proofpoint.

BERICHT

Europa und Naher Osten

2023 State of the Phish

Sicherheitsbewusstsein und Bedrohungsabwehr im Fokus – eine umfassende Bestandsaufnahme

proofpoint.com/de

EINE IN AUFTRAG GEGEBENE UMFRAGE UNTER:

7.500

berufstätigen Erwachsenen in 15 Ländern

1.050

IT-Sicherheitsexperten aus diesen Ländern

WIR ANALYSIERTEN AUSSERDEM:

135 Millionen

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

18 Millionen

E-Mails, die von Endnutzern unserer Kunden im Zeitraum von 12 Monaten gemeldet wurden

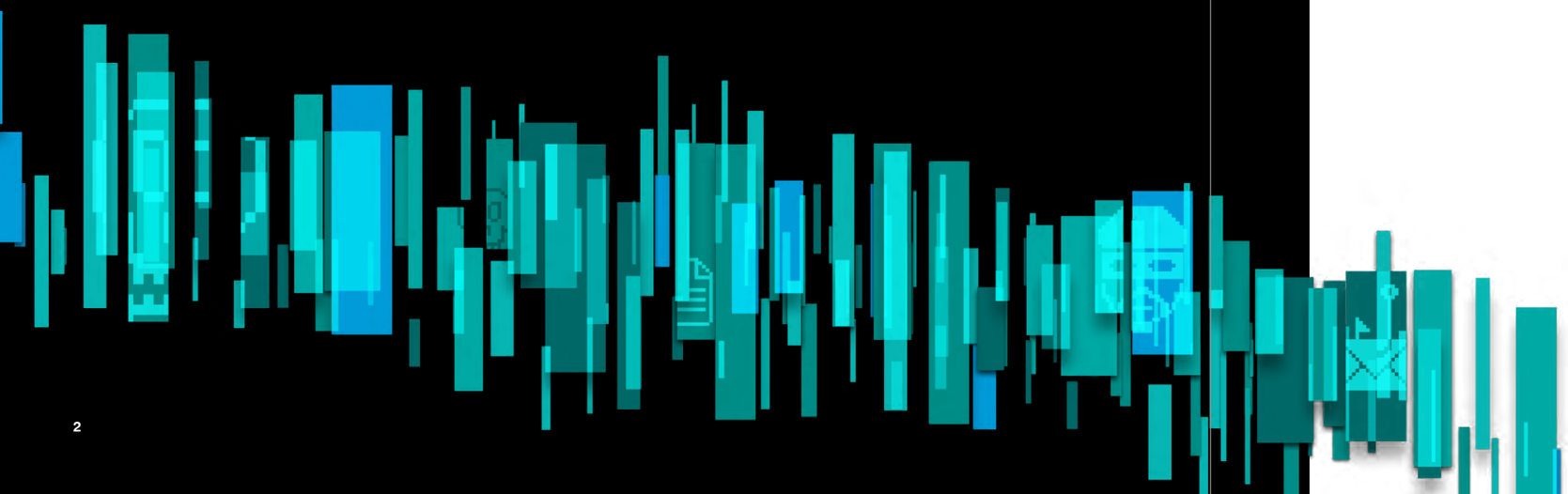
2022: Cyberkriminelle werden noch kreativer

Jedes Jahr versuchen Bedrohungsakteure mit neuen Methoden, ihre Opfer hinters Licht zu führen und Schutzmaßnahmen zu umgehen. Das war im Jahr 2022 nicht anders. Sobald Unternehmen neue Sicherheitskontrollen implementieren, reagieren die Cyberkriminellen umgehend.

Ihr Arsenal umfasst mittlerweile komplexe Techniken wie Angriffe per Telefon (Telephone-Oriented Attack Delivery, TOAD) und Umgehung von Multifaktor-Authentifizierung (MFA). Diese den meisten Anwendern bislang unbekannten Techniken boten den Cyberangreifern einen neuen Vorteil. Und weil Bedrohungsakteure ihre Bemühungen ständig verstärken, haben CISOs und IT-Sicherheitsteams alle Hände voll zu tun.

Unser mittlerweile neunter jährlich erscheinender *State of the Phish*-Bericht untersucht das Sicherheitsbewusstsein von Endnutzern, deren Resilienz und aktuelle Risiken. Der Bericht basiert auf Umfragedaten aus 15 Ländern. Er ermittelt, wie gut Anwender über typische Cyberangriffe und Schutzmaßnahmen Bescheid wissen, und untersucht, wie Wissenslücken und unzureichende Cyberhygiene reale Angriffe ermöglichen. Die meisten Angriffe nehmen eher Menschen als Systeme ins Visier. Aus diesem Grund gibt der letzte Abschnitt dieses Berichts Empfehlungen zu Sicherheitsschulungen und zeigt Möglichkeiten zum Aufbau einer nachhaltigen Sicherheitskultur für alle Unternehmensebenen.

Neben dem diesjährigen Hauptbericht haben wir auch regionale Zusammenfassungen erstellt, die aufzeigen, wie sich lokale Unterschiede auf das Sicherheitsbewusstsein auswirken. Die vorliegende regionale Zusammenfassung umfasst Daten aus **Deutschland, Frankreich, Großbritannien, Italien, den Niederlanden, Spanien, Schweden sowie den Vereinigten Arabischen Emiraten (VAE)**. Die Daten stammen aus Umfragen unter 4.000 berufstätigen Erwachsenen sowie 650 Sicherheitsexperten.

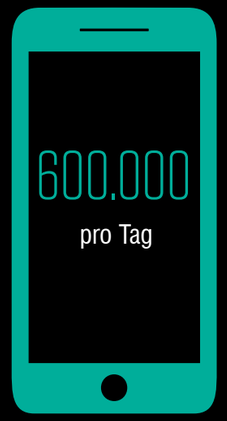


INHALT

Die wichtigsten Erkenntnisse: Weltweit

44 %

der Umfrageteilnehmer glauben, dass eine E-Mail sicher ist, wenn sie eine vertraute Marke zeigt



300.000–400.000 USD

Angriffe per Telefon pro Tag, mit einer Spitze von 600.000 pro Tag im August 2022

33 %

der Befragten führten während eines Angriffs eine riskante Aktion durch (z. B. Klicken auf Links oder Herunterladen von Malware)

76 %

Steigerung bei direkten finanziellen Verlusten durch erfolgreiches Phishing

30 Millionen

schädliche Nachrichten mit Microsoft-Markennamen oder -Produkten wurden 2022 verschickt

>10 %

aller Bedrohungen wurden aufgrund von Anwendermeldungen blockiert

Selbst grundlegende Konzepte werden nicht verstanden.

NUR 35 % der Unternehmen führen Phishing-Simulationen durch

64 % der mit Ransomware infizierten Unternehmen zahlten Lösegeld

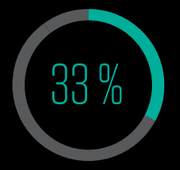
90 % der von Ransomware betroffenen Unternehmen hatten eine Cyberversicherung

65 % der Unternehmen meldeten mindestens einen Fall von Datenverlust durch Insider

NUR 56 % der Unternehmen mit einem Security-Awareness-Programm schulen alle ihre Mitarbeiter

der Sicherheitsexperten betrachten die Sicherheit als höchste Priorität für ihr Unternehmen

aber



der Mitarbeiter erklärten, dass Cybersicherheit für sie auf Arbeit keine Priorität hat

Bei schwedischen Unternehmen lag die Wahrscheinlichkeit eines erfolgreichen Phishing-Angriffs bei

94 %

aber...

Nur 18 %

der schwedischen Unternehmen schulen ihre Mitarbeiter, die als Angriffsziele bekannt sind

Schlaglicht auf Europa und den Nahen Osten

Es gab erhebliche Unterschiede zwischen allen 15 Ländern, die für den *State of the Phish*-Bericht untersucht wurden. Angesichts der unterschiedlichen Sprachen, Kulturen und digitalen Reifegrade ist das kaum überraschend. Auch bei den acht Ländern dieser Zusammenfassung gab es deutliche Unterschiede.

Von allen untersuchten Regionen zeigten Europa, der Nahe Osten und Afrika (EMEA) die größten Unterschiede. Diese Region reicht von der nördlichen bis zur südlichen Hemisphäre, ein riesiger geografischer Raum mit höchst verschiedenen Kulturen, politischen Systemen und Wirtschaftsleistungen. Wie viele Regionen erlebten die EMEA-Länder im Jahr 2022 geopolitische Veränderungen und größere Konflikte. Wenig überraschend zeigte sich das auch in der Cybersicherheitslandschaft.

Mit 94 % war die Wahrscheinlichkeit eines erfolgreichen Phishing-Angriffs im Vergleich zu allen in diesem Bericht untersuchten Ländern in schwedischen Unternehmen am größten. Natürlich können Ausreißerdaten das Ergebnis verschiedener Faktoren sein. Eine potenzielle Erklärung könnte der geringe Anteil von Security-Awareness-Schulungen in diesem Land sein: Nur 18 % der schwedischen Unternehmen schulen ihre Mitarbeiter, die als Angriffsziele bekannt sind – weniger als alle anderen Länder. Eine andere Erklärung können auch die höheren Meldungsraten sein. Schweden zählt seit den 1970er Jahren zu den Pionieren in der Datensicherheit und war eines der ersten europäischen Länder, die Datenschutzgesetze verabschiedet haben. Denkbar ist also, dass das Anerkennen von Sicherheitsverletzungen hier kulturell besser akzeptiert wird, sodass diese auch zuverlässiger gemeldet werden.

In diesem Jahr haben wir zum ersten Mal Italien in den Bericht einbezogen – und die Ergebnisse überraschen. Von allen 15 Ländern haben italienische Unternehmen am seltensten irgendeine Art von Bedrohung verzeichnet. Nur 47 % haben Daten oder geistiges Eigentum aufgrund externer Angriffe verloren (weltweiter Durchschnitt: 69 %). Im Vergleich zu anderen in diesem Bericht genannten Ländern war die Phishing-Erfolgsquote bei italienischen Unternehmen am geringsten (79 %). Diese Zahlen können darauf hinweisen, dass die Vorschriften für Sicherheitsmeldungen unzureichend sind. Ebenso gut ist es aber auch möglich, dass in dieser Kultur Transparenz und offene Informationen nicht im Vordergrund stehen.

Bei der Betrachtung weiterer Cyberangriffskategorien stellten wir fest, dass BEC-Attacken (Business Email Compromise) rapide zunehmen. Dabei verzeichneten die Niederlande und Schweden mit 92 % die höchste Angriffsrate (weltweiter Durchschnitt: 75 %). Den stärksten Anstieg bei Zwischenfällen beobachteten wir in Deutschland und Spanien (16,5 % im Jahresvergleich). Eine wichtige Ursache für die Zunahme von BEC-Attacken könnte in den Entwicklungen bei der verwendeten Sprache liegen: Während BEC-E-Mails bislang in erster Linie auf Englisch verfasst wurden, stellten wir in jüngster Zeit zunehmend E-Mails in deutscher, spanischer, slowenischer oder einer anderen Sprache fest. Das passt auch zur zunehmenden Raffinesse bei den Angriffen, die wir insgesamt beobachten.

Dabei hat die Niederlande die zweifelhafte Ehre, am häufigsten durch Insider (86 %, weltweiter Durchschnitt: 66 %) und externe Akteure (84 %, weltweiter Durchschnitt: 68 %) angegriffen zu werden. Doch anscheinend sind auch die Schulungen wirksam: Niederländische Angestellte geben am seltensten personenbezogene Informationen oder ihre Kennwörter weiter.

VERSTÄNDNIS DER FACHBEGRIFFE:

Sogar grundlegende Konzepte werden immer noch nicht gänzlich verstanden – mehr als ein Drittel kann die Begriffe Malware, Phishing oder Ransomware nicht definieren.

40 %

der Anwender wissen, was Ransomware ist – ein Anstieg um 9 Prozentpunkte gegenüber 2019 und die größte Zunahme unter den von uns abgefragten Begriffen

29 % und 30 %

der Anwender kannten jeweils die relativ neuen Begriffe Smishing und Vishing

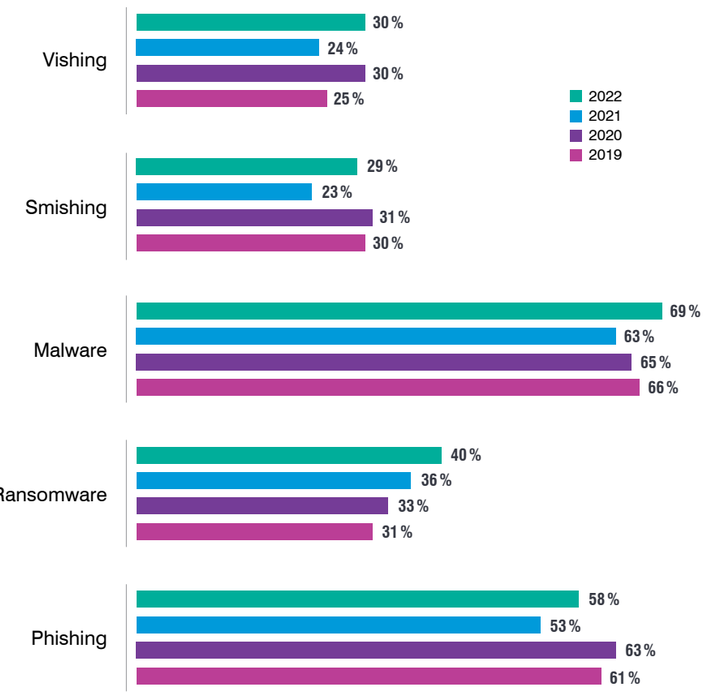
58 %

der Anwender wussten, was Phishing ist – eine Zunahme von 5 Prozentpunkten gegenüber dem letzten Jahr, aber immer noch 3 Prozentpunkte unter 2019

Sicherheitsbewusstsein: Erkenntnisse und Möglichkeiten

Über alle 15 Länder hinweg betrachtet zeigt sich ein ähnliches Muster, wenn wir den Durchschnitt beim Endnutzerwissen über grundlegende Sicherheitsbegriffe ermitteln. Häufige Bedrohungen wie Phishing, Ransomware und Malware sind seit Jahren im Umlauf, doch die Anwender wissen immer noch nicht sicher, was darunter zu verstehen ist. Neuere Bedrohungen wie Smishing (SMS-Phishing) und Vishing (Voice-Phishing) sind noch weniger bekannt. Enttäuschend ist auch, dass unsere Daten nur wenige Veränderungen im Jahresvergleich zeigen.

Wissensstand der Endnutzer zeigt wenige Veränderungen im Jahresvergleich



DAS UNSICHERHEITS-PRINZIP:

69 %

der Anwender in den Niederlanden wissen, was Phishing ist – der höchste Anteil unter den acht untersuchten Ländern dieser Region

45 %

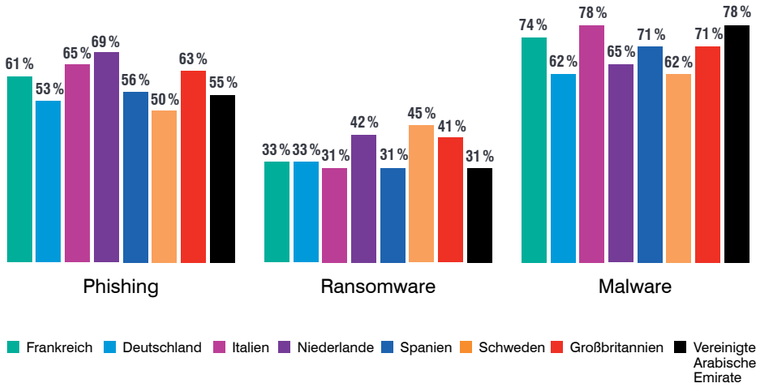
der Schweden kannten das Konzept von Ransomware, was mehr ist als in den anderen sieben Ländern

78 %

der Anwender in Italien und den VAE wussten, was Malware ist – der höchste Anteil unter den acht Ländern dieser Region

Beim Vergleich des Anwenderwissens der drei häufigsten Bedrohungen zeigen sich mehrere interessante Unterschiede. Umfrageteilnehmer in Schweden und Deutschland konnten am seltensten die Begriffe Malware und Phishing definieren. Im Gegensatz dazu konnten die meisten Befragten in den VAE und Italien zwar Ransomware definieren, blieben bei Ransomware jedoch unter dem Durchschnitt.

Wissen über häufige Bedrohungen (Genauigkeit)



Diese Unterschiede können darauf zurückzuführen sein, dass weniger als 50 % der Unternehmen in Europa und dem Nahen Osten ihre Mitarbeiter zu diesen Themen schulen. Der regionale Durchschnitt lag bei 37 % für Phishing, 34 % für Ransomware, 40 % für Malware und 27 % für BEC.

THEMENBEZOGENE SCHULUNGEN:

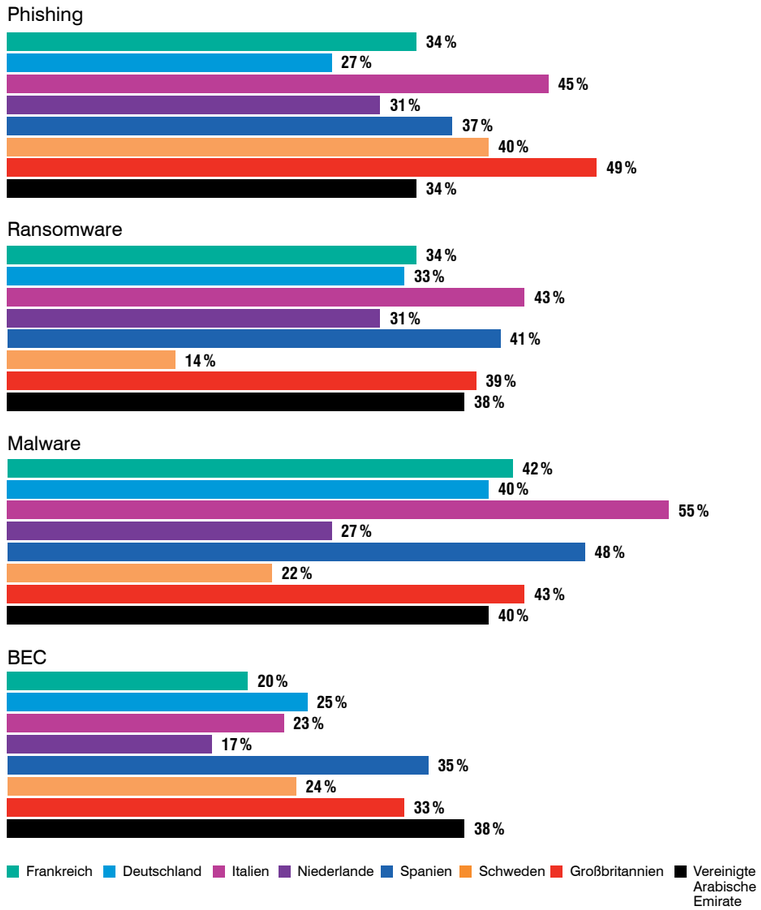
55 %

der italienischen Unternehmen schulen ihre Anwender über Malware – der höchste Anteil unter allen Ländern in dieser Region

14 %

der schwedischen Unternehmen schulen ihre Anwender über Ransomware – der geringste Anteil unter allen Ländern in dieser Region

Bedrohungsthemen in Security-Awareness-Schulungsprogrammen



Obwohl die meisten Unternehmen ein Security-Awareness-Programm implementiert haben, erhalten nicht alle Mitarbeiter diese Schulungen. Dabei stechen Unternehmen aus den VAE besonders heraus: 64 % schulen alle Mitarbeiter, während 52 % sich auf die Mitarbeiter beschränken, die als Angriffsziele bekannt sind. Hinzu kommt, dass 74 % der Unternehmen in den VAE ihre Mitarbeiter zu Sicherheitsthemen schulen, die sie explizit betreffen. Damit nehmen sie den Spitzenplatz unter den 15 Ländern ein.

AWARENESS-SCHULUNGEN FÜR ALLE:

64 %

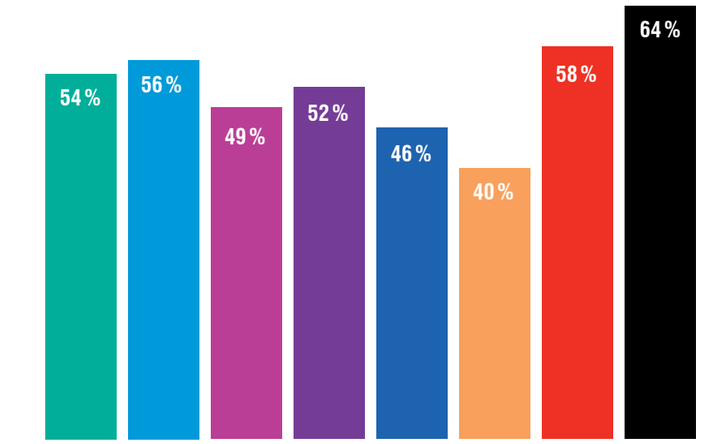
der Arbeitgeber in den VAE schulten alle Mitarbeiter in ihrem Unternehmen – der höchsten Anteil bei den untersuchten Ländern in Europa und dem Nahen Osten

40 %

der schwedischen Unternehmen haben das ebenfalls getan – der geringste Anteil unter den Ländern in dieser Region

CISOs in Großbritannien scheinen gute Arbeit dabei zu leisten, in ihren Unternehmen Sicherheit einen hohen Stellenwert zu geben. Britische Mitarbeiter hatten das größte Vertrauen in ihr IT-Team und gaben auch am häufigsten an, dass ihr Unternehmen Sicherheit einen hohen Stellenwert gibt. Diese Einstellung kann etwas mit den Schulungen zu tun haben – britische Unternehmen liegen gleichauf mit den VAE bei den höchsten Schulungsraten für Mitarbeiter, die als Angriffsziele bekannt sind (52 %).

Anteil der Unternehmen, die bei ihren Security-Awareness-Programmen alle Mitarbeiter



Schulten alle Mitarbeiter im Unternehmen

Frankreich | Deutschland | Italien | Niederlande | Spanien | Schweden | Großbritannien | Vereinigte Arabische Emirate

Mit 48 % waren Phishing-Simulationen in Spanien am beliebtesten (siehe Diagramme auf der nächsten Seite). Großbritannien bietet hingegen zu 45 % Präsenzschulungen an und legt damit großen Wert auf den persönlichen Touch. Innerhalb der Region behandelten britische Unternehmen am häufigsten das Thema Phishing (49 %), führten jedoch erheblich weniger Phishing-Simulationen durch als in Spanien (39 %).

SCHULUNGSFORMEN:

45 %

der britischen Unternehmen boten Präsenzschulungen an – der höchste Wert unter allen untersuchten Ländern in Europa und dem Nahen Osten

50 % und 48 %

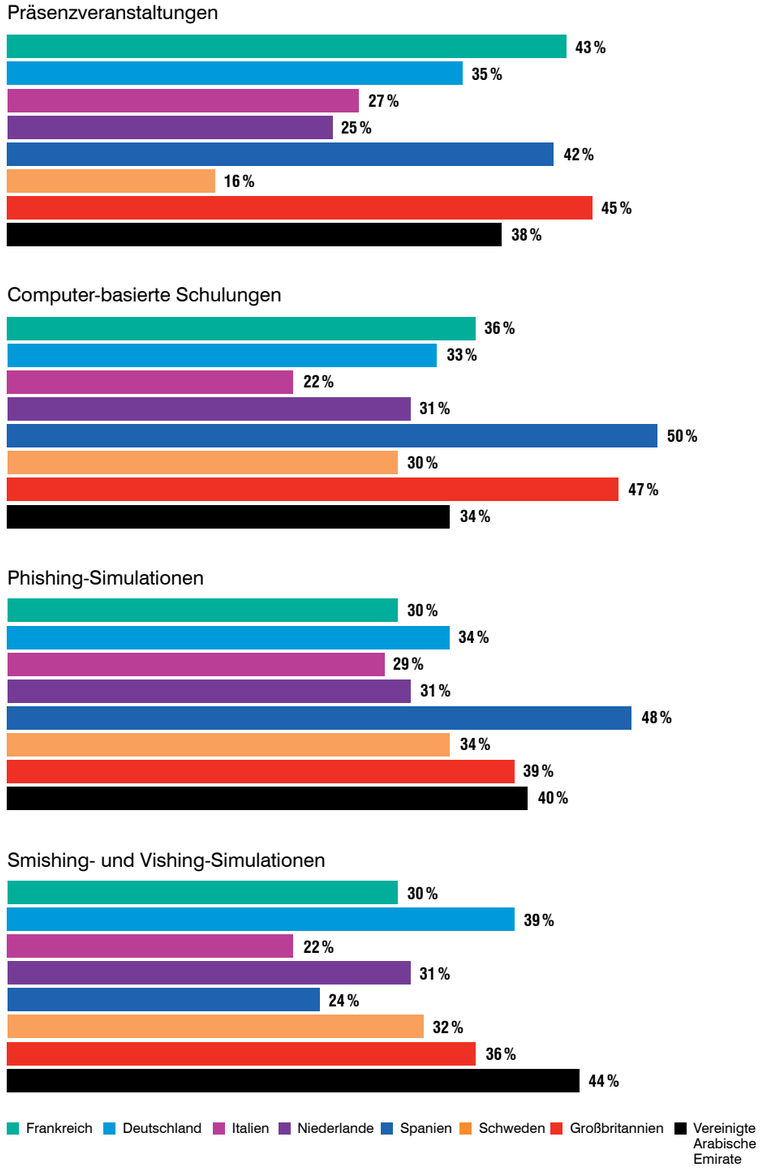
der spanischen Unternehmen boten Computer-basierte Schulungen an bzw. führten Phishing-Simulationen durch, was das Land im Regionalvergleich hervorhob

44 %

der Unternehmen in den VAE führten Smishing- und Vishing-Simulationen durch – der höchste Anteil in dieser Region

Auch die Schulungsdaten für Schweden sind bemerkenswert, da sie darauf hinweisen, dass die Unternehmen der Sicherheit keinen besonders hohen Stellenwert einräumen: Nur wenige Unternehmen führen Präsenzschulungen durch (16 %). Sie schulen auch am seltensten alle Mitarbeiter (40 %). Das überrascht, da Ransomware-Infektionen in Schweden häufiger auftreten als in allen anderen Ländern in diesem Bericht (82 %).

Schulungsmedien



Frankreich | Deutschland | Italien | Niederlande | Spanien | Schweden | Großbritannien | Vereinigte Arabische Emirate

BEDROHUNG VON INNEN:

71 %

der Unternehmen im EMEA-Raum verloren Daten aufgrund von Insider-Bedrohungen

54 %

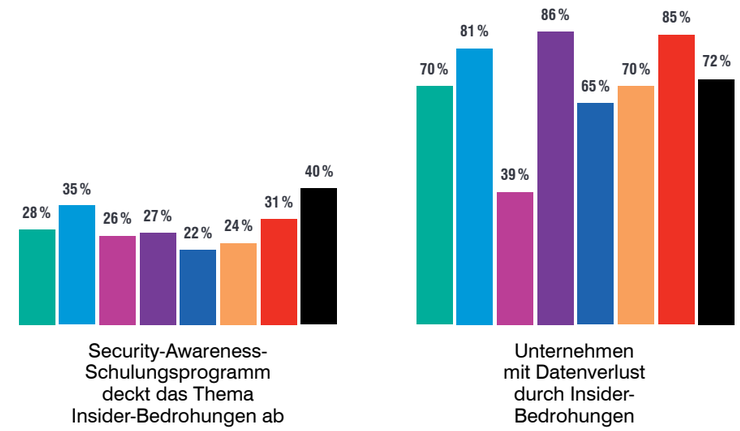
verzeichneten drei oder mehr Angriffe

Sicherheitsbewusstsein: Schlaglicht auf Insider-Bedrohungen

In diesem Jahr erweiterten wir unsere Umfrage, um den wachsenden Einfluss von Insider-Bedrohungen darzustellen – einer Kategorie, die böswilligen Datendiebstahl, fahrlässigen Datenverlust und Anmeldedatendiebstahl umfasst.

In der gesamten Region liegt der Anteil der Unternehmen, die Daten aufgrund von Insider-Bedrohungen verloren haben, bei 71 %. Bemerkenswert ist die Lücke zwischen der großen Zahl der Angriffe und der geringen durchschnittlichen Verbreitung von Security-Awareness-Schulungen (29 %).

Insider-Risiko von Datenverlust



Deutsche Unternehmen verzeichneten am häufigsten Insider-Angriffe (18 %), zudem nehmen mehr Mitarbeiter in Deutschland als in anderen Ländern arbeitsbezogene Informationen mit nach Hause. Ein Grund dafür könnte sein, dass deutsche Mitarbeiter schlichtweg der Meinung sind, dass diese Informationen ihnen gehören würden – zumal nur 35 % der deutschen Unternehmen Schulungen zu Insider-Bedrohungen durchführen. Das Gegenteil ist in den VAE der Fall: Zwar melden dort nur 4 % häufige Insider-Angriffe, doch schulen 40 % ihre Angestellten. Ein Grund dafür könnte sein, dass mit 29 % mehr Mitarbeiter versehentlich personenbezogene Informationen oder Kontokennwörter an nicht vertrauenswürdige Menschen weitergeben als in jedem anderen Land der Region.

ALLE WEGE FÜHREN NACH ROM:

Unternehmen in Italien verzeichneten weniger gezielte Angriffe verschiedener Kategorien als die anderen untersuchten Länder der Region.

79 %

verzeichneten Phishing-Angriffe

51 %

hatten mit BEC-Attacken zu tun

63 %

erlebten Ransomware (nur in den VAE war der Anteil geringer)

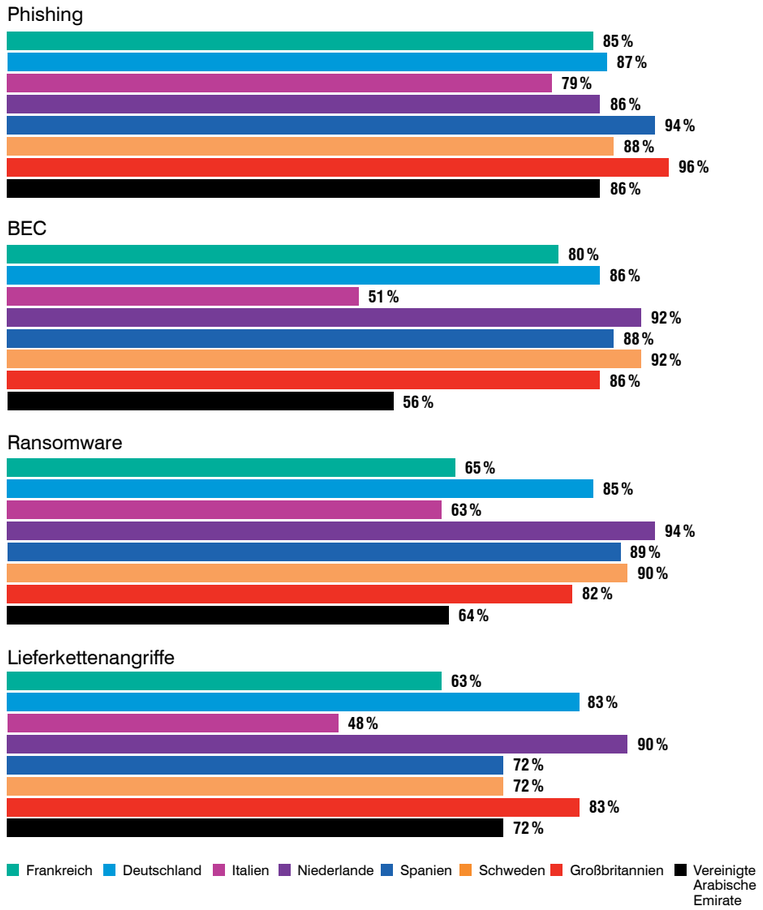
48 %

registrierten Lieferkettenangriffe

Trends in der Bedrohungslandschaft

Insgesamt fiel Frankreich dadurch auf, dass es bei erfolgreichen gezielten Angriffen zuverlässig im Mittelwert für die Region liegt. Wir vermuten, dass das einiges über den Reifegrad der Cybersicherheit in diesem Land aussagt.

Anteil der Unternehmen mit gezielten Angriffen



ZAHLTAG:

27 %

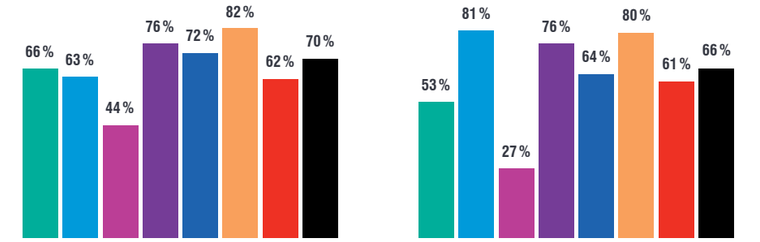
der mit Ransomware infizierten Unternehmen in Italien gingen auf die Lösegeldforderungen der Angreifer ein – der geringste Anteil unter allen Ländern in diesem Bericht. Italienische Unternehmen hatten auch den geringsten Anteil bei Infektionen (44 %) und wurden am seltensten von ihrem Versicherer entschädigt (56 %).

Ransomware: Hilfe durch Versicherungen

Nach der Erst-Kompromittierung kommt es sehr häufig zu einer Ransomware-Attacke. In fünf EMEA-Ländern war die Wahrscheinlichkeit einer Ransomware-Infektion sehr hoch.

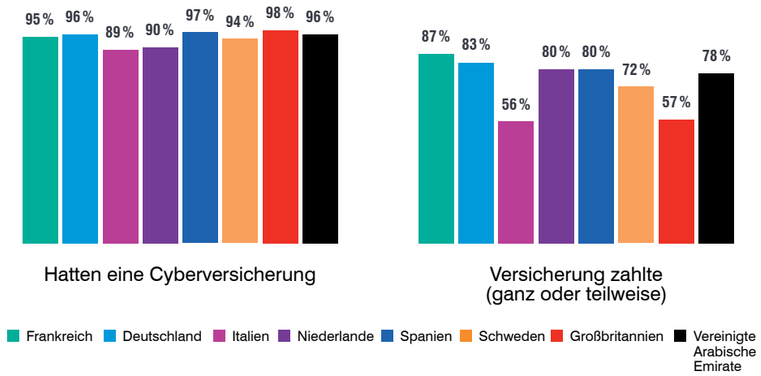
Von allen in diesem Bericht untersuchten Ländern war in Schweden die Wahrscheinlichkeit einer Ransomware-Infektion am größten (82 %). Als eines der weltweit am besten vernetzten Länder gehört Schweden bei der Digitalisierung des öffentlichen Sektors und der Kernindustrien zur Spitzengruppe. Möglicherweise waren viele Unternehmen während der Pandemie weniger stark auf den Schutz vor Cyberbedrohungen konzentriert.

Ransomware-Infektionen und Zahlungen



Während deutsche Unternehmen am häufigsten zahlten (81 %, weltweiter Durchschnitt: 64 %) bildeten Unternehmen in Großbritannien das Schlusslicht aller 15 Länder. Nicht nur, dass sie nach der Zahlung keinen Zugriff auf ihre Daten erlangten (33 % im Vergleich mit 52 %), auch ihre Ansprüche an Cyberversicherungen wurden am häufigsten abgelehnt (23 % im Vergleich mit 7 %).

Ransomware-Infektionen und Zahlungen



Empfehlungen

Angesichts der großen Unterschiede zwischen den Ländern und Unternehmen ist ein individuelles Sicherheitsprogramm ideal, das alltägliche Risiken und Anwenderrisiken berücksichtigt. Wenn Sie noch nicht so weit sind, bietet der diesjährige *State of the Phish*-Bericht einige hilfreiche Ansätze.

Verringern Sie die Komplexität, indem Sie die richtigen Fragen stellen.

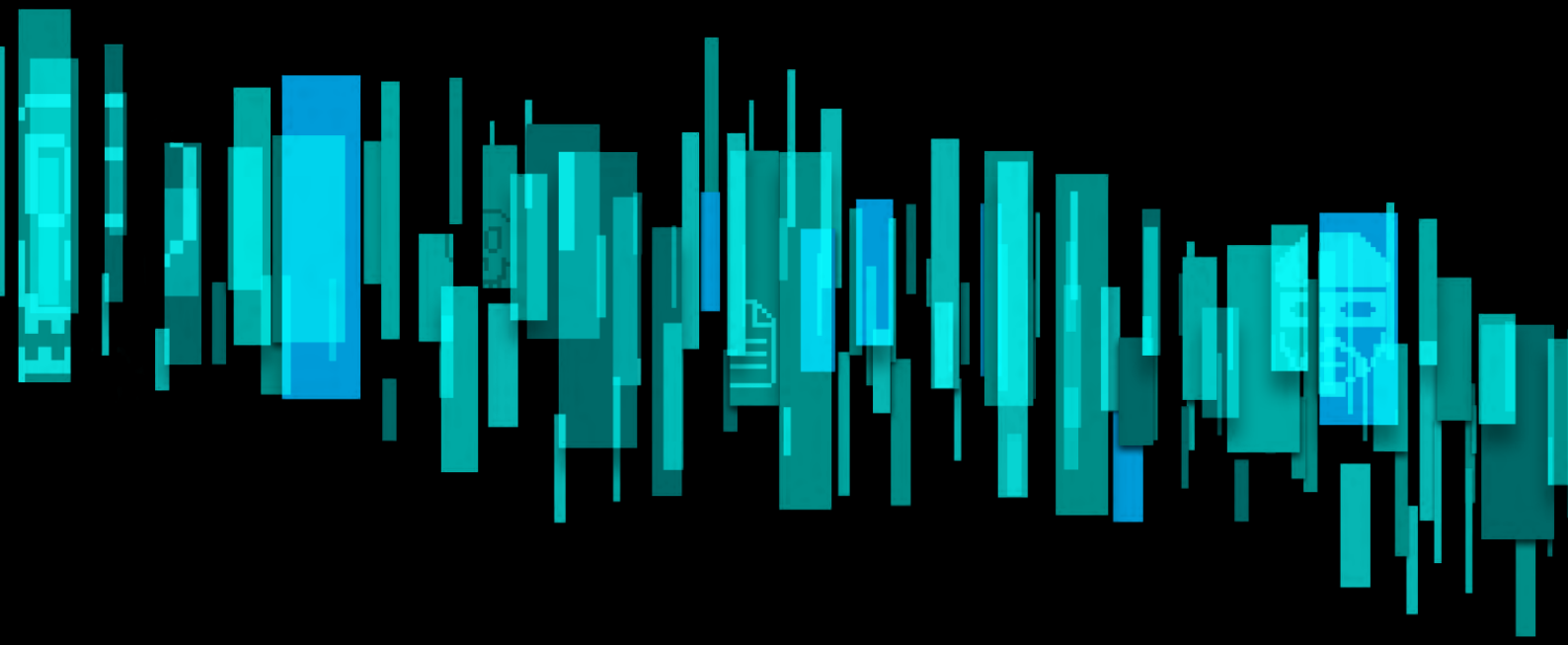
- Wer in meinem Unternehmen wird angegriffen?
- Wo bestehen aktuell Schutzlücken?
- Wo liegen meine Prioritäten zum Minimieren des Anwenderrisikos?

Verbinden Sie Ihre unternehmensweiten Security-Awareness-Schulungen mit aktuellen Bedrohungsdaten.

- Identifizieren Sie die Anwender, die am wahrscheinlichsten angegriffen werden bzw. auf Angriffe hereinfallen.
- Passen Sie die Schulungsinhalte an aktuell im Umlauf befindliche Bedrohungen an.
- Schulen Sie die Anwender in der Erkennung von Phishing-Versuchen mit realen Ködern.

Etablieren Sie eine Sicherheitskultur, die über Schulungen hinausgeht.

- Schulungen sind wichtig, genügen aber nicht.
- Eine starke Sicherheitskultur am Arbeitsplatz hält Anwender dazu an, Informationssicherheit auch im Privatleben ernst zu nehmen.
- Ermitteln Sie wichtige Kennzahlen und reagieren Sie mit angemessenen und fairen Maßnahmen.



WEITERE INFORMATIONEN

Weitere Informationen darüber, wie Sie mit Proofpoint Einblicke in Ihre Anwenderrisiken erhalten und diese mit einer personenzentrierten Cybersicherheitsstrategie minimieren können, finden Sie unter **proofpoint.com/de**.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter 75 Prozent der Fortune-100-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.de**.

proofpoint.

0400-013-04-01