit denen sie Anwender hinters Licht führen. Viele Unternehmen verzeichneten im Jahr 2019 ein hohes Aufkommen verschiedener Social-Engineering-Angriffe.

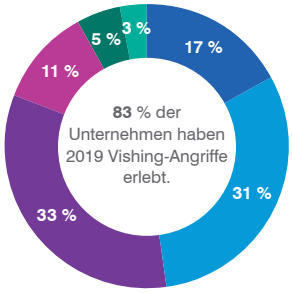
Aufkommen der Social-Media-Angriffe



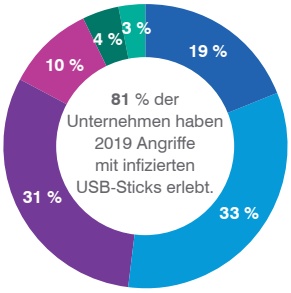
Aufkommen der Smishing-Angriffe



Aufkommen der Vishing-Angriffe



Aufkommen abgelegter mit Schadsoftware infizierter USB-Sticks



INTERNATIONAL

Spanische Unternehmen waren 2019 erheblich häufiger von diesen „alternativen" Social-Engineering-Angriffen betroffen:

100 %

verzeichneten Angriffe über soziale Netzwerke sowie per Smishing.

99 %

verzeichneten Vishing-Angriffe.

98 %

hatten mit manipulierten USB-Sticks zu tun.

VS.

Australische Unternehmen

66 %

verzeichneten Angriffe über soziale Netzwerke.

62 %

verzeichneten Smishing-Angriffe.

57 %

verzeichneten Vishing-Angriffe.

Britische Unternehmen

52 %

hatten mit manipulierten USB-Sticks zu tun.

Schulungen zur Steigerung des Sicherheitsbewusstseins: Schulung der Anwender, sodass diese nicht auf Phishing-Versuche hereinfallen

95 %

der Unternehmen schulen Mitarbeiter in der Erkennung und Vermeidung von Phishing-Angriffen.

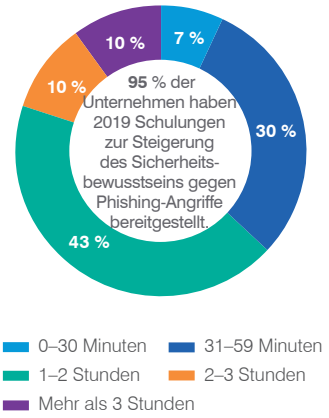
Technische Maßnahmen sind zwar ein unverzichtbarer Teil der Cybersicherheit, können jedoch nicht beeinflussen, wie Menschen sich verhalten. Cyberkriminelle suchen und finden Möglichkeiten, die Anwenderebene zu infiltrieren. Um von den Vorteilen eines personenorientierten Cybersicherheitsansatzes zu profitieren, müssen Sie das Sicherheitsbewusstsein und -verhalten der Anwender verbessern.

Die gute Nachricht dabei ist: 95 % der Umfrageteilnehmer erklärten, dass ihr Unternehmen Schulungen zur Erkennung von Phishing-Versuchen anbietet. Doch wenn wir ihre verwendeten Methoden genauer betrachten, ist das Bild weniger deutlich.

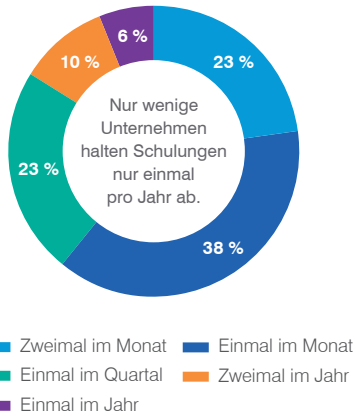
Beispielsweise schulen 30 % der Unternehmen nur einen Teil ihrer Anwender. Für die ungeschulten Endnutzer bleibt die Cybersicherheit deshalb auf der Strecke. (Gezielte Schulungen sind ein unverzichtbarer Teil aller Cybersicherheitsschulungen. Am besten funktionieren sie jedoch im Rahmen eines Programms, das unternehmensweit über bewährte Methoden informiert.)

So implementieren Unternehmen ihre Schulungsprogramme zur Steigerung des Sicherheitsbewusstseins.

Pro Jahr für Schulungen zur Steigerung des Sicherheitsbewusstseins vorgesehene Zeit



Häufigkeit von Schulungen zur Steigerung des Sicherheitsbewusstseins



INTERNATIONAL

Britische Unternehmen investieren am häufigsten in Endnutzerschulungen:

98 %

schulen ihre Mitarbeiter mehr als 30 Minuten im Jahr.

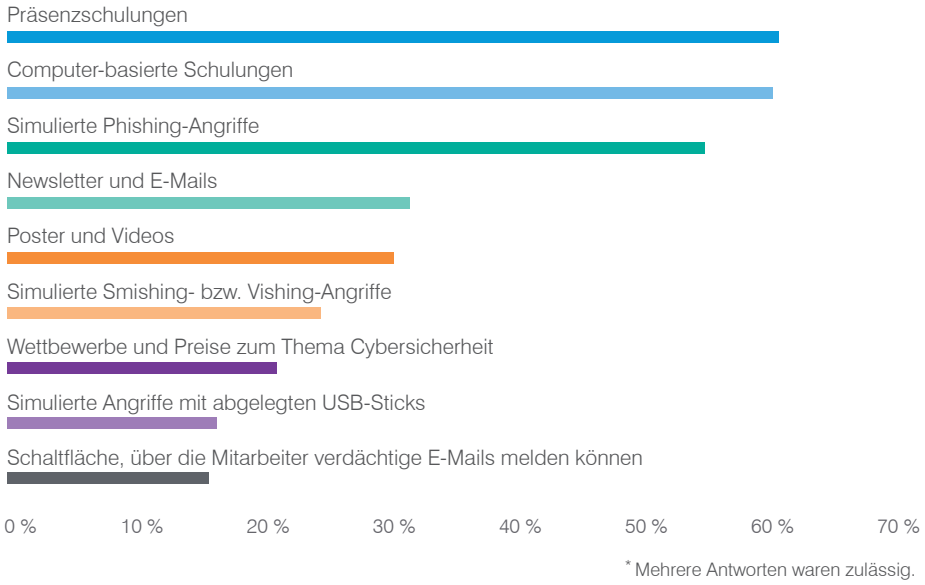
15 %

widmen ihren Programmen drei oder mehr Stunden pro Jahr.

11 %

der australischen Unternehmen führen einmal jährlich Schulungen zur Verbesserung des Endnutzerverhaltens durch.

Maßnahmen von Unternehmen, um das Sicherheitsbewusstsein zu steigern*



* Mehrere Antworten waren zulässig.

Eine stärkere Sensibilisierung ist nicht das Gleiche wie die Verankerung sicherer Verhaltensweisen. „Passive“ Hilfsmittel wie Newsletter, E-Mail-Benachrichtigungen und Poster können die Aufmerksamkeit der Mitarbeiter steigern, sie geben den Mitarbeitern jedoch keine Möglichkeit, ihre Entscheidungsfindung in Bezug auf die Cybersicherheit zu üben.

Wie im Diagramm oben gezeigt, bieten nur 60 % der Unternehmen ihren Anwendern formelle Cybersicherheitsschulungen an. Dieser Anteil ist erschreckend gering. Fehlende formelle Schulungen sowie augenscheinliche Schwächen, wenn es um die Möglichkeit für Endnutzer geht, verdächtige E-Mails zu melden, untergraben die Sicherheitslage von Unternehmen.

Konsequenzmodelle: Sind Strafen angemessen?

DIE FAKTEN

63 %

der Unternehmen bestrafen Anwender, die regelmäßig auf Phishing-Angriffe hereinfallen.

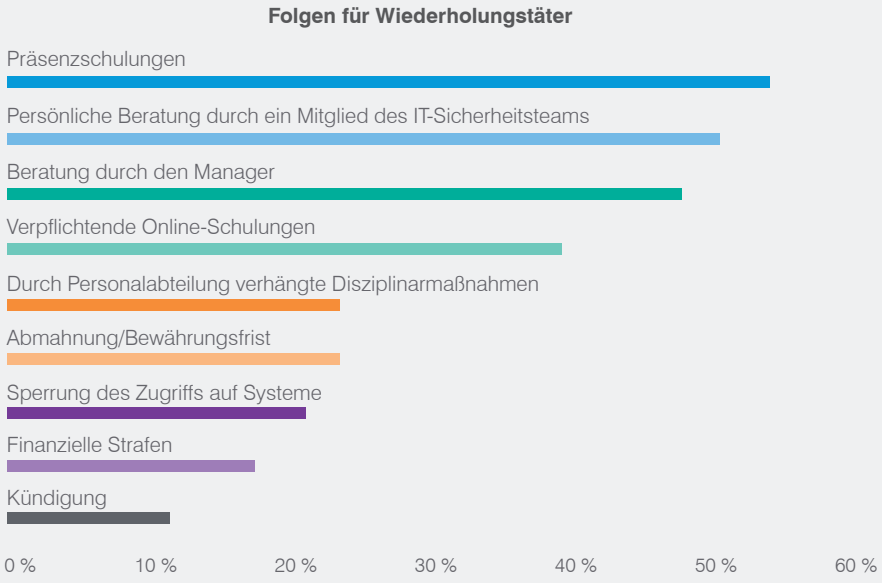
Die Frage nach „Zuckerbrot und Peitsche“ als Reaktion auf Sicherheitsfehler von Anwendern löst heftige Reaktionen bei Vertretern beider Lager aus – mit jeweils überzeugenden Argumenten. Unabhängig davon, wo Sie selbst stehen, sollten Sie Konsequenzmodelle kennen und in Ihrer Entscheidungsfindung berücksichtigen.

Laut unserer Umfrage haben 63 % der Unternehmen Strafmaßnahmen für Anwender implementiert, die regelmäßig Fehler begehen. Bei unserer Frage nutzten wir bewusst den Begriff „Strafe“. Warum? Weil die Wahrnehmung eine wichtige Rolle spielt. Wir würden uns nie gegen Gespräche mit Mitarbeitern oder Folgeschulungen für solche Endnutzer aussprechen, die wiederholt fingierten oder echten Phishing-Angriffen auf den Leim gehen. Doch wenn diese zusätzlichen Schulungsmaßnahmen als Strafen eingestuft (oder sogar noch weitergehende Maßnahmen verhängt werden), kann das dazu führen, dass Anwender diesen Schulungsprogrammen mit Misstrauen, Angst oder gar Ärger begegnen.

WIE HILFREICH SIND STRAFEN?

Bei der überwiegenden Mehrzahl der Unternehmen (84 %), die auf Strafen setzen, hat sich die Aufmerksamkeit der Mitarbeiter nach der Einführung eines Konsequenzmodells verbessert.

Die folgenden Strafen werden in Unternehmen mit einem Konsequenzmodell für „Wiederholungstäter“ verhängt. (Mehrere Antworten waren zulässig.)



78 %

der Unternehmen geben an, dass Schulungen zur Steigerung des Sicherheitsbewusstseins die Anfälligkeit für Phishing verringern.

Wichtigster Punkt: Zeit und Aufwand spielen eine Rolle

Phishing ist wie ein vielköpfiges Ungeheuer. Die Auswirkungen und Kosten erfolgreicher Angriffe sind erheblich und mit hohen Schäden verbunden. Cyberkriminelle arbeiten intensiv daran, ihre Techniken zu optimieren und die Mitarbeiter Ihres Unternehmens noch erfolgreicher anzugreifen. Bereiten Sie Ihre Anwender ebenso intensiv auf die Abwehr dieser Angriffe vor?

Es ist erfreulich zu sehen, dass die Schulungen zur Steigerung des Sicherheitsbewusstseins bei 78 % der Unternehmen zu einer messbar geringeren Anfälligkeit für Phishing geführt haben. Der Erfolg Ihres Unternehmens hängt dabei maßgeblich vom Zeit- und Arbeitsaufwand ab, den Sie in die Verbesserung der Endnutzerkenntnisse investieren.

ABSCHNITT 3

Phishing-Fehlerquoten: Ein frischer Blick auf frische Daten

Als wir zum ersten Mal die Phishing-Tests unserer Kunden analysierten und Berichte dazu erstellten, basierte unser Datensatz auf etwas mehr als 4,5 Millionen simulierten Phishing-Angriffen.[3] Der diesjährige Datensatz ist mit fast 50 Millionen Phishing-Tests um einige Größenordnungen umfangreicher – ein Hinweis darauf, wie viel sich in den letzten Jahren bei Schulungen zur Erkennung von Phishing-Versuchen getan hat. Die Zunahme ist sowohl auf den größeren Kundenstamm als auch auf umfassendere Schulungen in Unternehmen zurückzuführen.

Aufgrund dieses Wandels ist eine neue Betrachtung unserer Daten und unserer Berichte erforderlich.

9 %

Durchschnittliche Fehlerquote bei den aggregierten Anwendern für alle gesendeten Tests

VS.

12 %

Durchschnittliche Fehlerquote bei den Unternehmen für alle gesendeten Tests

Berechnung von Fehlerquoten: Benutzer- oder Unternehmensebene

In früheren Ausgaben des *State of the Phish*-Berichts berechneten wir die durchschnittliche Fehlerquote auf Anwenderebene. Dazu verglichen wir die Gesamtanzahl der Fehler mit der Gesamtanzahl der gesendeten simulierten Angriffe. Als wir diese Berechnungen mit den diesjährigen Daten durchführten, ermittelten wir eine Fehlerquote von 9 % – so wie in unseren beiden vorherigen Berichten auch.

Es gibt jedoch unterschiedliche Methoden zur Berechnung von Fehlerquoten. (Das haben Sie vielleicht schon beim Blick in andere Branchenuntersuchungen festgestellt.) Als wir die Daten des diesjährigen Datensatzes anders betrachteten, stellten wir fest, dass die Fehlerquoten auf Anwenderseite zum Teil erheblich durch „Vielflieger“ beeinflusst werden können. Anwender, die häufig geprüft werden, haben im Allgemeinen geringere Fehlerquoten. Das ist sehr positiv für Unternehmen, die regelmäßig Tests durchführen, aber nicht unbedingt ein realistischer Blick darauf, wie ein durchschnittliches Unternehmen allgemein abschneidet.

Für ein ausgeglicheneres Bild stellt der diesjährige Bericht Fehlerquoten (wenn möglich) sowohl auf Anwender- und Unternehmensebene dar. Für letztere werden alle Unternehmen einheitlich gewichtet, sodass große Unternehmen und umfangreiche Programme die Ergebnisse nicht mehr verfälschen können. Mit diesem Ansatz ermittelten wir eine durchschnittliche Fehlerquote von 12 % unter den Unternehmen, die unsere Phishing-Simulationen nutzen.

Möglicherweise halten Sie die Abweichung von 3 % zwischen diesen Zahlen für unbedeutend. Das wäre ein Fehler, denn die Untersuchung beider Datensätze kann wichtige Informationen zu Schwachstellen auf Unternehmensebene offenlegen – was dieser Bericht immer wieder betont.

[3] Wombat Security Technologies (jetzt Proofpoint): „2016 State of the Phish“ (State of The Phish-Bericht 2016), Januar 2016.

DIE FAKTEN

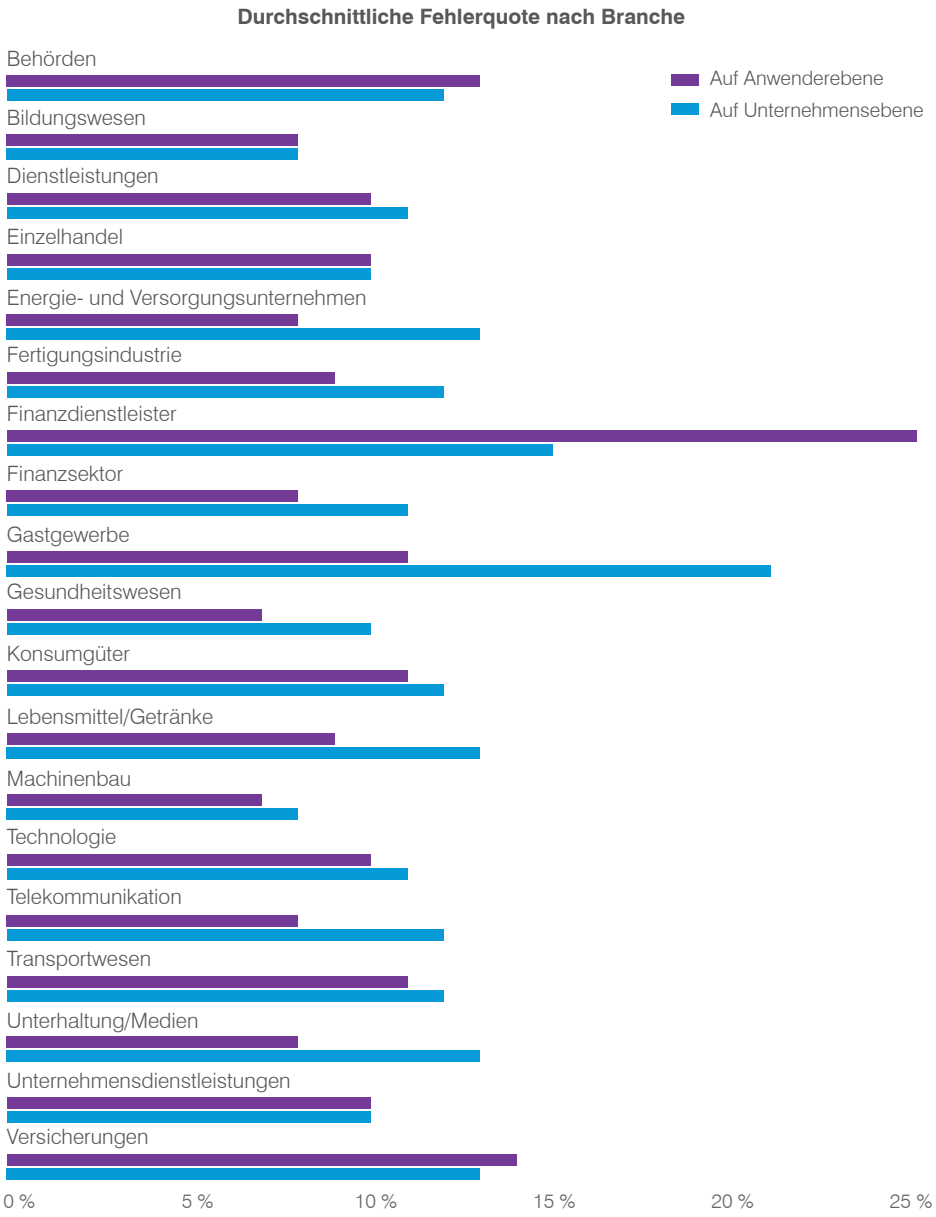
Die Branchen mit den häufigsten Phishing-Tests waren im Jahr 2019 das Gesundheitswesen, Fertigungsunternehmen, Technologieunternehmen, Finanzinstitute sowie Energie- und Versorgungsunternehmen.

Vergleich der Darstellung von Branchen-Fehlerquoten

Beim Vergleich der Fehlerquoten auf Unternehmens- und Anwenderebene nach Branche wird klar, welchen Einfluss umfangreiche Kampagnen auf die durchschnittlichen Fehlerquoten auf Anwenderebene haben können. Beispielsweise liegt die Anwender-Fehlerquote für alle Tests, die im Finanzsektor gesendet wurden, weit über der unternehmensweiten Fehlerquote. Zwei komplexe und umfangreiche simulierte Phishing-Kampagnen, die von einem Unternehmen durchgeführt wurden, ließen die Anwender-Fehlerquote für die gesamte Branche nach oben schießen.

Die Anwenderfehlerraten liegen jedoch meist unter den unternehmensweiten Fehlerquoten – in einigen Fällen sogar deutlich darunter, beispielsweise im Gastgewerbe. Der Grund: Anwender in Unternehmen mit einem umfangreichen Trainingsangebot schneiden meist besser ab als ihre Kollegen in Unternehmen, die weniger Phishing-Tests versenden. Eine größere Zahl besser geschulter Anwender kann sich auf die durchschnittliche Anwender-Fehlerquote auswirken. Die gleiche Gewichtung jedes Unternehmens und die Durchschnittsermittlung ihrer Ergebnisse ermöglicht einen repräsentativeren Blick auf die branchenspezifischen Fehlerquoten.

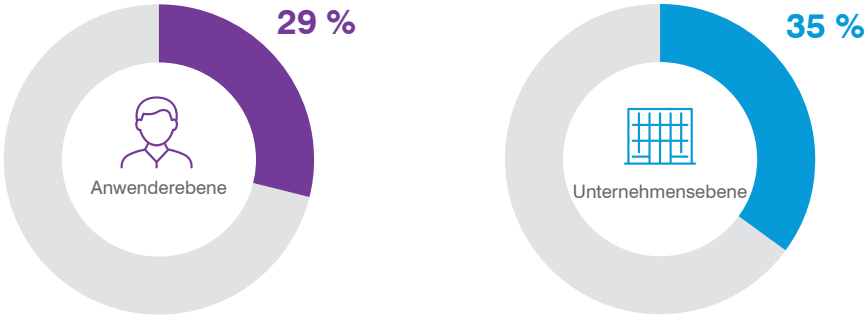
Jede in unserem Fehlerquotenvergleich aufgeführte Branche umfasst Daten von mindestens fünf Unternehmen sowie mindestens 100.000 simulierten Phishing-Angriffen.



Liegen die Fehlerquoten wirklich bei 30 %?

Eine Untersuchung der Fehlerquoten bei den Phishing-E-Mails, die tatsächlich von Anwendern geöffnet wurden, lieferte tatsächlich weitere hilfreiche Erkenntnisse. Diese Kennzahl ist besonders interessant, weil nur geöffnete Phishing-E-Mails eine Chance auf Erfolg haben: Anwender werden nur in diesem Fall tatsächlich angesprochen und können so eventuell auf den Köder hereinfallen.

Nicht jeder simulierte Phishing-Angriff wurde bei jedem Endnutzer angezeigt, doch in Bezug auf die geöffneten Nachrichten stellten wir die folgenden Fehlerquoten fest:



Mit anderen Worten: Nur ein Drittel der Anwender, die eine simulierte Phishing-E-Mail geöffnet haben, hat richtig gehandelt. Im Hinblick auf reale Angriffe sind das wirklich ernüchternde Zahlen.

Es muss allerdings auch dazu gesagt werden, dass bei dieser Methode zur Fehlerquotenberechnung die Anwender unberücksichtigt bleiben, die E-Mails *absichtlich* nicht öffnen, weil sie deren Gefährlichkeit erkennen. Die Trennung absichtlicher und unbeabsichtigter Aktionen ist jedoch sehr schwierig. (Es sei denn, der Anwender meldet die E-Mail – mehr dazu später.)

Einige Anwender ignorieren möglicherweise E-Mails, weil sie diese für gefährlich halten. Allerdings bleiben E-Mails häufig nicht nur wegen möglicher Cybersicherheitsprobleme ungeöffnet, sondern auch aus einer Vielzahl anderer Gründe: Die Anwender sind nicht im Büro und ignorieren Nachrichten in ihrem immer voller werdenden Posteingang oder sie sind mit anderen Aufgaben beschäftigt. Andererseits können Nachrichten auch automatisch in einen Unterordner abgelegt und vom Endnutzer damit nie gesehen werden. Oder die E-Mail wird ignoriert, weil der Betreff bzw. Inhalt den Anwender einfach nicht interessiert oder betrifft.

Alle Endnutzer, die es innerhalb eines Tages (oder selbst eines Monats) schaffen, alle E-Mails zu lesen, haben sich eine herzliche (und neidvolle) Gratulation verdient. Die meisten Arbeitnehmer haben jedoch unzählige ungelesene Nachrichten in ihren Postfächern. Ungeöffnete Phishing-Nachrichten sind also nicht immer ein Zeichen für besonders aufmerksame Anwender.

Der richtige Blick auf Fehlerquoten

Fehlerquoten stellen zwar interessante und wichtige Referenzpunkte dar, sind aber nicht das ultimative Maß zur Bewertung einer erfolgreichen Schulung.

Um den Erfolg Ihrer Schulungen zur Steigerung des Sicherheitsbewusstseins zu ermitteln, sollten Sie sich nicht zu stark auf Fehlerquoten stützen, da diese schwanken können – und sollen. Auch wenn Anwender die Phishing-Köder im Laufe der Zeit besser erkennen sollten, müssen sie immer wieder mit unterschiedlichen und schwer zu erkennenden Tests und Ködern herausgefordert werden. Das kann gelegentlich zu Spitzen bei der Fehlerquote führen, ist jedoch kein Zeichen dafür, dass Ihre Anwender ein hoffnungsloser Fall sind.

Erfassen Sie die Fehlerquoten, aber interpretieren Sie nicht zu viel hinein. Betrachten Sie die Öffnungsraten und vergleichen Sie sie mit den Fehlerquoten. Wenn Sie beispielsweise eine geringe Fehlerquote bei einer Kampagne verzeichnen, die tatsächlich aber nur von wenigen Anwendern überhaupt geöffnet wurde, ist diese geringe Rate eher die Ausnahme als die Norm.

Die beste Methode zur Ermittlung des Erfolgs ist ein umfassender Blick auf verhaltensbezogene Kennzahlen. Parallel zu den Fehlerquoten empfehlen wir die Erfassung von Veränderungen in folgenden Bereichen:

- Anzahl erfolgreicher realer Phishing-Angriffe
- Rate der Malware-Infektionen
- Menge und Art der Anrufe beim IT-Helpdesk
- Ausfallzeiten bei Endnutzern, die auf Phishing-Angriffe hereinfallen
- Behebungsaufwand in Stunden für IT-Mitarbeiter, die Phishing-Angriffe beheben müssen
- Anzahl der Computer, für die nach Angriffen ein Re-Imaging durchgeführt werden muss
- Menge und Art der von Anwendern gemeldeten E-Mails (mehr dazu in Abschnitt 5)

Letztendlich besteht Ihr Ziel nicht darin, die Anwender aufzufordern, erhaltene E-Mails blindlings zu melden oder zu ignorieren, da beides die Geschäftsabläufe beeinträchtigen kann. Stattdessen sollten Sie nach einer durchdachten Behandlung eingehender E-Mails streben. Durch praxisnahe Schulungen werden Ihre Anwender zu einer stärkeren letzten Verteidigungslinie.

Im vergangenen Jahr legten wir den Lesern des *State of the Phish*-Berichts nahe, mehr Dateneingabe-Kampagnen durchzuführen, um dem wachsenden Trend der Anmeldedaten-Kompromittierungsangriffe etwas entgegenzusetzen. Diese Empfehlung traf auf offene Ohren, sodass die Nutzung der Dateneingabe-Vorlagen im Jahresvergleich um fast 30 % stieg.

ABSCHNITT 4

Aufgeschlüsselt: Sensibilisierung von Mitarbeitern für Phishing-Angriffe in der Praxis Aus

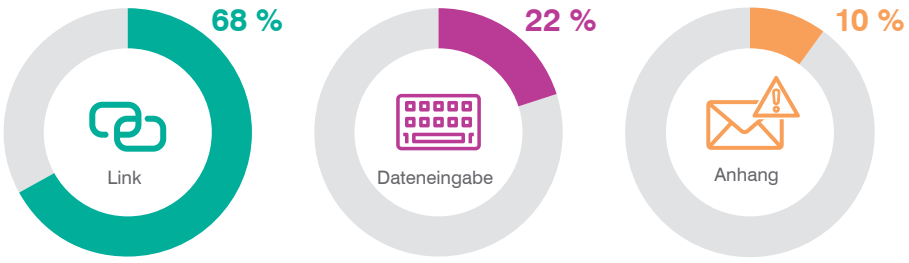
Wir untersuchten, wie unsere Kunden die Tools für simulierte Angriffe nutzen, um die Endnutzer für Phishing zu sensibilisieren und über bewährte Methoden zur Identifizierung und Vermeidung dieser Bedrohung zu schulen. Dieser Abschnitt bietet wichtige Einblicke und Empfehlungen.

Link-basierte Tests deutlich beliebter

Unsere Kunden können die Anfälligkeit ihrer Anwender in Bezug auf drei Phishing-Ködertypen testen und messen: Links, Anhänge und Dateneingabe-Aufforderungen (d. h. die Köder können vertrauliche Informationen wie Anmeldedaten abfragen).

Ebenso wie im Jahr 2018 setzten die Unternehmen auch 2019 verstärkt auf Link-basierte Tests.

Arten der Phishing-Vorlagen: Häufigkeit der Nutzung



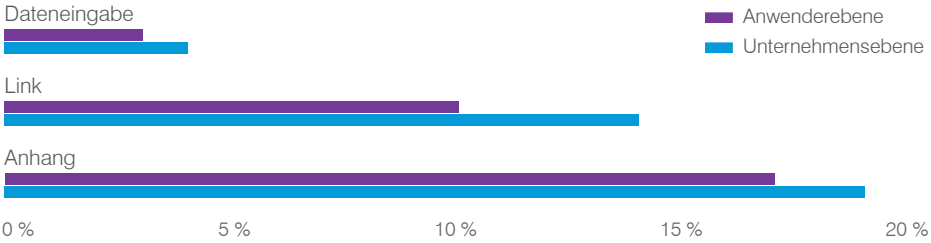
Der Fokus auf Link-basierte Tests hat einen guten Grund. Wie unsere Forscher feststellten, wurde im Jahr 2019 der Großteil der Schaddaten über URLs verbreitet.

Dennoch sollten Sie nicht nur die Häufigkeit von Angriffsmethoden, sondern auch die Anfälligkeit Ihrer Anwender für bestimmte Köder berücksichtigen. Links in E-Mails führen häufig zu kritischen sekundären Entscheidungspunkten, beispielsweise zu einer Webseite, die Anmeldedaten von Anwender abfragt oder sie zum Herunterladen einer Datei auffordert. Daher sind Tests der Reaktionen Ihrer Anwender in solchen Situationen unverzichtbar, insbesondere dann, wenn Ihr Unternehmen realen Angriffen ausgesetzt ist, die auf diese Techniken setzen.

Wir berechneten die Fehlerquoten für jeden Vorlagentyp. Obwohl im Jahr 2019 die Anhang-Tests in den Prioritäten von Unternehmen weit hinten lagen, erwiesen sie sich beim Ködern der Anwender als besonders wirksam.

Anwender, die den Dateneingabe-Test nicht „bestanden“, haben nach dem Klick auf einen Link im simulierten Angriff Daten eingegeben.

Durchschnittliche Fehlerquote nach Art der Vorlage



Im Anhang finden Sie weitere Angaben mit den branchenspezifischen Fehlerquoten für Link-, Dateneingabe- und Anhang-Vorlagen.

Personalisierung: Verbesserungspotenzial

Cyberkriminelle nutzen für ihre Angriffe einen raffinierteren und personenorientierten Ansatz. Das bedeutet, dass sich Phishing-E-Mails schwerer von legitimen Nachrichten unterscheiden lassen. Personalisierung spielt bei diesem Wandel eine wichtige Rolle. Die Angreifer erledigen ihre Hausaufgaben und ihre E-Mails erscheinen für die Empfänger häufig persönlich relevant.

Leider enthielt im Jahr 2019 weniger als die Hälfte der simulierten Phishing-Kampagnen unserer Kunden benutzerdefinierte Felder wie Vor- und Nachnamen sowie E-Mail-Adressen. (Interessant ist, dass das Einbeziehen des eigenen Unternehmensnamens in Phishing-Tests die Fehlerquoten fast immer erhöhte.)

Wir empfehlen unseren Kunden daher die regelmäßige Nutzung von Personalisierungstechniken in ihren Tests. Auf diese Weise werden die Anwender besser auf gezielte Angriffe vorbereitet und verstehen leichter, wie raffiniert solche Attacken sein können. Dieses Verständnis ist insbesondere bei neueren Phishing-Sensibilisierungsprogrammen wichtig. Bei Schulungen, die seit mindestens einem Jahr laufen, werden die Anwender weniger häufig von benutzerdefinierten Feldern hinters Licht geführt.

Häufige Trends bei den raffiniertesten Vorlagen

Leser der *State of the Phish*-Berichte interessieren sich häufig ganz besonders für ein Thema: die simulierten Phishing-Vorlagen, mit denen Anwender sich ganz besonders schwer tun.

In diesem Jahr untersuchten wir die Phishing-Tests mit den höchsten Fehlerquoten – fast 100 % – und einem Umfang von mindestens 1.500 individuellen E-Mails. Dabei entdeckten wir einige interessante Gemeinsamkeiten bei diesen Vorlagen:

- 65 % waren Tests mit Anhängen, 35 % waren Tests mit Links, es waren jedoch keine Dateneingabe-Vorlagen darunter.
- 65 % der Vorlagen basierten auf realen Angriffen, die von unseren Bedrohungsforschern aufgedeckt wurden.
- Fast 90 % der Tests stammten scheinbar von einer vertrauten internen E-Mail-Adresse (z. B. der Personalabteilung).

Zu den interessantesten Betreffzeilen in diesen „erfolgreichsten“ Programmen gehörten:

- Armbanduhr verloren
- Ring verloren
- SharePoint-Dokument
- Gescannt mit einem Xerox-Multifunktionsdrucker
- Vertragsangebot
- Aktualisierter Gebäudeevakuierungsplan (seit drei Jahren einer unserer Dauerbrenner)
- Vertrauliches Dokument
- <Vorname>, bitte fügen Sie mich zu Ihrem LinkedIn-Netzwerk hinzu

Die ersten beiden Einträge auf dieser Liste sind bemerkenswert, weil sie einfach gehalten sind und die Neugier sowie Hilfsbereitschaft der Leser ansprechen. Auch der letzte Punkt auf der Liste ist interessant. Diese Einladung stammt scheinbar vom CIO des Unternehmens – und wer schlägt schon den Kontaktwunsch eines VIPs aus? (Offensichtlich kaum jemand.)

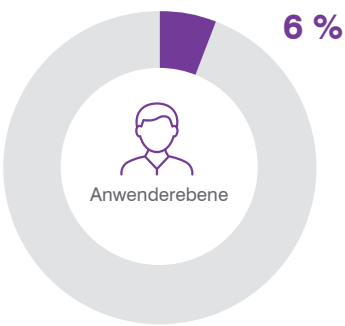
Die Gemeinsamkeiten sowie die Betreffzeilen in diesen Listen untermauern unsere Empfehlung, die Anfälligkeit für Anhänge häufig zu testen und simulierte Phishing-Kampagnen stärker zu personalisieren. Selbst wenn Sie Angriffe mit Anhängen seltener registrieren, werden sie zum Problem für Ihr Unternehmen, wenn fast alle Anwender darauf hereinfallen.

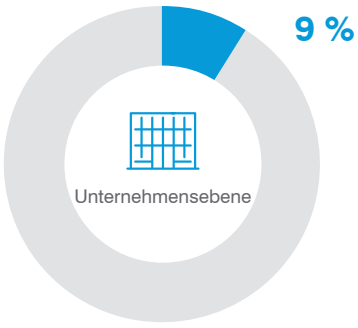
Ein Hinweis zu Smishing

Einige unserer Kunden testen nicht nur die Anfälligkeit ihrer Anwender für E-Mail-basiertes Phishing, sondern auch die für Smishing (also SMS-/Textnachrichten-Phishing), allerdings nicht besonders häufig. Der Grund liegt teilweise an der Zunahme der Bring Your Own Device (BYOD)-Kultur in Unternehmen. Viele Anwender nutzen ihre eigenen Mobilgeräte auch für berufliche Zwecke. Aus rechtlichen Gründen kann es schwierig sein, das Verhalten der Anwender auf ihren eigenen Smartphones zu testen.

Smishing ist jedoch eine Bedrohung, die alle angeht. Wie bereits erwähnt, erlebten die meisten Unternehmen 2019 solche Angriffe. Da Textnachrichten privater erscheinen können als E-Mails, sind Anwender unter Umständen stärker für Smishing anfällig, wenn sie nicht auf diese Bedrohung aufmerksam gemacht wurden.

Folgende durchschnittliche Fehlerquoten haben wir in den Smishing-Simulationen unserer Kunden 2019 registriert:





DIE FAKTEN

Die Anwender meldeten 2019 fast **9,2 Mio.** verdächtige E-Mails, was einer Steigerung im Vorjahresvergleich um 67 % entspricht.

Die durchschnittliche Zeit zwischen Erhalt und Meldung einer E-Mail liegt bei **einer Stunde**.

Im Durchschnitt meldete jeder PhishAlarm-Anwender im Jahr 2019 **fünf E-Mails**.

ABSCHNITT 5

Endnutzer-Berichte: Der Weg zum Nirvana

Seit langem empfehlen wir unseren Kunden, ihren Anwendern bequeme Möglichkeiten zum Melden verdächtiger E-Mails zu geben und diese Meldungen zu erfassen. Solche Kennzahlen sind eine hervorragende Möglichkeit, die Effektivität von Schulungsinitiativen zu ermitteln. Der Grund:

- Der Mehrwert Ihres Trainings wird gesteigert, da die Anwender eine Möglichkeit erhalten, ihr Wissen anzuwenden.
- Gemeldete E-Mails signalisieren Bedacht und Absicht – sind also Anzeichen dafür, dass die Anwender mit erhaltenen Nachrichten vorsichtiger umgehen. Dies ist ein zuverlässigeres Maß für Sensibilisierung und Sicherheitsverständnis als geringe Fehlerquoten bei simulierten Phishing-Angriffen, insbesondere in Anbetracht ungeöffneter E-Mails.
- Detaillierte Berichte können aktive Angriffe aufdecken, die den softwarebasierten Sicherheitslösungen Ihres Unternehmens entgangen sind.

Allgemeine Betrachtungen zu Meldungsdaten

Wir verzeichneten eine weiterhin steigende Nutzung unseres PhishAlarm®-Tools zur E-Mail-Meldung. Dabei handelt es sich um eine Schaltfläche im E-Mail-Client, mit der Nachrichten mit vollständigem Header an festgelegte Postfächer weitergeleitet werden. Im Jahr 2019 leiteten Endnutzer fast 9,2 Millionen verdächtige E-Mails weiter, was im Vergleich zu 2018 einem Anstieg um 67 % entspricht.

Mehr als die Hälfte dieser gemeldeten Nachrichten wurden als potenzielle Phishing-Nachrichten gekennzeichnet und von PhishAlarm Analyzer, unserem Tool zur Echtzeit-Priorisierung von Bedrohungen, untersucht. Diese automatisierte Analyse deckt E-Mails auf, bei denen es sich wahrscheinlich um Phishing-Versuche handelt, sodass diese schnell von IT-Sicherheitsteams abgewehrt werden können.

Bei der Bewertung von Daten zu gemeldeten simulierten Angriffen entdeckten wir einige Trends. Im Allgemeinen taten sich Anwender mit dem Melden von Phishing-Tests mit behördlichen und technischen Themen leichter. Am seltensten werden simulierte Angriffe gemeldet, die mithilfe von Nachrichten in sozialen Netzwerken und Bildern erfolgten.

Die Meldungsrate in einem Unternehmen sollte im Laufe der Zeit steigen, da die Anwender bei der Erkennung von Anzeichen für verdächtige Nachrichten sicherer werden. Gleichzeitig müssen Unternehmen berücksichtigen, dass das Melden selbst erst von den Anwendern erlernt werden muss. Machen Sie nicht den Fehler zu glauben, dass es mit der Installation einer Schaltfläche getan ist. Sie müssen Ihre Mitarbeiter auch darin schulen, wann (und wie) sie zu nutzen ist.

Die Suche nach dem Nirvana

In den letzten Jahren wurden wir mehrfach von Unternehmen danach gefragt, wie viele E-Mails die Endnutzer idealerweise melden sollten.

Eine Antwort ist schwierig, vor allem weil die Bedingungen sich ständig ändern. Die Anzahl der E-Mails, die gemeldet werden „sollten", hängt zunächst von der Anzahl der simulierten Phishing-Tests ab, die das Unternehmen versendet. Außerdem ist sie abhängig von der Anzahl der Phishing-Angriffe, die die vorhandenen technischen Schutzmaßnahmen überwinden können. Die erste Zahl können Sie leicht identifizieren, doch die zweite lässt sich nur schwer (oder gar nicht) mit Sicherheit quantifizieren.

Jeder PhishAlarm-Anwender meldete 2019 im Durchschnitt fünf E-Mails. Wir raten jedoch davon ab, eine bestimmte Anzahl an Meldungen für Endnutzer als Ziel festzulegen. Wenn Sie Ihren Mitarbeitern erklären, dass sie „X" E-Mails melden sollen, werden sie sich auf Quantität statt auf Qualität konzentrieren. Allerdings ist die Qualität der Meldungen viel wichtiger (siehe die Fallstudie am Ende dieses Abschnitts für eine Analyse aller im 3. Quartal 2019 gemeldeten E-Mails).

Im Idealfall werden Anwender alle simulierten Phishing-Tests melden, doch eine Meldungsrate von 100 % ist ebenso unrealistisch wie eine Fehlerquote von 0 %.

Statt unerfüllbare Ziele zu verfolgen, sollten Sie sich an der folgenden Formel orientieren:

Hohe Meldungsrate + niedrige Fehlerquote = Nirvana

Die 70/5-Regel: Ihr Weg zum Nirvana

Sie kennen vielleicht die 80/20-Regel (auch bekannt als das Pareto-Prinzip). Wir möchten die 70/5-Regel für simulierte Phishing-Angriffe vorstellen: Das bedeutet, dass die Meldungsrate mehr als 70 % und die Fehlerquote weniger als 5 % betragen sollte.

Tabelle 1 zeigt die Top 5 der Kundenkampagnen, die 2019 die 70/5-Regel bei mindestens 350 gesendeten Tests erreichten.

Hohe Meldungsraten, niedrige Fehlerquoten

Betreffzeile	Vorlagenstil	Anzahl gesendeter Nachrichten	Fehlerquote	Meldungsrate
Jemand kennt Ihr Kennwort	Dateneingabe	798	<1 %	86 %
Bitte dieses Dokument per DocSign unterschreiben: Vertragsänderung	Anhang	441	2 %	85 %
VERTRAULICHE UNTERNEHMENS-INFORMATION: Wichtige Ankündigung	Link	442	2 %	83 %
Benachrichtigung über Geschwindigkeitsverstoß[4]	Link	676	4 %	81 %
Netzwerkzugriffsversuch	Dateneingabe	360	1 %	80 %

Tabelle 1

[4] Diese Vorlage hatte im Jahr 2018 eine der höchsten durchschnittlichen Fehlerquoten. Wir freuen uns, dass sich diese Zahlen zum Positiven geändert haben.

Eine kleinere simulierte Phishing-Kampagne (mit weniger als 100 Nachrichten) zeigte einen interessanten Statistikwert: eine Fehlerquote von 7 % mit einer Meldungsrate von 100 %. Obwohl die 70/5-Regel nicht ganz erreicht wird, zeigt sich hier ein interessanter Fakt: die Bereitschaft der Anwender in einem Unternehmen, eine Nachricht zu melden, nachdem sie einen Fehler gemacht haben.

Das allein ist schon ein Stück Nirvana. Ihre Anwender sollten sich sicher genug fühlen, um E-Mails zu melden, selbst wenn sie befürchten, dass sie mit einer schädlichen Nachricht interagiert haben – oder vielleicht *gerade dann*. Die Ehrlichkeit eines Endnutzers ist vielleicht die schnellste Möglichkeit, einen erfolgreichen Phishing-Angriff abzuwehren.

Wenn Sie in einem größeren Unternehmen arbeiten, denken Sie vielleicht: „Das ist ja alles gut und schön, aber was ist mit umfangreicheren Kampagnen?“ Wir sind der Meinung, dass die 70/5-Regel dennoch das Ziel sein sollte. Es ist insbesondere für größere Unternehmen ein Fernziel. Aber wie Tabelle 2 zeigt, ist es durchaus erreichbar.

Wir wissen, dass der Ausreißer in dieser Tabelle („Neue Rechnung“) abschreckend wirken kann. Möglicherweise glauben Sie, dass bei einem realen Angriff eine Fehlerquote von 13 % zu hoch wäre.

Unser Gegenargument: Wenn mehr als 60 % der Empfänger einen aktiven Angriff melden, sind Sie in einer guten Position, den 13 % zuvorzukommen, die auf den Phishing-Versuch hereingefallen wären. Das ist insbesondere dann der Fall, wenn Sie die Maßnahmen zur Behebung bei erfolgten Angriffen automatisieren. (Weitere Empfehlungen finden Sie in der Seitenleiste „Lassen Sie sich von gemeldeten E-Mails nicht stressen“.)

Höchste Meldungsraten umfangreicher Kampagnen

Betreffzeile	Vorlagenstil	Anzahl gesendeter Nachrichten	Fehlerquote	Meldungsrate
Anfrage von <Unternehmensname>	Anhang	5.689	6 %	65 %
Neue Rechnung	Anhang	5.704	13 %	65 %
Bitte dringend beachten	Link	6.230	5 %	61 %
Kompromittiertes Kennwort	Dateneingabe	5.444	<1 %	53 %

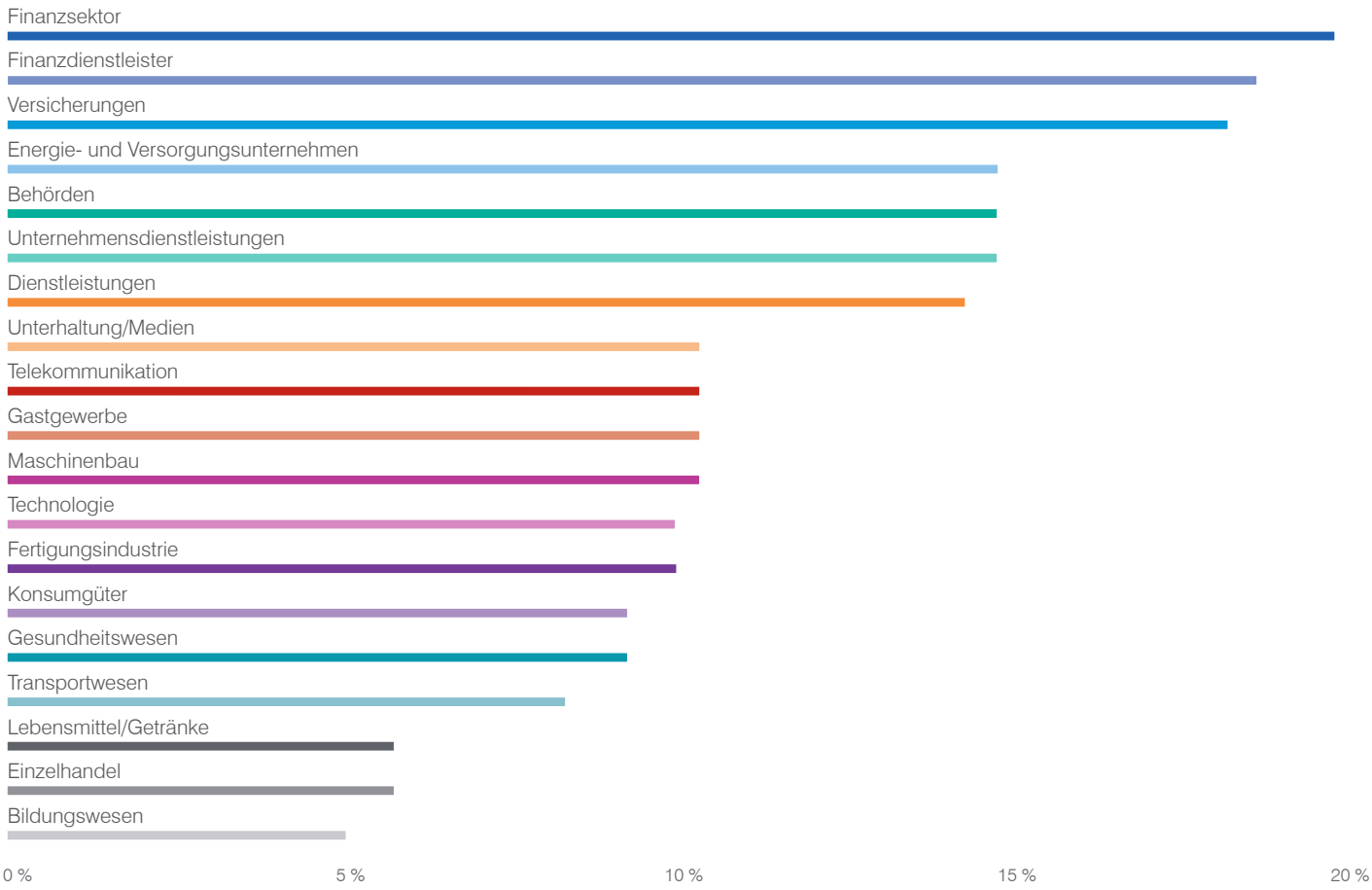
Tabelle 2

Meldungsraten nach Branche

Unsere Analyse der branchenspezifischen Meldungsraten zeigt die Bedeutung von Meldungen als Kennzahl für den Gesamterfolg eines Trainingsprogramms.

Die Finanz- und Bildungssektoren verzeichneten im Jahr 2019 auf Anwenderebene jeweils eine Fehlerquote von 8 % – und dennoch liegen sie am jeweils anderen Ende des Meldungsspektrums. Anwender in der Finanzbranche meldeten Phishing-E-Mails deutlich häufiger als die im Bildungssektor. In realen Angriffen hätten IT-Sicherheitsteams von Finanzunternehmen erheblich größere Chancen, Angriffe abzufangen, die Peripherieschutzmaßnahmen unterlaufen.

Durchschnittliche Rate gemeldeter Phishing-Nachrichten nach Branche



Lassen Sie sich von gemeldeten E-Mails nicht stressen

In Ihrem Unternehmen ist es unverzichtbar, Anwender anzusprechen und sie anzuhalten, verdächtige E-Mails zu melden. Ebenso wichtig ist eine Methode für die Anwender, diese Nachrichten schnell und einfach an die richtigen Mitarbeiter weiterzuleiten. (Wir empfehlen dringend die Verwendung einer Meldungsschaltfläche im Client, z. B. PhishAlarm.)

Doch was geschieht, wenn diese gemeldeten E-Mails bei Ihrem IT-Sicherheitsteam eintreffen? Könnten Sie Opfer Ihres eigenen Erfolges werden? Wenn Sie nicht über die notwendige Bandbreite für zusätzliche Analysen und Behebungsmaßnahmen verfügen, ist die Zeit der Automatisierung gekommen.

Die beste Möglichkeit dazu ist die Proofpoint-Lösung CLEAR – Closed-Loop Email Analysis and Response, die E-Mail-Meldungen und -Behebungen integriert und so den Zeitraum bis zur Neutralisierung einer aktiven Bedrohung von Tagen auf Minuten verkürzt. Mit CLEAR werden gemeldete E-Mails automatisch von mehreren Bedrohungsdaten- und Reputationssystemen analysiert und alle Links sowie Anhänge in einer Sandbox überprüft. Als schädlich identifizierte Nachrichten können mit einem einzigen Klick gelöscht oder isoliert werden. Zudem kann der Anwender, der die E-Mail gemeldet hat, automatisch benachrichtigt (und für die Wachsamkeit gelobt) werden.

ANWENDUNGSBEISPIEL

Anmeldedaten-Phishing wurde im 3. Quartal 2019 am häufigsten gemeldet.

Im 3. Quartal 2019 analysierten wir mehr als 600.000 gemeldete E-Mails – ca. 8.500 Nachrichten pro Arbeitstag. (Die Anwendermeldungen gehen an Wochenenden und Feiertagen erheblich zurück.) Die Daten zeigen die Bedeutung eines personenorientierten Cybersicherheitsansatzes sowie der Einbeziehung von Anwendern in die Phishing-Abwehr.

Anwender helfen bei der Aufdeckung schwerwiegender Sicherheitsbedrohungen

Aufgrund des Anstiegs von Anmeldedaten-Phishing-Angriffen werden diese schädlichen E-Mail-Typen am häufigsten von Anwendern gemeldet. Die Anwender erkennen und melden jedoch auch Malware-basierte Angriffe – von denen einige extrem gefährliche Schaddaten enthalten.

Im 3. Quartal 2019 enthielten fast 20.000 von Endnutzern gemeldete E-Mails Anmeldedaten-Phishing-Köder und weitere über 4.000 gemeldete Nachrichten Malware-Schaddaten wie Keylogger und APT-Malware (Advanced Persistent Threat).

Es geht jedoch nicht nur um Quantität – entscheidend ist die Qualität. Unsere Systeme klassifizieren Bedrohungen nicht nur nach Kategorie, sondern auch nach Schweregrad. Dank der Aufmerksamkeit der Endnutzer konnten IT-Sicherheitsteams einige schwerwiegende Bedrohungen identifizieren, darunter Phishing-Versuche wie die folgenden Malware-Schaddaten:

BACKDOOR-TROJANER	DOWNLOADER
INFORMATIONSDIEBE	REMOTE-ZUGRIFFS-TROJANER (RATS)

Alle sehen mehr

Da Angestellte auf allen Unternehmensebenen angegriffen werden können, sollten alle Anwender die Möglichkeit zur Meldung verdächtiger E-Mails haben.

Die Erfahrungen unserer Kunden bestätigen das. In einem aktuellen Beispiel entdeckten und meldeten zwei regionale CFOs bei einem Fortune 50-Unternehmen mehrere schwerwiegende Anmeldedaten-Phishing-Versuche.

Bei einer führenden Versicherungsagentur waren es hingegen zwei Schadensregulierer und ein Jurist, die ihr IT-Sicherheitsteam über gefährliche Anmeldedaten-basierte Angriffe informierten.

Diese Beispiele zeigen, dass nicht nur hochrangige Führungskräfte Zugang zu wichtigen Schulungstools erhalten sollten. Vielmehr sollten alle Angestellten über eine Möglichkeit verfügen, das eigene Cybersicherheitsverhalten zu verbessern und neues Wissen anzuwenden.

ABSCHNITT 6

Der Schlüssel zum Wissen: Vorteile detaillierter Daten

Mittlerweile haben Sie wahrscheinlich ein durchgehendes Thema unseres Berichts erkannt: den Bedarf nach einem besseren Einblick in das Cybersicherheitsverhalten Ihrer Anwender. Ihre Daten helfen bei der Erkennung schwerwiegender Schwachstellen in Ihrem Unternehmen und bei der besseren Koordinierung Ihrer Phishing-Schutzmaßnahmen.

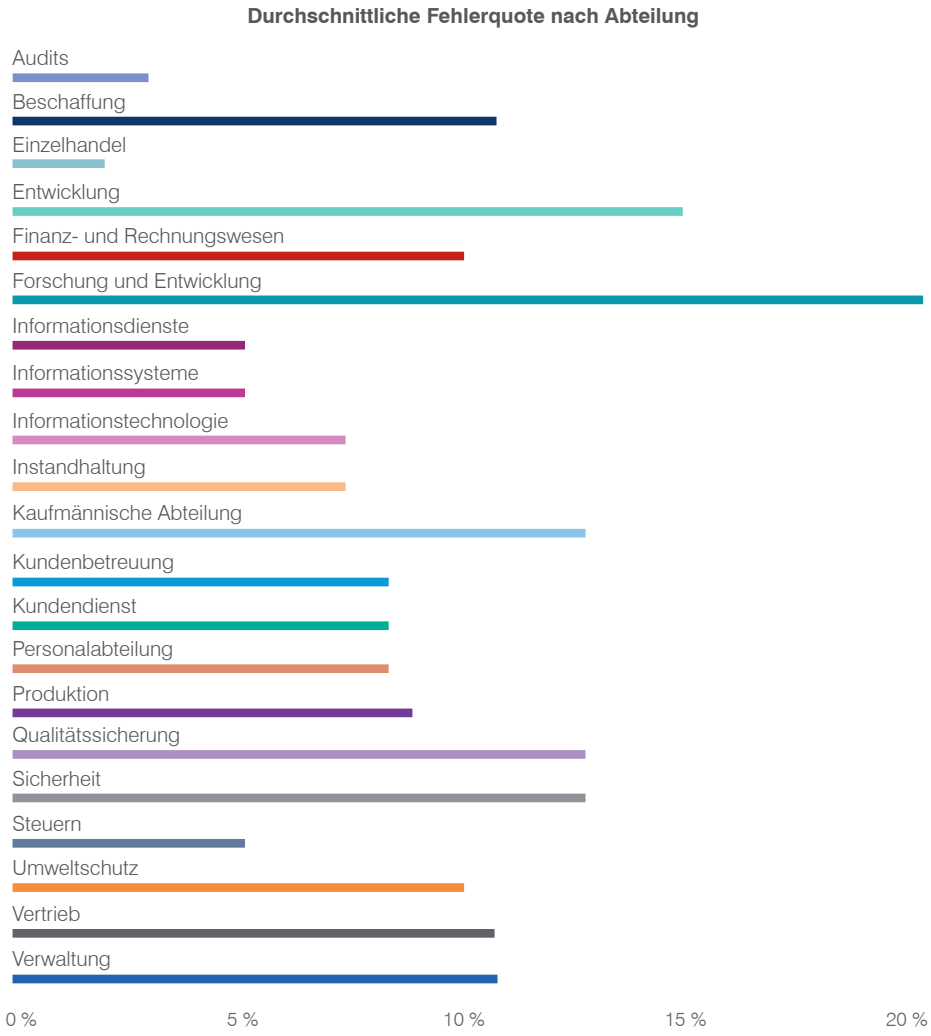
Fehlerquoten auf Abteilungsebene

Viele Unternehmen lassen eine wichtige Gelegenheit ungenutzt: die Möglichkeit, Fehlerquoten auf Abteilungsebene anzuzeigen. Da Unternehmen ihre Anwender zu Berichtszwecken nur selten nach Abteilungen gruppieren, fehlt ihnen die Möglichkeit, das Abschneiden (und die Anfälligkeit) nach Tätigkeitsbereich aufzuschlüsseln.

Das ist jedoch ein wichtiger Bestandteil des Puzzles. Angreifer nehmen häufig bestimmte Mitarbeiter – und E-Mail-Aliase – basierend auf den Rollen und Verantwortungsbereichen innerhalb eines Unternehmens ins Visier (siehe den Abschnitt „Genauere Betrachtung“).

Das folgende Diagramm zeigt die am häufigsten genutzten Abteilungsbezeichnungen unter den Kunden, die ihre Daten so detailliert klassifizieren.[5] Diese Bezeichnungen wurden von mindestens zehn Unternehmen angegeben und umfassten mindestens 1.000 Anwender.

[5] Die Bezeichnungen der Abteilungen bedeuten nicht in jedem Unternehmen das Gleiche. Sie verwenden vielleicht einige gemeinsame Begriffe, doch die jeweiligen Tätigkeitsbereiche unterscheiden sich häufig. Beispielsweise kann sich „Sicherheit“ in einigen Unternehmen auf physische Sicherheit und in anderen auf Informationssicherheit beziehen.



Unternehmen, die diese Daten nicht erfassen, haben einen Nachteil – sie können Warnzeichen (sowie angenehme Überraschungen) verpassen. Nehmen Sie beispielsweise die Durchschnittswerte aus dem Diagramm:

- Hohe Fehlerquoten in den Abteilungen für Forschung, Entwicklung und Technik sind besorgniserregend. Diese Personen haben wahrscheinlich Zugriff auf wichtiges geistiges Eigentum und Zukunftstechnologien.
- Geringe Fehlerquoten bei Informationsdiensten, Systemen und Technologien sind hingegen positive Anzeichen. Aufgrund ihrer Zugriffsrechte sind Angestellte in diesen Tätigkeitsbereichen wahrscheinliche Angriffsziele, sodass unbedingte Wachsamkeit notwendig ist (wie im Abschnitt „Der Schlüssel zum Wissen“ genauer erklärt).
- Eine durchschnittliche Fehlerquote von 11 % für den Vertrieb ist nicht extrem hoch. Allerdings erhalten die Angestellten in diesem Tätigkeitsbereich wahrscheinlich sehr viele E-Mails, sodass selbst eine nur mäßig hohe Fehlerquote auf ein Problem bei Gruppen mit einem allgemein hohen Nachrichtenaufkommen hindeuten kann.
- Ebenso ist die durchschnittliche Fehlerquote von 10 % für Angestellte im Finanz- und Rechnungswesen nicht weit vom Durchschnittswert von 9 % für alle Anwender entfernt. Die Angestellten in diesen Tätigkeitsbereichen haben jedoch direkten Zugriff auf Bankkonten sowie wichtige Finanzdaten und sollten daher zu den aufmerksamsten und am besten vorbereiteten Mitarbeitern in Ihrem Unternehmen zählen (ebenso wie beispielsweise Mitarbeiter in Audit- und Steuer-bezogenen Funktionen).

Genauere Betrachtung: Ihre Very Attacked People (VAPs)

Wir bezeichnen die am häufigsten mit Cyberangriffen attackierten Anwender (und E-Mail-Postfächer) in einem Unternehmen als Very Attacked People™ (VAPs, besonders häufig angegriffene Personen). Dank unserer Bedrohungsdaten können wir Ihre VAPs sowie die bei Kompromittierungsversuchen der Angreifer eingesetzten Methoden identifizieren. Immer wieder haben wir dabei festgestellt, dass Ihre VAPs nicht immer auch Ihre VIPs sind.

Die VAPs können sich nicht nur je nach Branche und Unternehmen unterscheiden, sondern ändern sich auch im Zeitverlauf teils erheblich. Unternehmen erleben regelmäßig Fluktuationen bei ihren VAPs. Die Art der angegriffenen Rollen schwankt von Monat zu Monat und von Jahr zu Jahr und zeigt, wie bereitwillig sich die Angreifer innerhalb der Unternehmenshierarchien auf- und abwärts orientieren, um Einfallstore zu den für sie interessanten Daten und Systemen zu finden.

Es ist wichtig, die VAPs Ihres Unternehmens kennenzulernen. Der Grund:

- So können Sie schnell die gezielt angegriffenen Mitarbeiter sowie die Kompromittierungsmethoden der Angreifer identifizieren. Das gibt Ihnen die Möglichkeit, den richtigen Personen zum richtigen Zeitpunkt die richtigen Schulungen bereitzustellen.
- Sie können Bedrohungen mit größerer Wahrscheinlichkeit beheben. Sie müssen keine Vermutungen mehr über wertvolle Ziele anstellen, sondern können verwertbare Daten nutzen.
- Sie können potenzielle Angriffstrends identifizieren. Beispielsweise können Gemeinsamkeiten bei Angriffsmethoden und angegriffenen Tätigkeitsbereichen darauf hinweisen, dass die Angreifer ein bestimmtes Ziel im Sinn haben. Ein solcher Überblick ist Gold wert.
- Sie können fundiertere Entscheidungen zu Ihrem allgemeinen Schulungsansatz treffen. Vielleicht haben Sie Schwierigkeiten, die nötigen Ressourcen für ein umfassendes Schulungsprogramm zu erhalten, weil die Entscheidungsträger davon ausgehen, dass nur ein Teil der Angestellten geschult werden muss. VAP-Berichte können wichtige Einblicke liefern und Ihnen helfen, das Interesse der Angreifer für bestimmte Rollen und Tätigkeitsbereiche zu verdeutlichen.

ABSCHNITT 7

Fazit: Nutzen Sie Ihre Daten

Ihr Programm zur Steigerung des Sicherheitsbewusstseins sollte das Ziel haben, die Verhaltensweisen zu verbessern, die für Ihr Unternehmen die größte Bedeutung haben. Die beste Möglichkeit dazu ist eine Mischung aus allgemeinen und gezielten Schulungen, die Mitarbeiter mit direkten umsetzbaren Empfehlungen unterstützen.

Die Daten in diesem Bericht zeigen das deutlich. Angreifer konzentrieren sich auf menschliche Ziele – *Ihre* Mitarbeiter. Wenn Sie das ignorieren, wird der Schaden nicht lange auf sich warten lassen. Sofern Sie bislang noch keinen personenorientierten Ansatz für Sicherheitsschulungen umgesetzt haben, sollten Sie das umgehend tun. Gehen Sie wie folgt vor:

1. Aufbau einer sicherheitsorientierten Unternehmenskultur

Die Erlebnisse in unterschiedlichen Unternehmen und Branchen gleichen sich in vielerlei Hinsicht stark. Auch wenn sich unsere Ziele, Kunden und Daten unterscheiden, stehen wir letztendlich vor der gleichen Aufgabe: der Stärkung unseres Schutzes. Wenn Sie wirklich einen Wandel bewirken möchten, der die Einstellungen und Verhaltensweisen im Unternehmensalltag zum Positiven verändert, müssen Sie sich dafür einsetzen, dass Cybersicherheit eine zentrale Rolle einnimmt – und das sollte für jeden Mitarbeiter in Ihrem Unternehmen gelten.

Der Grund:

- Jeder Mitarbeiter in Ihrem Unternehmen kann ins Visier der Angreifer geraten.
- Zu jedem Zeitpunkt kann jeder Angestellte in Ihrem Unternehmen die Sicherheitslage verbessern oder beeinträchtigen.

Der Aufbau einer Sicherheitskultur ist unverzichtbar. Alle Mitarbeiter in Ihrem Unternehmen sollten wissen, wie sie die Cybersicherheit verbessern können. Ein umfassendes und unternehmensweites Programm zur Steigerung des Sicherheitsbewusstseins hilft Ihnen dabei.

2. Antwort auf die drei W-Fragen

Neben den gemeinsamen Erlebnissen sehen wir auch viele Unterschiede zwischen Branchen, Abteilungen und Anwendergruppen. Wenn Sie verstehen, was diese Unterschiede für Ihr Unternehmen bedeuten, können Sie die spezifischen Methoden der Angreifer zur Kompromittierung Ihrer Mitarbeiter besser abwehren.

Vielleicht Sie sind mit den sechs W-Fragen vertraut, denen Journalisten, Forscher und Ermittler folgen: Wer, Was, Wo, Wann, Warum und Wie. Dies alles sind wichtige Fragen, mit denen Sie sich der Ursache eines Problems nähern können. Wir empfehlen, mindestens die ersten drei Fragen zu beantworten:

- **Wer in meinem Unternehmen wird von Angreifern attackiert?** Die Antwort ist nicht so einfach wie ein Blick auf die obersten Unternehmensebenen.
- **Welchen Arten von Angriffen sind sie ausgesetzt?** Wenn Sie die Köder und Fallen der Angreifer kennen, können Sie Ihre Abwehrmaßnahmen besser aufstellen.
- **Wie kann ich das Risiko minimieren, wenn diese Angriffe doch durchkommen?** Die Antwort: Nutzen Sie die erfassten Informationen, um den richtigen Personen zum richtigen Zeitpunkt die richtigen Schulungen bereitzustellen.

Mit dieser Faustregel können Sie die gefährlichsten und neuesten Bedrohungen abwehren. Wenn Sie die Schwachstellen detaillierter untersuchen und mit Ihren Bedrohungsdaten abgleichen, können Sie die genaue Schnittstelle zwischen der menschlichen und technischen Anfälligkeit bestimmen und so lokalisieren, wo das Unheil droht.

3. Flexibilität ist unverzichtbar

Zeit ist ein knappes Gut. Wer unter Zeitdruck steht, neigt dazu, bei seiner Cybersicherheit einem „Einstellen und Vergessen"-Ansatz zu folgen. Das ist zwar nachvollziehbar, in einer Zeit ständig wechselnder Angriffstechniken und immer neuer Bedrohungen jedoch keine praktikable Vorgehensweise.

Unsere ersten beiden Empfehlungen sind keine einmaligen Aktionen.

Der Aufbau einer Sicherheitskultur erfordert ständige Bemühung und Aufmerksamkeit. Planen Sie regelmäßige Schulungen sowie Maßnahmen zur Festigung ein, aber reagieren Sie gleichzeitig flexibel auf Veränderungen in der Bedrohungslandschaft (und in Ihrem Unternehmen).

Die Ziele der Angreifer ändern sich im Laufe der Zeit. Wir empfehlen daher, mindestens monatlich und besser noch wöchentlich Ihre am häufigsten angegriffenen Personen – die VAPs – zu identifizieren. Wenn Sie detaillierte Analysen mit unternehmensweiten Schulungen verbinden, verfügt ein neuer VAP über die notwendigen Cybersicherheitsgrundlagen, auf denen Sie mit weiteren gezielten Schulungen aufbauen können.

Das Wissen um allgemeine Phishing-Trends ist sehr wichtig, ebenso wie Benchmarks, mit denen Sie Ihre Anwender bewerten können. Doch die Daten eines anderen Unternehmens sind für Sie weniger aussagekräftig als Daten Ihres eigenen Unternehmens. Sie müssen Ihre eigene Bedrohungssituation kennen, um sie verbessern zu können.

ANHANG

A. Umfrage unter berufstätigen Erwachsenen: Aufschlüsselung nach Ländern

	USA	AUSTRALIEN	FRANKREICH	DEUTSCHLAND	JAPAN	SPANIEN	GROSS-BRITANNIEN	WELTWEITER DURCHSCHNITT
Was ist Phishing?								
Richtige Antwort	49 %	61 %	64 %	66 %	60 %	65 %	63 %	61 %
Falsche Antwort	38 %	19 %	21 %	15 %	29 %	26 %	22 %	24 %
Weiß nicht	13 %	20 %	15 %	19 %	11 %	9 %	15 %	15 %
Was ist Ransomware?								
Richtige Antwort	29 %	42 %	26 %	23 %	39 %	22 %	38 %	31 %
Falsche Antwort	48 %	26 %	36 %	22 %	22 %	32 %	32 %	31 %
Weiß nicht	23 %	32 %	38 %	55 %	39 %	46 %	30 %	38 %
Was ist Malware?								
Richtige Antwort	52 %	70 %	68 %	65 %	61 %	79 %	67 %	66 %
Falsche Antwort	37 %	12 %	17 %	13 %	8 %	11 %	20 %	17 %
Weiß nicht	11 %	18 %	15 %	22 %	31 %	10 %	13 %	17 %
Was ist Smishing?								
Richtige Antwort	36 %	20 %	54 %	28 %	17 %	35 %	22 %	30 %
Falsche Antwort	26 %	21 %	19 %	14 %	24 %	15 %	24 %	21 %
Weiß nicht	38 %	59 %	27 %	58 %	59 %	50 %	54 %	49 %
Was ist Vishing?								
Richtige Antwort	19 %	22 %	48 %	17 %	20 %	25 %	24 %	25 %
Falsche Antwort	38 %	17 %	17 %	26 %	17 %	20 %	18 %	22 %
Weiß nicht	43 %	61 %	35 %	57 %	63 %	55 %	58 %	53 %

	USA	AUSTRALIEN	FRANKREICH	DEUTSCHLAND	JAPAN	SPANIEN	GROSS-BRITANNIEN	WELTWEITER DURCHSCHNITT
Nutzen Sie Ihr Smartphone gleichzeitig für berufliche sowie private Aktivitäten?								
Ja	46 %	50 %	37 %	23 %	43 %	55 %	31 %	41 %
Nein	54 %	50 %	63 %	77 %	57 %	45 %	69 %	59 %
Wie sperren Sie Ihr Smartphone?								
Biometrische Sperre	49 %	38 %	34 %	38 %	52 %	45 %	40 %	42 %
Komplexes Wischmuster	11 %	9 %	13 %	12 %	9 %	22 %	8 %	12 %
Alphanumerisches Kennwort	5 %	6 %	7 %	6 %	12 %	7 %	4 %	7 %
4-stellige PIN	21 %	26 %	33 %	31 %	10 %	19 %	26 %	24 %
6-stellige PIN	5 %	9 %	6 %	5 %	5 %	2 %	8 %	5 %
Ich nutze keine Sicherheitssperren	9 %	12 %	7 %	8 %	12 %	5 %	14 %	10 %
Wenn Sie an einem Ort sind, an dem Sie sich sicher fühlen (z. B. das Café um die Ecke), dürfen Sie darauf vertrauen, dass Ihre Daten dort im kostenlosen WLAN-Netzwerk sicher geschützt sind.								
Wahr	45 %	26 %	26 %	20 %	13 %	28 %	26 %	26 %
Falsch	47 %	59 %	53 %	60 %	65 %	60 %	56 %	57 %
Weiß nicht	8 %	15 %	21 %	20 %	22 %	12 %	18 %	17 %
Welche der folgenden Antworten trifft für Ihr WLAN-Netzwerk zu Hause zu? (Mehrere Antworten zulässig.)								
Netzwerkname ist personalisiert	71 %	44 %	40 %	46 %	41 %	45 %	31 %	45 %
Kennwort zum Verbinden erforderlich	63 %	61 %	28 %	54 %	41 %	34 %	51 %	49 %
Standardkennwort des Routers geändert	40 %	34 %	22 %	32 %	29 %	40 %	23 %	31 %
Router-Firmware überprüft/aktualisiert	26 %	19 %	10 %	17 %	28 %	18 %	13 %	19 %
Nur einige bzw. keine diese Sicherheits-aktionen durchgeführt, da sie zu zeitaufwändig bzw. nicht praktikabel sind	13 %	8 %	15 %	7 %	6 %	15 %	10 %	11 %
Nur einige bzw. keine diese Sicherheitsaktionen durchgeführt, da zu wenig darüber bekannt ist	9 %	15 %	18 %	5 %	17 %	13 %	21 %	14 %

	USA	AUSTRALIEN	FRANKREICH	DEUTSCHLAND	JAPAN	SPANIEN	GROSS-BRITANNIEN	WELTWEITER DURCHSCHNITT
Zu Hause: Mit einer aktuellen Virenschutzlösung können Sie Zugriffe von Cyberangreifern auf Ihre Geräte verhindern.								
Wahr	73 %	69 %	55 %	70 %	52 %	76 %	68 %	66 %
Falsch	15 %	17 %	22 %	15 %	25 %	11 %	14 %	17 %
Weiß nicht	12 %	14 %	23 %	15 %	23 %	13 %	18 %	17 %
Auf Arbeit: Wenn Sie versehentlich einen Virus oder eine schädliche Software installieren, wird Ihr IT-Team automatisch von den Überwachungstools informiert, sodass das Problem behoben werden kann.								
Wahr	60 %	54 %	49 %	49 %	40 %	63 %	46 %	51 %
Falsch	19 %	19 %	17 %	19 %	27 %	12 %	24 %	20 %
Weiß nicht	21 %	27 %	34 %	32 %	33 %	25 %	30 %	29 %
Wie viele unterschiedliche Kennwörter nutzen Sie für Ihre Online-Konten? (Wählen Sie die am ehesten zutreffende Antwort.)								
Für meine Konten nutze ich einen Kennwort-Manager	44 %	23 %	15 %	17 %	22 %	20 %	22 %	23 %
Für jedes Konto gebe ich manuell ein anderes Kennwort ein	24 %	35 %	34 %	40 %	28 %	30 %	35 %	32 %
Ich wechsle zwischen fünf bis zehn Kennwörtern	20 %	25 %	32 %	33 %	29 %	33 %	28 %	29 %
Ich verwende die gleichen ein oder zwei Kennwörter für die meisten/alle Online-Konten	12 %	17 %	19 %	10 %	21 %	17 %	15 %	16 %
Ist auf den von Ihnen genutzten Computern oder Mobilgeräten ein VPN installiert?								
Ja	51 %	36 %	35 %	37 %	39 %	38 %	37 %	39 %
Nein, ich glaube nicht, dass ich ein VPN nutzen muss	25 %	34 %	32 %	30 %	24 %	30 %	30 %	29 %
Nein, ich weiß nicht, was ein VPN ist	24 %	30 %	33 %	33 %	37 %	32 %	33 %	32 %
Wie häufig nutzen Sie Ihr VPN?								
Jedes Mal, wenn Sicherheit wichtig ist	63 %	39 %	50 %	36 %	45 %	52 %	44 %	47 %
Häufig zu Hause oder unterwegs	25 %	40 %	31 %	47 %	26 %	30 %	35 %	33 %
Nur bei Bedarf (z. B. für den Zugriff auf geschützte Unternehmenssysteme)	7 %	13 %	8 %	6 %	24 %	13 %	11 %	12 %
Selten/nie	5 %	8 %	11 %	11 %	5 %	5 %	10 %	8 %

	USA	AUSTRALIEN	FRANKREICH	DEUTSCHLAND	JAPAN	SPANIEN	GROSS-BRITANNIEN	WELTWEITER DURCHSCHNITT
Für welche dieser privaten Aktivitäten nutzen Sie Ihr vom Arbeitgeber gestelltes Notebook bzw. Smartphone? (Mehrere Antworten zulässig.)								
E-Mails abrufen und beantworten	86 %	78 %	74 %	72 %	83 %	83 %	72 %	79 %
Beiträge in sozialen Netzwerken lesen/ veröffentlichen	44 %	35 %	34 %	23 %	38 %	29 %	37 %	34 %
Medien streamen (Musik, Videos etc.)	40 %	26 %	25 %	18 %	18 %	21 %	23 %	25 %
Online einkaufen	41 %	29 %	27 %	23 %	15 %	31 %	25 %	27 %
Nachrichtenartikel lesen	40 %	42 %	41 %	38 %	50 %	47 %	29 %	41 %
Recherchieren (neue Produkte, Reiseziele etc.)	38 %	42 %	37 %	33 %	39 %	45 %	23 %	37 %
Spielen	20 %	9 %	10 %	6 %	6 %	7 %	9 %	10 %
Nichts davon	5 %	8 %	10 %	19 %	7 %	11 %	9 %	10 %
Welche dieser Aktivitäten gestatten Sie Freunden/Familienmitgliedern auf Ihrem vom Arbeitgeber gestellten Notebook bzw. Smartphone? (Mehrere Antworten zulässig.)								
E-Mails abrufen und beantworten	59 %	37 %	31 %	27 %	28 %	36 %	40 %	38 %
Beiträge in sozialen Netzwerken lesen/ veröffentlichen	40 %	23 %	20 %	16 %	15 %	20 %	23 %	23 %
Medien streamen (Musik, Videos etc.)	34 %	21 %	14 %	12 %	7 %	15 %	20 %	18 %
Online einkaufen	29 %	18 %	10 %	12 %	5 %	14 %	14 %	15 %
Nachrichtenartikel lesen	22 %	15 %	16 %	11 %	11 %	18 %	9 %	15 %
Hausaufgaben recherchieren/erledigen	21 %	11 %	11 %	8 %	5 %	15 %	9 %	12 %
Spielen	15 %	10 %	8 %	3 %	3 %	7 %	7 %	8 %
Nichts davon	29 %	49 %	51 %	64 %	65 %	54 %	47 %	51 %

B. Umfrage zu IT-Sicherheit: Aufschlüsselung nach Ländern

	USA	AUSTRALIEN	FRANKREICH	DEUTSCHLAND	JAPAN	SPANIEN	GROSS-BRITANNIEN	WELTWEITER DURCHSCHNITT
Hat Ihr Unternehmen im Jahr 2019 einen erfolgreichen Phishing-Angriff verzeichnet?								
Ja	65 %	54 %	53 %	46 %	42 %	56 %	62 %	55 %
Nein	33 %	46 %	43 %	49 %	58 %	39 %	36 %	42 %
Weiß nicht	2 %	0 %	4 %	5 %	0 %	5 %	2 %	3 %
Ist die Anzahl der Phishing-Angriffe auf Ihr Unternehmen im Jahr 2019 im Vergleich zu 2018 gestiegen oder gesunken?								
Anzahl gestiegen	57 %	43 %	29 %	39 %	33 %	33 %	43 %	40 %
Anzahl gesunken	14 %	31 %	35 %	17 %	9 %	26 %	19 %	22 %
Gleich geblieben	29 %	25 %	31 %	41 %	54 %	39 %	37 %	36 %
Weiß nicht	0 %	1 %	5 %	3 %	4 %	2 %	1 %	2 %
Wie viele Spearphishing-Angriffe hat Ihr Unternehmen 2019 verzeichnet?								
0	20 %	25 %	4 %	4 %	4 %	1 %	29 %	12 %
1–10	21 %	37 %	21 %	26 %	56 %	28 %	21 %	28 %
11–25	20 %	15 %	20 %	30 %	17 %	43 %	20 %	24 %
26–50	11 %	9 %	24 %	18 %	0 %	13 %	7 %	13 %
51–100	12 %	8 %	13 %	14 %	6 %	6 %	11 %	10 %
Mehr als 100	10 %	5 %	13 %	3 %	11 %	7 %	11 %	9 %
Weiß nicht	6 %	1 %	5 %	5 %	6 %	2 %	1 %	4 %

	USA	AUSTRALIEN	FRANKREICH	DEUTSCHLAND	JAPAN	SPANIEN	GROSS-BRITANNIEN	WELTWEITER DURCHSCHNITT
Wie viele BEC-Angriffe hat Ihr Unternehmen 2019 verzeichnet?								
0	21 %	32 %	3 %	4 %	4 %	0 %	35 %	14 %
1–10	21 %	28 %	21 %	17 %	48 %	33 %	25 %	26 %
11–25	16 %	19 %	26 %	29 %	23 %	30 %	12 %	22 %
26–50	14 %	9 %	23 %	22 %	11 %	23 %	14 %	18 %
51–100	15 %	12 %	16 %	17 %	6 %	8 %	4 %	11 %
Mehr als 100	5 %	0 %	5 %	6 %	4 %	5 %	7 %	5 %
Weiß nicht	8 %	0 %	6 %	5 %	4 %	1 %	3 %	4 %
Welches der folgenden Ereignisse hat Ihr Unternehmen nach einem Phishing-Angriff im Jahr 2019 verzeichnet? (Mehrere Antworten zulässig.)								
Datenverlust	54 %	51 %	49 %	48 %	59 %	45 %	66 %	53 %
Kompromittierte Anmeldedaten/Konten	60 %	31 %	49 %	50 %	41 %	36 %	47 %	47 %
Ransomware-Infektion	51 %	54 %	42 %	50 %	32 %	43 %	48 %	47 %
Infektionen mit sonstiger Malware	36 %	26 %	28 %	33 %	41 %	55 %	28 %	35 %
Finanzielle Verluste/Überweisungsbetrug	37 %	40 %	25 %	26 %	45 %	29 %	39 %	34 %
Hat Ihr Unternehmen 2019 einen Ransomware-Angriff verzeichnet und das Lösegeld gezahlt?								
Ja	51 %	37 %	32 %	28 %	10 %	26 %	35 %	33 %
Nein, wir wurden infiziert, zahlten jedoch nicht	22 %	25 %	44 %	29 %	36 %	36 %	32 %	32 %
Nein, wir wurden nicht infiziert	27 %	38 %	24 %	43 %	54 %	38 %	33 %	35 %
Wenn Sie Lösegeld gezahlt haben, was war das Ergebnis?								
Erhielten nach der ersten Zahlung wieder Zugriff auf Daten/Systeme	80 %	88 %	50 %	39 %	100 %	81 %	69 %	69 %
Erhielten weitere Lösegeldforderungen und verzichteten dann jedoch auf eine weitere Zahlung	2 %	0 %	22 %	15 %	0 %	4 %	6 %	7 %
Zahlten erneut Lösegeld und erhielten schließlich Zugriff auf die Daten	0 %	0 %	0 %	7 %	0 %	4 %	25 %	2 %
Erhielten nie wieder Zugriff auf Daten	18 %	12 %	28 %	39 %	0 %	11 %	0 %	22 %

	USA	AUSTRALIEN	FRANKREICH	DEUTSCHLAND	JAPAN	SPANIEN	GROSS-BRITANNIEN	WELTWEITER DURCHSCHNITT
Wie berechnet Ihr Unternehmen die Kosten von Phishing-Angriffen? (Mehrere Antworten zulässig.)								
Ausfallzeiten für Endnutzer	65 %	60 %	51 %	47 %	46 %	45 %	50 %	52 %
Behebungsaufwand für IT-Sicherheitsteams	56 %	43 %	54 %	45 %	50 %	59 %	39 %	50 %
Rufschädigung	48 %	45 %	41 %	39 %	35 %	48 %	48 %	44 %
Geschäftliche Folgen durch den Verlust geistigen Eigentums	35 %	43 %	29 %	36 %	35 %	30 %	41 %	35 %
Direkte finanzielle Verluste (z. B. durch Überweisungsbetrug)	20 %	28 %	25 %	29 %	38 %	30 %	22 %	27 %
Compliance-Probleme/Geldbußen	29 %	18 %	8 %	22 %	38 %	21 %	26 %	22 %
Kosten durch Vorfallreaktion und Abhilfemaßnahmen (z. B. externe Forensik)	27 %	20 %	16 %	19 %	33 %	19 %	25 %	22 %
Gerichts- und Anwaltskosten	18 %	14 %	15 %	16 %	21 %	17 %	26 %	18 %
Umsatzverlust durch Ausfallzeiten/ verlorene Kunden	13 %	29 %	8 %	18 %	19 %	23 %	24 %	19 %
Wir ermitteln die Kosten von Phishing-Angriffen nicht	6 %	8 %	6 %	11 %	10 %	1 %	10 %	7 %
Wie viele Smishing-Angriffe (SMS-/Textnachrichten-Phishing) hat Ihr Unternehmen 2019 verzeichnet?								
0	23 %	38 %	5 %	4 %	6 %	0 %	37 %	16 %
1–10	18 %	25 %	28 %	36 %	42 %	45 %	27 %	31 %
11–25	18 %	8 %	26 %	39 %	25 %	27 %	16 %	23 %
26–50	13 %	14 %	16 %	10 %	11 %	12 %	8 %	12 %
51–100	17 %	11 %	14 %	8 %	4 %	11 %	4 %	10 %
Mehr als 100	4 %	0 %	10 %	2 %	10 %	3 %	6 %	5 %
Weiß nicht	7 %	4 %	1 %	1 %	2 %	2 %	2 %	3 %

	USA	AUSTRALIEN	FRANKREICH	DEUTSCHLAND	JAPAN	SPANIEN	GROSS-BRITANNIEN	WELTWEITER DURCHSCHNITT
Wie viele Vishing-Angriffe (Voice-Phishing) hat Ihr Unternehmen 2019 verzeichnet?								
0	22 %	43 %	4 %	5 %	4 %	1 %	43 %	17 %
1–10	20 %	22 %	31 %	39 %	54 %	42 %	21 %	31 %
11–25	19 %	9 %	27 %	31 %	19 %	27 %	9 %	21 %
26–50	12 %	12 %	13 %	10 %	9 %	16 %	9 %	12 %
51–100	15 %	9 %	15 %	11 %	6 %	7 %	9 %	11 %
Mehr als 100	5 %	0 %	8 %	2 %	6 %	6 %	6 %	5 %
Weiß nicht	7 %	5 %	2 %	2 %	2 %	1 %	3 %	3 %
Wie viele Angriffe mit manipulierten USB-Sticks hat Ihr Unternehmen 2019 verzeichnet?								
0	27 %	43 %	4 %	3 %	4 %	2 %	48 %	19 %
1–10	17 %	22 %	33 %	49 %	50 %	44 %	19 %	33 %
11–25	16 %	15 %	22 %	21 %	25 %	27 %	10 %	19 %
26–50	13 %	11 %	18 %	11 %	2 %	15 %	11 %	12 %
51–100	17 %	8 %	14 %	11 %	6 %	7 %	5 %	10 %
Mehr als 100	5 %	0 %	7 %	3 %	11 %	2 %	5 %	4 %
Weiß nicht	5 %	1 %	2 %	2 %	2 %	3 %	2 %	3 %

	USA	AUSTRALIEN	FRANKREICH	DEUTSCHLAND	JAPAN	SPANIEN	GROSS-BRITANNIEN	WELTWEITER DURCHSCHNITT
Wie viele Social-Media-Angriffe (z. B. Pretexting und Versuche der Kontoübernahme) hat Ihr Unternehmen 2019 verzeichnet?								
0	22 %	34 %	3 %	4 %	4 %	0 %	33 %	14 %
1–10	25 %	26 %	28 %	37 %	50 %	37 %	34 %	33 %
11–25	10 %	8 %	23 %	24 %	23 %	29 %	12 %	19 %
26–50	16 %	18 %	20 %	18 %	8 %	18 %	9 %	16 %
51–100	13 %	9 %	20 %	10 %	5 %	11 %	6 %	11 %
Mehr als 100	6 %	3 %	4 %	3 %	8 %	5 %	3 %	4 %
Weiß nicht	8 %	2 %	2 %	4 %	2 %	0 %	3 %	3 %
Schult Ihr Unternehmen Mitarbeiter in der Erkennung und Vermeidung von Phishing-Angriffen?								
Ja, wir führen unternehmensweite Schulungen durch	86 %	63 %	62 %	65 %	86 %	58 %	60 %	68 %
Ja, wir schulen einige Abteilungen/Rollen	8 %	32 %	31 %	26 %	10 %	38 %	36 %	27 %
Nein	6 %	5 %	4 %	6 %	4 %	3 %	4 %	4 %
Weiß nicht	0 %	0 %	3 %	3 %	0 %	1 %	0 %	1 %
Wie häufig bietet Ihr Unternehmen den Mitarbeitern Schulungen zur Verbesserung des Sicherheitsbewusstseins an?								
Zweimal im Monat	31 %	18 %	25 %	15 %	20 %	23 %	25 %	23 %
Einmal im Monat	42 %	48 %	31 %	31 %	30 %	38 %	43 %	38 %
Einmal im Quartal	18 %	16 %	28 %	27 %	28 %	21 %	26 %	23 %
Zweimal im Jahr	4 %	7 %	12 %	18 %	20 %	11 %	5 %	10 %
Einmal im Jahr	5 %	11 %	4 %	9 %	2 %	7 %	1 %	6 %

	USA	AUSTRALIEN	FRANKREICH	DEUTSCHLAND	JAPAN	SPANIEN	GROSS-BRITANNIEN	WELTWEITER DURCHSCHNITT
Wie viel Zeit widmet Ihr Unternehmen den Schulungen zur Verbesserung des Sicherheitsbewusstseins in einem Kalenderjahr?								
0–30 Minuten	9 %	8 %	12 %	3 %	12 %	6 %	2 %	7 %
31–59 Minuten	32 %	31 %	31 %	31 %	24 %	28 %	30 %	30 %
1–2 Stunden	37 %	43 %	37 %	51 %	48 %	46 %	40 %	43 %
2–3 Stunden	12 %	8 %	15 %	9 %	2 %	7 %	13 %	10 %
Mehr als 3 Stunden	10 %	10 %	5 %	6 %	14 %	13 %	15 %	10 %
Welche Hilfsmittel zur Steigerung des Sicherheitsbewusstseins nutzt Ihr Unternehmen? (Mehrere Antworten zulässig.)								
Simulierte Phishing-Angriffe	66 %	53 %	52 %	49 %	72 %	55 %	49 %	56 %
Präsenzschulungen	59 %	66 %	60 %	56 %	40 %	66 %	69 %	61 %
Computer-basierte Schulungen	62 %	63 %	48 %	60 %	58 %	65 %	64 %	60 %
Poster und Videos	32 %	35 %	40 %	16 %	26 %	20 %	36 %	30 %
Newsletter und E-Mails	31 %	32 %	28 %	43 %	34 %	20 %	30 %	31 %
Wettbewerbe und Preise zum Thema Cybersicherheit	22 %	27 %	16 %	22 %	22 %	20 %	23 %	21 %
Simulierte Smishing- und Vishing-Angriffe	17 %	27 %	29 %	23 %	28 %	32 %	24 %	25 %
Simulierte Angriffe mit abgelegten manipulierten USB-Sticks	16 %	18 %	11 %	13 %	28 %	13 %	18 %	16 %
Schaltfläche, über die Mitarbeiter verdächtige E-Mails melden können	13 %	19 %	9 %	15 %	18 %	15 %	17 %	15 %
Konnte Ihr Unternehmen nach Schulungen zur Steigerung des Sicherheitsbewusstseins eine reduzierte Anfälligkeit für Phishing feststellen?								
Ja	91 %	79 %	71 %	71 %	72 %	80 %	78 %	78 %
Nein	7 %	16 %	23 %	18 %	18 %	17 %	17 %	16 %
Weiß nicht	2 %	5 %	6 %	11 %	10 %	3 %	5 %	6 %
Nutzt Ihr Unternehmen ein Konsequenzmodell für Mitarbeiter, die regelmäßig auf Phishing-Angriffe hereinfallen? (D. h. gibt es Strafen für Wiederholungstäter?)								
Ja	78 %	62 %	67 %	53 %	60 %	59 %	60 %	63 %
Nein	22 %	32 %	28 %	39 %	38 %	39 %	38 %	33 %
Weiß nicht	0 %	6 %	5 %	8 %	2 %	2 %	2 %	4 %

	USA	AUSTRALIEN	FRANKREICH	DEUTSCHLAND	JAPAN	SPANIEN	GROSS-BRITANNIEN	WELTWEITER DURCHSCHNITT
Welche Strafen werden im Rahmen des Konsequenzmodells in Ihrem Unternehmen verhängt? (Mehrere Antworten zulässig.)								
Beratung durch den Manager	63 %	53 %	25 %	47 %	58 %	47 %	45 %	48 %
Beratung durch das IT-Sicherheitsteam	42 %	55 %	66 %	47 %	65 %	47 %	47 %	51 %
Präsenzschulungen	50 %	60 %	49 %	62 %	42 %	47 %	68 %	54 %
Verpflichtende Online-Schulungen	35 %	38 %	43 %	32 %	39 %	44 %	45 %	39 %
Durch Personalabteilung verhängte Disziplinarmaßnahmen	25 %	20 %	18 %	26 %	35 %	24 %	21 %	23 %
Sperrung des Zugriffs auf Systeme	18 %	28 %	15 %	26 %	45 %	17 %	18 %	21 %
Finanzielle Strafen	20 %	8 %	16 %	17 %	16 %	15 %	21 %	17 %
Abmahnung/Bewährungsfrist	23 %	15 %	19 %	32 %	26 %	19 %	31 %	23 %
Kündigung	12 %	10 %	13 %	11 %	10 %	10 %	11 %	11 %
Hat die Nutzung eines Konsequenzmodells zu einer Verbesserung der Mitarbeiter-Sensibilisierung geführt?								
Ja, es hat einen Unterschied gemacht	92 %	80 %	79 %	83 %	84 %	83 %	86 %	84 %
Nein, es hat keinen Unterschied gemacht	6 %	13 %	21 %	15 %	10 %	15 %	11 %	13 %
Nicht sicher, wir haben das nicht ausgewertet	2 %	2 %	0 %	2 %	6 %	2 %	3 %	2 %
Weiß nicht	0 %	5 %	0 %	0 %	0 %	0 %	0 %	1 %

C. Fehlerquoten nach Branchen bei simulierten Phishing-Vorlagenstilen

Unterschiedliche Ansichten Ihrer Daten können neue Erkenntnisse bringen. Die folgende Tabelle zeigt die Fehlerquoten auf Anwender- und Unternehmensebene bei den drei unterschiedlichen Phishing-Test-Stilen in jeder Branche. Die Unterschiede zwischen diesen beiden Zahlen sind oft erheblich.

Wie weiter oben in diesem Bericht bereits erwähnt, kann der Durchschnittswert auf Anwenderebene von bestimmten Faktoren übermäßig beeinflusst werden. Dies ist der Fall bei den Fehlerquoten Anhang-basierter Tests. Dieser Vorlagenstil wurde 2019 am wenigsten von unseren Kunden genutzt – nur 10 % aller simulierten Phishing-E-Mails testeten die Anwenderreaktionen auf Anhänge. Die Anwender-Fehlerquoten in diesen kleineren Proben können durch schwer zu erkennende Köder sowie geringe Anwendersensibilisierung für Anhang-basiertes Phishing beeinflusst worden sein.

DURCHSCHNITTLICHE FEHLERQUOTE (ANWENDEREBENE, UNTERNEHMENSEBENE)

BRANCHE	TESTS MIT LINK	TESTS MIT ANHANG	TEST, DER ZUR DATENEINGABE AUFFORDERT
Behörden	14 %, 14 %	22 %, 21 %	5 %, 4 %
Bildungswesen	10 %, 10 %	9 %, 17 %	3 %, 4 %
Dienstleistungen	11 %, 14 %	14 %, 13 %	3 %, 4 %
Einzelhandel	11 %, 11 %	20 %, 27 %	3 %, 4 %
Energie- und Versorgungsunternehmen	8 %, 14 %	13 %, 18 %	2 %, 3 %
Fertigungsindustrie	9 %, 13 %	19 %, 22 %	3 %, 4 %
Finanzdienstleister	15 %, 14 %	34 %, 26 %	5 %, 3 %
Finanzsektor	8 %, 11 %	13 %, 18 %	3 %, 3 %
Gastgewerbe	14 %, 14 %	17 %, 51 %	5 %, 7 %
Gesundheitswesen	8 %, 12 %	11 %, 16 %	4 %, 4 %
Konsumgüter	12 %, 13 %	27 %, 23 %	2 %, 3 %
Lebensmittel/Getränke	9 %, 16 %	24 %, 12 %	2 %, 2 %
Maschinenbau	7 %, 10 %	4 %, 9 %	7 %, 7 %
Technologie	10 %, 13 %	14 %, 16 %	6 %, 4 %
Telekommunikation	8 %, 11 %	14 %, 18 %	6 %, 5 %
Transportwesen	14 %, 14 %	9 %, 14 %	6 %, 5 %
Unterhaltung/Medien	17 %, 16 %	18 %, 28 %	3 %, 3 %
Unternehmensdienstleistungen	9 %, 10 %	59 %, 23 %	4 %, 4 %
Versicherungen	11 %, 12 %	39 %, 26 %	4 %, 2 %

WEITERE INFORMATIONEN

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

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) ist ein führendes Cybersicherheitsunternehmen. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, setzen auf die personenorientierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.com**.

proofpoint.

0400-002-01-01 12/19