proofpoint.

State of the Phish: Auf einen Blick

EINFÜHRUNG

Cybersicherheit kann schon unter normalen Umständen schwierig sein. In turbulenten Zeiten wie einer weltweiten Pandemie, die zu dramatischen Veränderungen in beruflichen Umgebungen führt, kann sie unmöglich erscheinen. Im Laufe des letzten Jahres erlebten IT-Sicherheitsexperten eine Lawine von Phishing-Betrug mit Coronavirus-Bezug sowie eine Flut von Ransomware-Angriffen. Gleichzeitig haben sie Schwierigkeiten, nach dem abrupten Wechsel ins Home Office die Sicherheit ihrer Anwender zu gewährleisten.

Unser *State of the Phish-Bericht 2021* beleuchtet diese und weitere Entwicklungen. Er stellt die aktuell schwerwiegendsten Bedrohungen vor und analysiert dazu simulierte Phishing-Übungen, Umfragen und reale Cyberangriffe. Ebenso werden die größten Schwachstellen der Anwender thematisiert. Vor allem aber bietet er Empfehlungen für Ihre weiteren Schritte.

Das sind die wichtigsten Erkenntnisse im diesjährigen Bericht.

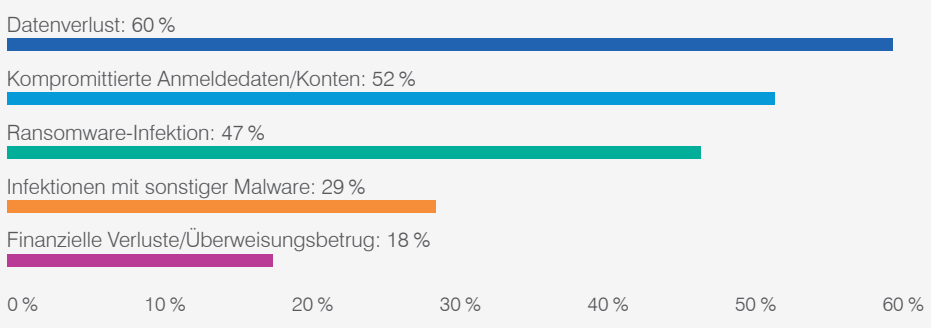
DIE BEDROHUNGEN NEHMEN ZU

Für Phishing-Angriffe war 2020 ein Erfolgsjahr, in dem Opfer auf verschiedenste Weise angegriffen wurden.

57 %

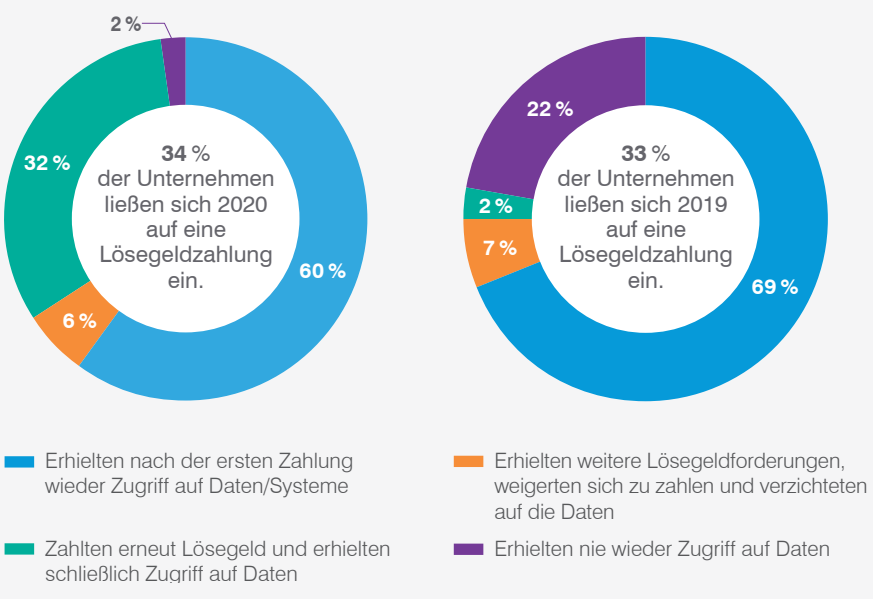
der Teilnehmer einer Drittanbieter-Umfrage gaben an, ihr Unternehmen hätte 2020 einen erfolgreichen Phishing-Angriff erlebt. 2019 waren es mit **55 %** etwas weniger.

Folgen erfolgreicher Phishing-Angriffe



Ein etwas höherer Anteil der Ransomware-Opfer bezahlte die Angreifer, um wieder Zugriff auf die eigenen Daten und Systeme zu erlangen. Doch seltener als bisher wurde das Versprechen auch eingehalten, sodass fast ein Drittel weitere Lösegelder zahlte.

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



INTERNATIONAL

68 % der US-Unternehmen gaben an, 2020 ein Lösegeld bezahlt zu haben (doppelt so viel wie der weltweite Durchschnitt).

41 % der spanischen Unternehmen lehnte die Zahlung von Lösegeld nach einer Infektion ab und verhandelten am seltensten mit den Angreifern.

78 % der französischen Unternehmen hatten nach der Zahlung eines einmaligen Lösegeldes das Glück, wieder Zugriff auf ihre Daten und Systeme zu erhalten. Das ist die höchste Zahl unter allen befragten Regionen (die USA lagen mit **76 %** auf Platz 2).

14 % der deutschen Unternehmen lehnten die Zahlung eines Folgelösegeldes ab, der höchste Wert unter den untersuchten Regionen.

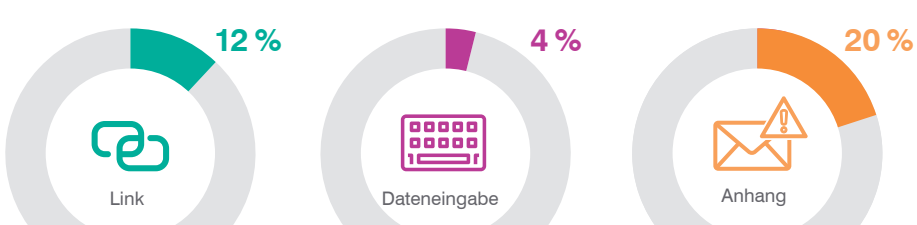
GRÖSSTE SCHWACHSTELLEN DER ANWENDER

Heutige Angriffe richten sich nicht mehr ausschließlich gegen Technologie, sondern auch gegen Menschen. Erst wenn Sie wissen, wo Anwender ihre größten Schachstellen haben, können Sie die richtigen Maßnahmen ergreifen.

Mehr als 10 % der Anwender klickten auf eine simulierte Phishing-E-Mail. Bei Phishing-Tests mit Anhängen lag der Wert sogar bei 20 %!

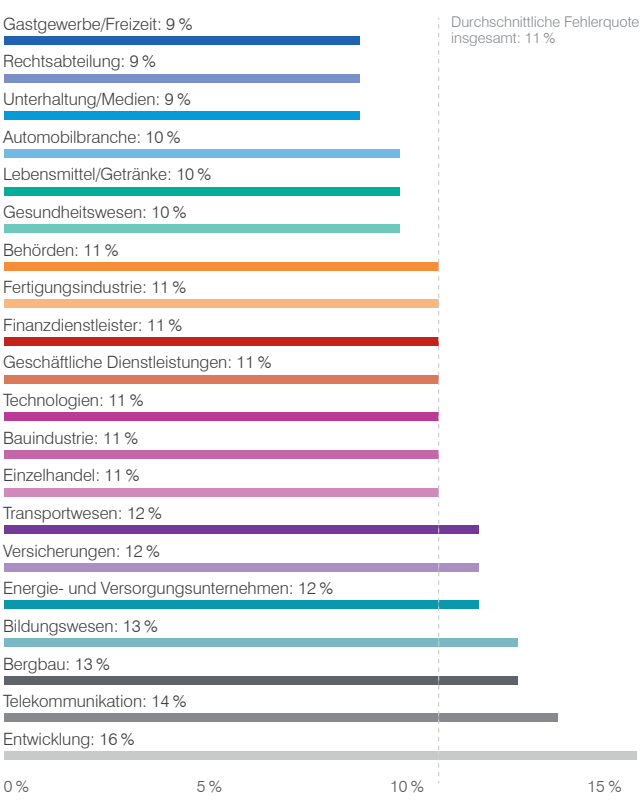
11 %
durchschnittliche Fehlerquote bei Phishing-Tests

Arten der Phishing-Vorlagen: Durchschnittliche Fehlerquoten

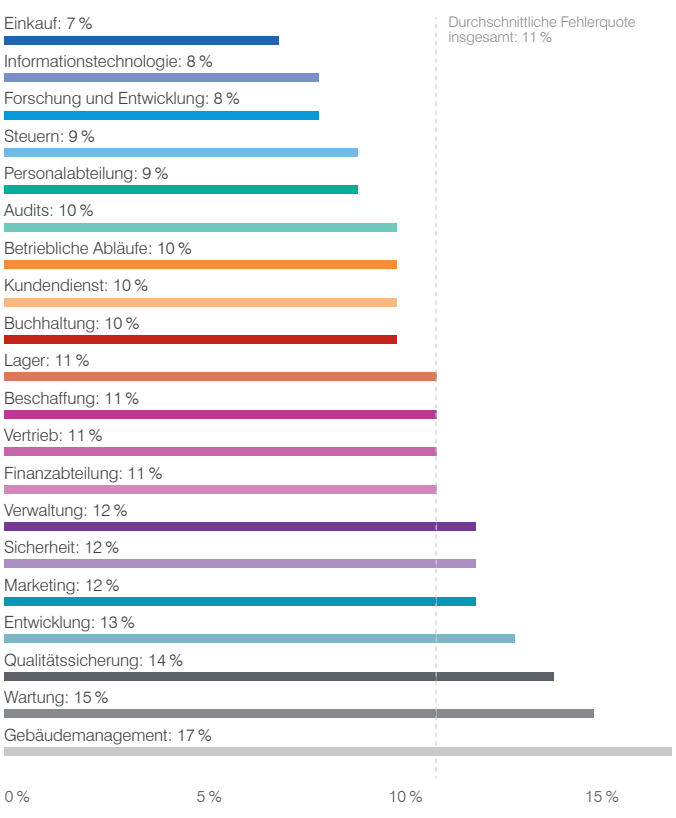


Die Anfälligkeit von Anwendern ist nicht nur je nach Branche unterschiedlich, sondern auch je nach Abteilung.

Durchschnittliche Fehlerquote nach Branche



Durchschnittliche Fehlerquote nach Abteilung



Typische Cybersicherheitsbegriffe mögen zum alltäglichen Sprachgebrauch von IT-Experten gehören, doch für viele Anwender sind sie Fremdwörter.

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

Was ist PHISHING?

Richtig	Falsch	Weiß nicht
63 %	22 %	15 %

US-amerikanische Angestellte schnitten am schlechtesten ab (52 % richtige Antworten)

Britische Angestellte schnitten am besten ab (69 % richtige Antworten)

Was ist RANSOMWARE?

Richtig	Falsch	Weiß nicht
33 %	36 %	31 %

Nur 26 % der deutschen Angestellten lagen richtig

42 % der australischen Angestellten lagen richtig

Was ist MALWARE?

Richtig	Falsch	Weiß nicht
65 %	21 %	14 %

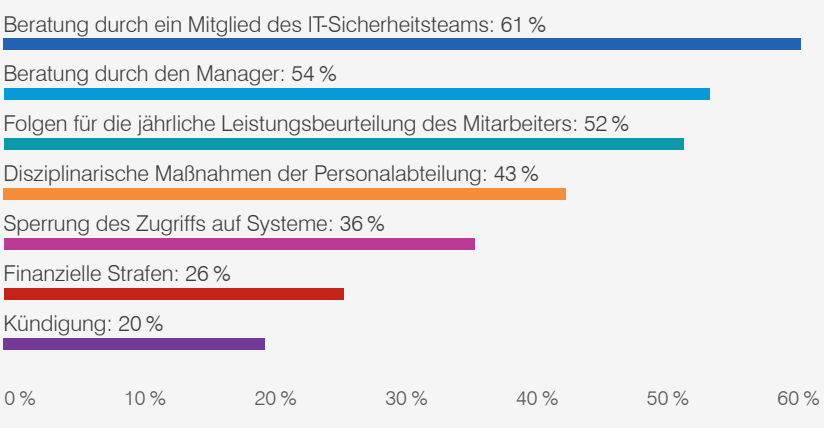
Spanische Angestellte schnitten am besten ab (75 %)

US-amerikanische Angestellte zeigten die schlechteste Leistung (54 %)

REAKTION DER UNTERNEHMEN

Unsere Empfehlung lautet stets, Anwender für unabsichtliche Fehler nicht zu bestrafen. Wir verstehen jedoch, dass manche Firmen ein Konsequenzmodell für „Wiederholungstäter" einführen möchten.

Folgen für Wiederholungstäter



INTERNATIONAL

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

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

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

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

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

VOLLSTÄNDIGEN BERICHT LESEN

Sie möchten mehr erfahren? Der *State of the Phish-Bericht 2021* enthält Daten aus folgenden Quellen:

Eine Drittanbieterumfrage unter **3.500** berufstätigen Erwachsenen in sieben Ländern (Australien, Deutschland, Frankreich, Großbritannien, Japan, Spanien und USA)	Eine Drittanbieterumfrage unter **600** IT-Sicherheitsexperten aus diesen sieben Ländern	Mehr als **60 Mio.** simulierte Phishing-Angriffe, die von unseren Kunden innerhalb von 12 Monaten gesendet wurden	Etwa **15 Mio.** E-Mails, die von Endnutzern unserer Kunden gemeldet wurden

Dieser Bericht bietet einen detaillierten Überblick über aktuelle Phishing-Bedrohungen und empfiehlt Schritte, mit denen Sie eine personenzentrierte Cybersicherheitsstrategie aufbauen können. Damit verbessern Sie das Sicherheitsbewusstsein der Anwender, minimieren Risiken und stärken die Resilienz Ihrer Mitarbeiter.

www.proofpoint.com/de/resources/threat-reports/state-of-phish

proofpoint.