Phishing-Report 2021 – Aktuelle Einblicke

Phishing ist keine neue Erscheinung, bleibt aber nach wie vor eine hocheffektive Technik für Cyberangriffe. Denn Phishing entwickelt sich kontinuierlich weiter. Für Hacker bieten sich immer wieder neue Gelegenheiten für Phishing-Angriffe, so etwa auch vermehrt in der Corona-Pandemie. Dabei passen sie ihre Taktiken und Techniken fortlaufend an neue Situationen an.

Phishing bildet häufig den ersten Schritt eines komplexen, mehrstufigen Angriffs auf Organisationen. Dabei verleiten Cyberkriminelle Benutzer meist dazu, Malware zu installieren oder sensible Daten zu teilen, die Zugang zum Netzwerk ihrer Opfer ermöglichen. Eine vermeintlich harmlose E-Mail kann so Ransomware, Cryptojacking oder Datendiebstahl nach sich ziehen.

Dieser Report basiert auf den Ergebnissen einer unabhängigen Befragung von 5.400 IT-Entscheidern in aller Welt und liefert aktuelle Erkenntnisse zum Thema Phishing. Außerdem können Sie in einer Case Study eines realen Phishing-Angriffs nachlesen, wie Cyberkriminelle Ransomware installieren und mehrere Millionen Dollar Lösegeld fordern konnten.

Dem Verizon 2021 Data Breach Investigation Report zufolge sind 36 % aller bestätigten Datenschutzverletzungen unter anderem auf Phishing zurückzuführen (ggü. 25 % in 2019). Nutzen Sie die Umfrageergebnisse und unsere Tipps, um Ihren aktuellen Schutz gegen Phishing zu bewerten und zu entscheiden, welche zusätzlichen Maßnahmen Ihren Schutz verbessern können.

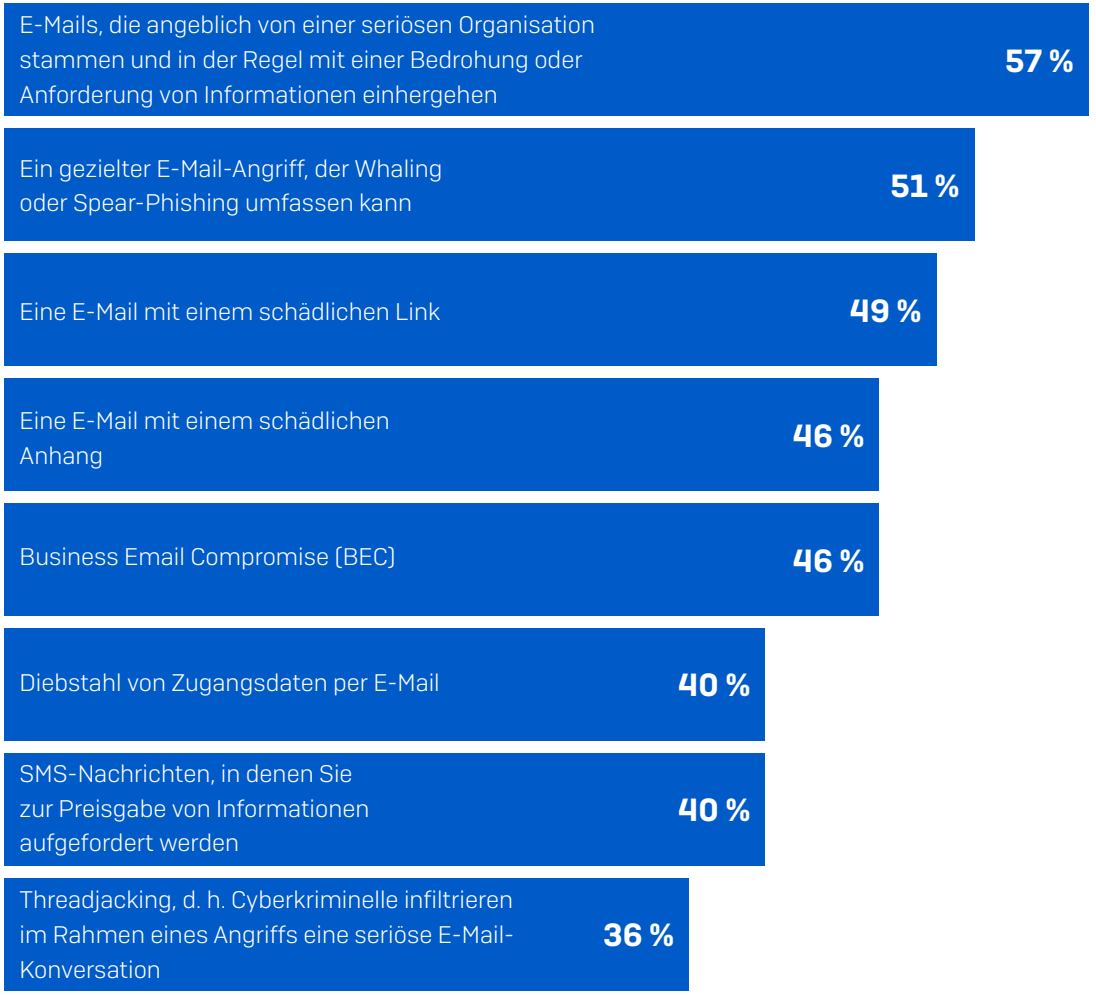
SOPHOS

1. Phishing bedeutet nicht für jeden das Gleiche

Was ist Phishing? Wie unsere Umfrage zeigt, gehen selbst unter IT-Fachleuten die Meinungen darüber auseinander, was genau unter einem Phishing-Angriff zu verstehen ist. Die Mehrheit der Umfrageteilnehmer definiert Phishing als *E-Mails, die angeblich von einer seriösen Organisation stammen und in der Regel mit einer Bedrohung oder Anfrage nach Informationen einhergehen*. Allerdings wählten lediglich 57 % (weniger als sechs von zehn) der Befragten diese Antwort-Option aus, was zeigt, dass Phishing oft sehr unterschiedlich verstanden wird.

46 % halten Business Email Compromise (BEC)-Angriffe für Phishing. Mehr als ein Drittel (36 %) geht dagegen davon aus, dass Phishing mit Threadjacking (Angreifer infiltrieren einen echten geschäftlichen E-Mail-Thread) gleichzusetzen ist.

Welche der folgenden Antworten beschreibt Ihrer Meinung nach einen Phishing-Angriff?



Welche Antwort beschreibt Ihrer Meinung nach einen Phishing-Angriff? [5.400], wobei einige Antwortmöglichkeiten übersprungen wurden

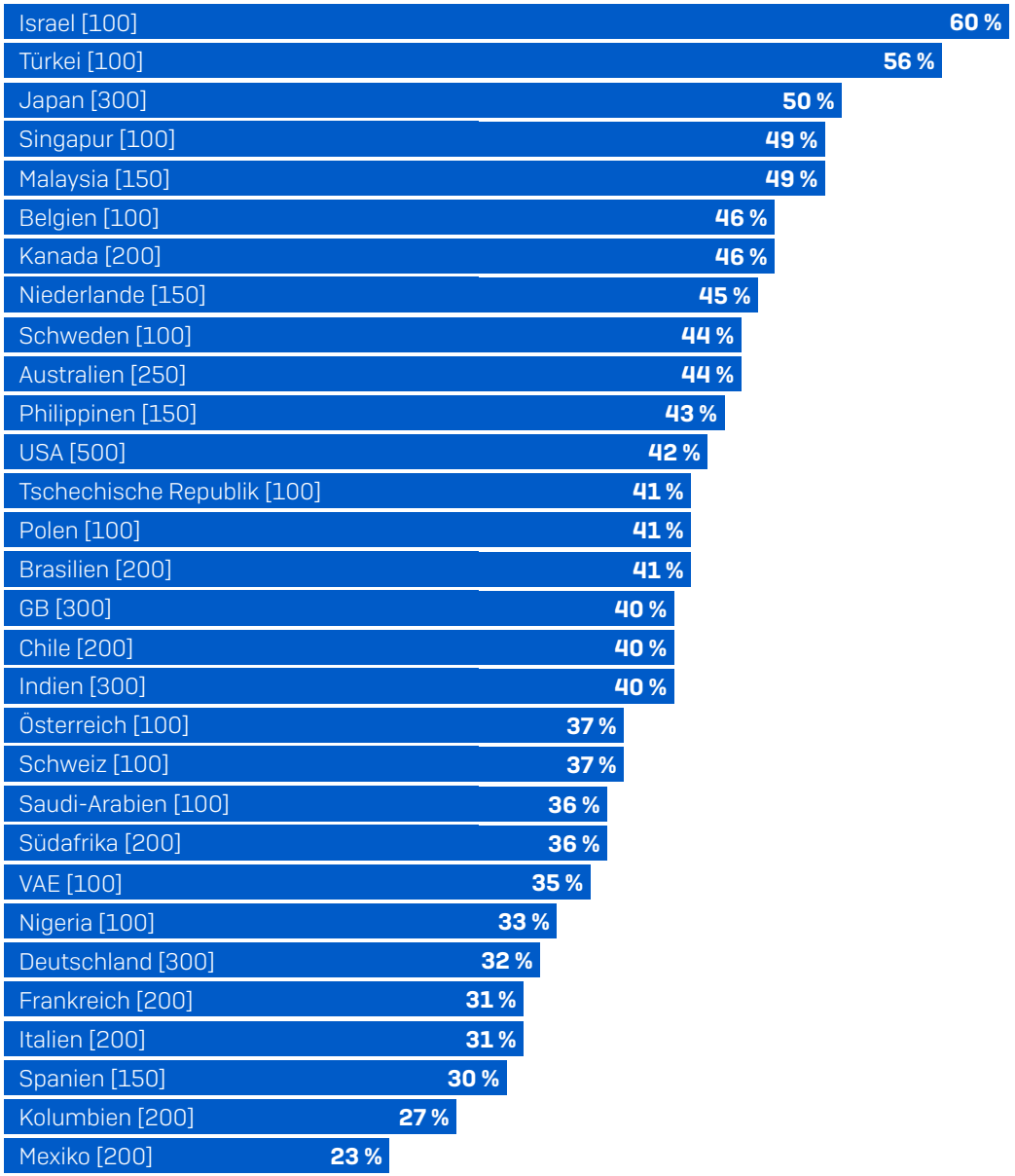
Zudem ist das Verständnis von Phishing stark von kulturellen Faktoren geprägt. So sehen beispielsweise im Vergleich zu den Befragten in Mexiko etwa mehr als doppelt so viele israelische Umfrageteilnehmer (60 % ggü. 23 %) SMS-Nachrichten, die zur Preisgabe von Daten auffordern, als Phishing an. Zwar sprechen viele IT-Experten hier eher von Smishing, das Prinzip ist jedoch das gleiche, denn es geht um betrügerische Nachrichten von vermeintlich seriösen Unternehmen.

Wenn IT-Experten Phishing-Angriffe auf so unterschiedliche Weise verstehen und definieren, ist davon auszugehen, dass die Meinungen dazu auch unter Mitarbeitern, die nicht in der IT tätig sind, auseinander gehen.

Daher spielt die Tatsache, dass Phishing nicht für jeden das Gleiche bedeutet, bei der Ausarbeitung oder Durchführung von Phishing-Awareness-Programmen und -Schulungen eine wesentliche Rolle. Damit das Phishing-Training auch effektiv ist, sollte vorab eine einheitliche Begriffsdefinition erfolgen. Nur so kann das Gelernte im richtigen Kontext verstanden werden.

TIPP: Bedenken Sie bei Phishing-Awareness-Angeboten und -Schulungsmaterialien, dass Phishing nicht für jeden das Gleiche bedeutet. Ohne den richtigen Kontext sind Schulungsmaßnahmen weniger effektiv.

Umfrageteilnehmer, die SMS-Nachrichten, in denen sie zur Preisgabe von Informationen aufgefordert werden, als Phishing ansehen



Welche Antwort beschreibt Ihrer Meinung nach einen Phishing-Angriff? [Basiszahlen im Diagramm] SMS-Nachrichten, in denen Sie zur Preisgabe von Informationen aufgefordert werden

2. Phishing-Angriffe haben seit Beginn der Corona-Pandemie stark zugenommen

70 % der Umfrageteilnehmer meldeten eine Zunahme der Phishing-Attacken auf ihre Organisation seit Beginn der Pandemie. Davon waren alle Branchen und Sektoren betroffen: Den größten Zuwachs (77 %) verzeichneten Bundesbehörden, gefolgt von Unternehmens- und Fachdienstleistungen (76 %) und dem Gesundheitswesen (73 %).

Die geringe Abweichung zwischen den Branchen bzw. Sektoren (nur 10 Prozentpunkte vor Rundung)* zeigt, dass Cyberkriminelle oft wahllos vorgehen und versuchen, so viele Benutzer wie möglich zu erreichen, um die Erfolgswahrscheinlichkeit zu erhöhen.

Studien der SophosLabs zufolge konnten die Angreifer die Pandemie und die damit einhergehenden verschwimmenden Grenzen zwischen beruflicher und privater Computernutzung schnell zu ihrem Vorteil nutzen. Faktoren waren u.a.:

- **Wesentlich mehr Mitarbeiter im Homeoffice.** Wahrscheinlich hofften Cyberkriminelle, dass Benutzer bei der Umstellung auf die Arbeit im Homeoffice weniger Vorsicht walten lassen würden.
- **Zunehmende Nutzung von Versanddiensten**. In den ersten Monaten der Pandemie häuften sich Phishing-Nachrichten, die vermeintlich von Versanddiensten stammten, da immer mehr Menschen online bestellten.
- **Angst vor der Pandemie.** Hacker nutzten die Ängste und den Informationsbedarf der Menschen aus und verschickten COVID-19-Scams. Sie gingen davon aus, dass Benutzer aufgrund der allgemeinen Beunruhigung auf Nachrichten klicken würden, ohne zu prüfen, ob diese seriös sind.

Branchen/Sektoren	Umfrageteilnehmer, die eine Zunahme der Phishing-Angriffe auf ihre Organisation seit Beginn der Pandemie verzeichneten
Bundesbehörden und öffentliche Einrichtungen [117]	77 %
Unternehmens- & Fachdienstleistungen [361]	76 %
Gesundheitswesen [328]	73 %
Medien, Freizeit und Unterhaltung [145]	72 %
Energie, Öl/Gas und Versorgungsunternehmen [197]	72 %
Hersteller, Dienstleister & Einzelhandel [435]	71 %
Bildung [499]	71 %
Sonstige [768]	71 %
Behörden auf Landes- und Kommunalebene [131]	69 %
Vertrieb und Transport [203]	68 %
Finanzdienstleistungen [550]	68 %
Bauwesen und Immobilien [232]	68 %
IT, Technologie und Telekommunikation [996]	68 %
Fertigung und Produktion [438]	66 %

Konnten Sie eine Veränderung der Anzahl der Phishing-Angriffe auf Ihre Organisation seit Beginn der Pandemie feststellen? [Basiszahlen im Diagramm] Ja, signifikanter Anstieg, Ja, geringer Anstieg

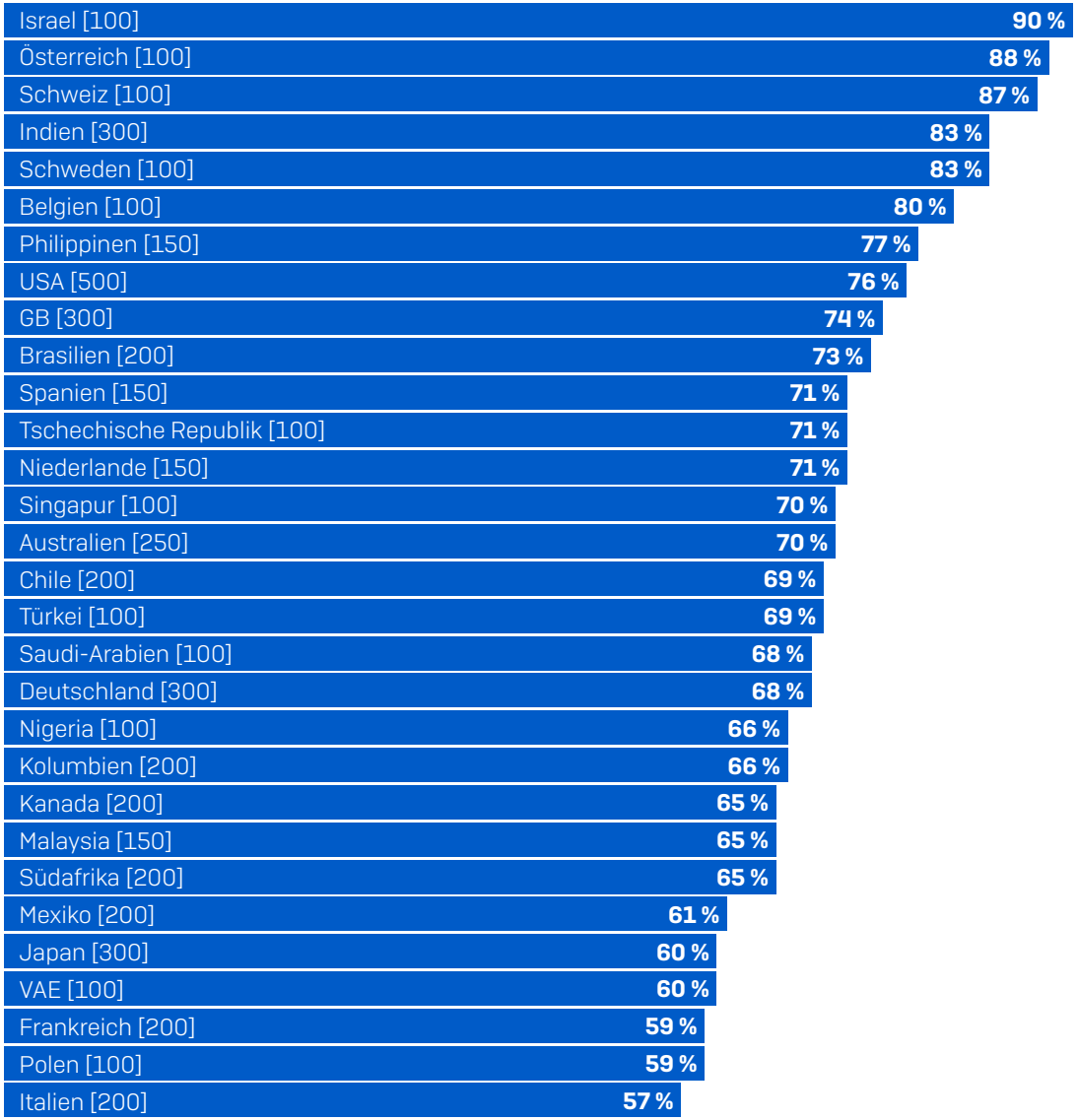
** Vor Rundung meldeten 76,92 % der Umfrageteilnehmer aus Bundesbehörden einen Anstieg gegenüber 66,43 % aus dem Bereich Fertigung und Produktion. Daraus ergibt sich eine tatsächliche Differenz von 10,48 %*

Trotz größtenteils homogener Ergebnisse über alle Branchen/Sektoren hinweg zeigte die Umfrage im Ländervergleich jedoch enorme Diskrepanzen bei der Zunahme von Phishing-Angriffen seit Beginn der Pandemie. So verzeichneten etwa 90 % der Befragten in Israel mehr Phishing-Angriffe. In Italien lag der prozentuale Anteil hingegen lediglich bei 57 %. Auch wenn diese Ergebnisse von der jeweiligen Phishing-Definition der Umfrageteilnehmer sowie deren Fähigkeit, Angriffe nachzuverfolgen, beeinflusst wurden, bieten sie dennoch wertvolle Einblicke in die realen Erfahrungen von IT-Mitarbeitern an vorderster Front.

Es gibt viele unterschiedliche Arten von Phishing-Emails. In gleichem Maße unterscheiden sich auch die Drahtzieher hinter den Angriffen. Versierte Akteure konzentrieren sich in der Regel gezielt auf Länder mit höherem BIP, wie etwa Österreich, die Schweiz oder Schweden, um maximalen Profit aus ihren Angriffen zu schlagen – ein Umstand, der möglicherweise das hohe Phishing-Aufkommen in den genannten Ländern erklärt. Gleichzeitig findet Phishing auch bei generischen Spray-and-Pray-Angriffen Anwendung. Solche Scams zielen auf möglichst viele Benutzer ab, in der Hoffnung, dass sich irgendwann ein Opfer findet.

TIPP: Vernachlässigen Sie nicht Ihre Anti-Phishing-Maßnahmen. Cyberkriminelle greifen vermehrt auf Phishing zurück: Keine Branche, kein Land bleibt verschont.

Umfrageteilnehmer, die eine Zunahme der Phishing-Angriffe auf ihre Organisation seit Beginn der Pandemie verzeichneten



Konnten Sie eine Veränderung der Anzahl der Phishing-Angriffe auf Ihre Organisation seit Beginn der Pandemie feststellen? [Basiszahlen im Diagramm] Ja, signifikanter Anstieg, Ja, geringer Anstieg

3. Viele Organisationen schulen ihre Mitarbeiter in puncto Phishing

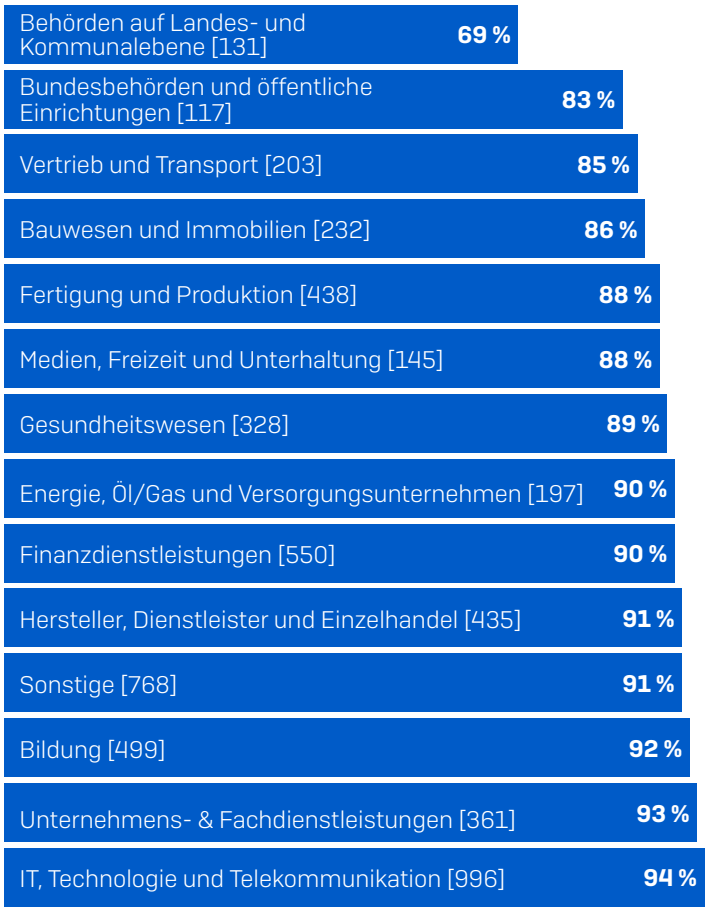
90 % der befragten Organisationen nutzen bereits Cybersecurity-Awareness-Programme zum Schutz vor Phishing. 6 % planen, ein solches Programm einzuführen.

Die Mehrheit der Organisationen (58 %) setzt dabei auf Online-Training. Mehr als die Hälfte (53 %) setzt auf Schulungen mit einem Kursleiter, 43 % führen Phishing-Simulationen durch. 16 % kombinieren alle drei Methoden (Online-Training, Schulungen mit Kursleiter und Phishing-Simulationen) bei ihren Awareness-Programmen.

Unsere Umfrage hat gezeigt, dass insbesondere im öffentlichen Sektor Nachholbedarf bei der Aufklärung über Phishing durch Cybersecurity-Awareness-Programme besteht: Behörden auf Landes- und Kommunalebene liegen mit 69 % und Bundesbehörden mit 83 % auf den letzten Plätzen. Ein beunruhigendes Lagebild, zumal Cyberkriminelle häufig gezielt Behörden ins Visier nehmen. So sind Bundesbehörden und öffentliche Einrichtungen besonders anfällig für Extortion-Angriffe. Bei Behörden auf Landes- und Kommunalebene hingegen ist die Wahrscheinlichkeit am größten, dass Daten im Zuge eines Ransomware-Angriffs verschlüsselt werden.

TIPP: Wenn Ihre Organisation zu den 10 % zählt, die Phishing noch nicht mit Cybersecurity-Awareness-Programmen bekämpfen, sollten Sie dies umgehend ändern.

Einsatz von Cybersecurity-Awareness-Programmen zu Phishing



Nutzt Ihre Organisation Cybersecurity-Awareness-Programme zum Schutz vor Phishing? [5.400] Ja, wir führen Online-Trainingsprogramme durch; Ja, wir führen Schulungen mit Kursleiter durch; Ja, wir führen Phishing-Simulationen durch

90 %

nutzen Cybersecurity-Awareness-Programme zum Schutz vor Phishing

58 %

führen Online-Trainingsprogramme durch

53 %

führen Schulungen mit Kursleiter durch

43 %

führen Phishing-Simulationen durch

Nutzt Ihre Organisation Cybersecurity-Awareness-Programme zum Schutz vor Phishing? [5.400] Ja, wir führen Online-Trainingsprogramme durch; Ja, wir führen Schulungen mit Kursleiter durch; Ja, wir führen Phishing-Simulationen durch

4. Phishing-Awareness-Programme werden häufig genutzt

Beinahe zwei Drittel (65 %) der Phishing-Awareness-Programme wurden in den letzten ein bis drei Jahren eingeführt. Damit reagierten die Organisationen auf neue Angriffstechniken. Aufgrund verbesserter Abwehrmechanismen vor webbasierten Angriffen in der Mitte der 2010er Jahre griffen Cyberkriminelle auf neue Angriffsvektoren wie E-Mails zurück, weshalb wiederum die Belegschaft entsprechend geschult werden musste.

Angesichts des hohen Phishing-Aufkommens seit Beginn der Pandemie stimmt es positiv, dass 98 % der Organisationen Phishing-Awareness-Programme schon vor 2020 eingeführt hatten. So gelang es ihnen, die Flut an Phishing-E-Mails des letzten Jahres abzuwehren.

TIPP: Überprüfen und aktualisieren Sie Ihre Phishing-Awareness-Materialien und -Programme in regelmäßigen Abständen, um sicherzustellen, dass sie nach wie vor auf dem neuesten Stand sind.

Wann hat Ihre Organisation Cybersecurity-Awareness-Programme zum Schutz vor Phishing eingeführt?	
Innerhalb des letzten Jahres	2 %
Vor 1–2 Jahren	30 %
Vor 2–3 Jahren	35 %
Vor 3–4 Jahren	20 %
Vor 4–5 Jahren	12 %
Vor mehr als 5 Jahren	0 %
Unsicher	1 %

Organisationen, die Awareness-Programme zum Schutz vor Phishing nutzen [4.866]

5. Positives Verhalten der Nutzer wird gemessen, um Effektivität des Awareness-Trainings zu bewerten

Fast alle (98 %) Organisationen, die User-Awareness-Programme einsetzen, analysieren die Effektivität ihrer Maßnahmen. So können sie ihre Programme optimieren und noch bessere Ergebnisse erzielen.

Am häufigsten (68 %) werden an die IT gemeldete Phishing-E-Mails und/oder von Benutzern gemeldetes Phishing (65 %) erfasst. Tracking-Maßnahmen, die ein positives Verhalten der Nutzer und die Phishing-Awareness von Mitarbeitern bewerten, sind am weitesten verbreitet. Durch das Erkennen von Phishing-Angriffen und die Sensibilisierung von Mitarbeitern können IT-Teams proaktiv verhindern, dass andere den Hackern in die Falle gehen.

Die Hälfte der Organisationen (50 %) erfassen Klickraten bei Phishing-E-Mails. Auch wenn Klickraten negatives Verhalten (Benutzer klicken auf Links) messen, liefern sie IT-Teams dennoch wertvolle Daten zur gezielten, bedarfsgerechten Durchführung von Awareness-Programmen und individuellen Anpassung von Schulungsmaterialien. Je mehr Daten zum Verhalten (positiv wie negativ) Sie erfassen können, desto besser.

TIPP: Passen Sie Ihre Mitarbeiterschulungen regelmäßig an die Ergebnisse Ihrer Phishing-Tests an und honorieren Sie ein positives Verhalten der Nutzer.

98 %
analysieren die Effektivität ihrer Awareness-Programme

68 %
erfassen die Zahl der IT-Tickets im Zusammenhang mit Phishing

65 %
erfassen die Zahl der an die IT gemeldeten Phishing-E-Mails

50 %
erfassen Klickraten bei Phishing-E-Mails

Wie beurteilen Sie die Effektivität Ihrer Awareness-Programme? [4.866 Umfrageteilnehmer, die Awareness-Programme zum Schutz vor Phishing nutzen] Zahl der IT-Tickets im Zusammenhang mit Phishing; Zahl der an die IT gemeldeten Phishing-E-Mails; Klickrate bei Phishing-E-Mails. Wir analysieren die Effektivität unserer Awareness-Programme nicht. Einige Antwortmöglichkeiten wurden übersprungen

Case Study: Folgenschwere Phishing-E-Mail: Cyberkriminelle fordern Lösegeld in Millionenhöhe

Vor Kurzem wurden die Rapid-Response-Experten von Sophos damit beauftragt, ein Unternehmen bei der Abwehr eines groß angelegten Ransomware-Angriffs zu unterstützten. Nachdem der Angriff erfolgreich eingedämmt war, analysierte das Rapid-Response-Team die Ursache des Vorfalls. Das Ergebnis:

Drei Monate vor dem Angriff erhielt ein Mitarbeiter eine Phishing-E-Mail. Allem Anschein nach handelte es sich bei dem Absender der E-Mail um einen Kollegen aus einer anderen Niederlassung. Wahrscheinlich hatten sich die Angreifer Zugriff auf das E-Mail-Konto des Kollegen verschafft, um die Nachricht vertrauenswürdig erscheinen zu lassen.

Die E-Mail war sehr kurz und in gebrochenem Englisch verfasst. Der betroffene Mitarbeiter wurde in der E-Mail dazu aufgefordert, auf einen Link zu klicken und ein Dokument zu prüfen. Dabei handelte es sich jedoch um einen schädlichen Link: Sobald der Empfänger darauf geklickt hatte, konnten sich die Angreifer Zugriff auf Domänen-Admin-Anmeldeinformationen verschaffen.

Das Rapid-Response-Team geht davon aus, dass die Phishing-E-Mail von einem sogenannten Initial Access Broker (IAB) versendet wurde. IABs sind darauf spezialisiert, Zugangsdaten zu hacken und diese an andere Cyberkriminelle für Ransomware-Angriffe oder Datendiebstahl zu verkaufen.

In diesem Fall schritt die IT-Abteilung des betroffenen Unternehmens ein und wehrte den Phishing-Angriff ab. Scheinbar war der Vorfall damit behoben.

Acht Wochen später installierte ein Angreifer jedoch zwei Tools (Cobalt Strike und PowerSploit PowerView) auf dem betroffenen System und führte diese aus. Hierbei handelt es sich um kommerziell verfügbare Tools von Penetrationstestern, die Cyberkriminelle für illegale Zwecke missbrauchen. Vermutlich kundschafteten die Angreifer das kompromittierte Netzwerk zunächst mit PowerView aus. Cobalt Strike sorgte dabei für Persistenz im Netzwerk.

Nach ca. zwei Wochen stellten die Angreifer ihre Aktivitäten ein. Das Rapid-Response-Team vermutet, dass der Initial Access Broker in diesem Zeitraum nach einem Käufer für die Zugangsdaten suchte.

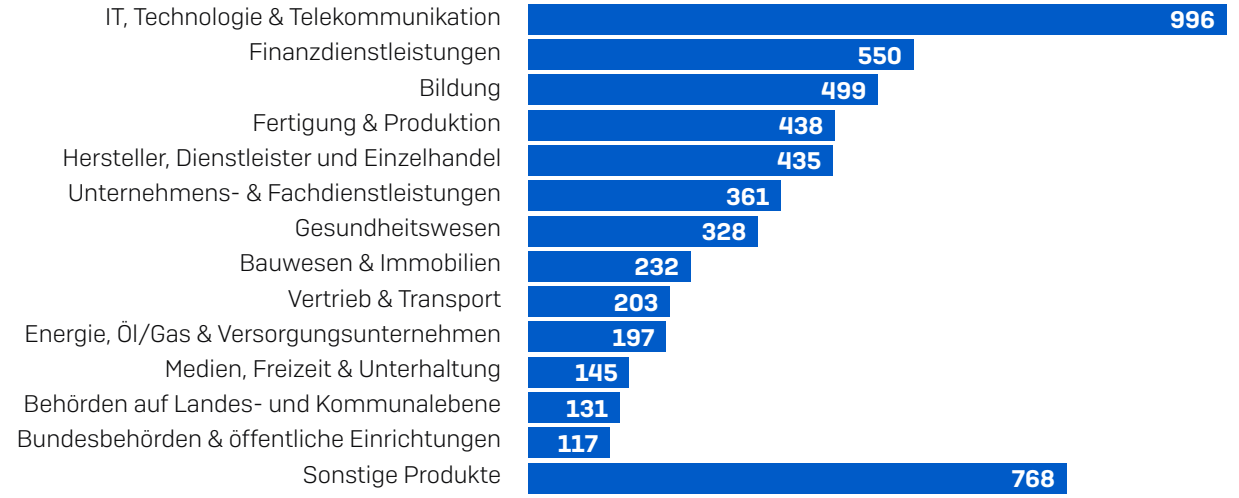
Im Anschluss an die Transaktion brachten die neuen „Besitzer" die erworbenen Zugangsdaten schnell zum Einsatz. Sie installierten Cobalt Strike auf weiteren Systemen und sammelten und stahlen Daten.

Drei Monate nach der ursprünglichen Phishing-E-Mail brachten die Angreifer die Ransomware „REvil" um 4 Uhr Ortszeit in Umlauf und forderten ein Lösegeld in Höhe von 2,5 Millionen US-Dollar.

Über die Studie

Sophos hat eine unabhängige Befragung zum Thema Phishing in Auftrag gegeben, die vom Marktforschungsinstitut Vanson Bourne zwischen Januar und Februar 2021 durchgeführt wurde. Im Rahmen dieser Studie wurden 5.400 IT-Entscheider aus mittelständischen Unternehmen und öffentlichen Einrichtungen (100 bis 5.000 Mitarbeiter) in 30 Ländern befragt.

Anzahl der Befragten nach Branche/Sektor



Anzahl der Befragten pro Land

Land	# Umfrageteilnehmer	Land	# Umfrageteilnehmer	Land	# Umfrageteilnehmer
Australien	250	Indien	300	Saudi-Arabien	100
Österreich	100	Israel	100	Singapur	150
Belgien	100	Italien	200	Südafrika	200
Brasilien	200	Japan	300	Spanien	150
Kanada	200	Malaysia	150	Schweden	100
Chile	200	Mexiko	200	Schweiz	100
Kolumbien	200	Niederlande	150	Türkei	100
Tschechische Republik	100	Nigeria	100	VAE	100
Frankreich	200	Philippinen	150	GB	300
Deutschland	300	Polen	100	USA	500

2021-08-13 WPDE (NP)

SOPHOS