proofpoint.

Europa und Naher Osten

BERICHT

State of the Phish 2024

Riskantes Verhalten, reale Bedrohungen und Anwenderresilienz vor dem Hintergrund personenzentrierter Cybersicherheit

proofpoint.com/de

EINLEITUNG

Die Schlagzeilen zum Thema Cybersicherheit konzentrieren sich häufig auf Vorfälle, bei denen Angreifer besonders clevere Social-Engineering-Taktiken eingesetzt und Zero-Day-Schwachstellen ausgenutzt haben. Cyberkriminelle müssen sich aber nicht immer so viel Mühe geben. Laut der diesjährigen Umfrage zum State of the Phish-Bericht geben 71 % der berufstätigen Erwachsenen zu, dass sie mitunter riskant handeln, z. B. Kennwörter für mehrere Konten nutzen oder weitergeben, auf Links von unbekannten Absendern klicken oder Anmeldedaten auf einer nicht vertrauenswürdigen Seite eingeben. Dabei sind sich 96 % dieser Erwachsenen bewusst, dass sie damit ein Risiko eingehen. Der Faktor Mensch ist ein wichtiges Element jeder guten Abwehrstrategie – kann jedoch auch das schwächste Glied sein. Anwender können Fehler machen, auf Betrugsversuche hereinfallen oder einfach bewährte Sicherheitsmethoden ignorieren.

Der diesjährige weltweite Bericht basiert auf einer Umfrage unter 7.500 Endnutzern und 1.050 Sicherheitsexperten aus 15 Ländern, einschließlich acht Ländern in Europa und im Nahen Osten. Zudem haben wir Daten aus Proofpoint-Produkten sowie Bedrohungsforschungsergebnisse ausgewertet. Außerdem wurden Erkenntnisse aus 183 Millionen simulierten Phishing-Nachrichten analysiert, die innerhalb von 12 Monaten von unseren Kunden gesendet wurden, sowie mehr als 24 Millionen E-Mails, die von deren Endnutzern gemeldet wurden. Und zum zweiten Mal in Folge haben wir auch regionale Zusammenfassungen erstellt, die lokale Besonderheiten und Abweichungen aufzeigen.

Die meisten Anwender in Europa und im Nahen Osten wissen nicht genau, ob die Verantwortung für Sicherheit bei ihnen oder bei anderen Personen liegt. Diese fehlende Klarheit kann schwerwiegende Folgen haben. Unsere Daten zeigen in der gesamten Region eine starke Korrelation zwischen den Einstellungen der Anwender und den Ergebnissen.

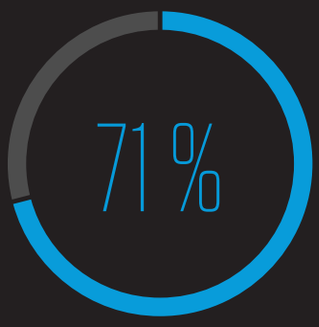
Jeden Tag entscheiden Anwender in der Region zwischen Sicherheit und Bequemlichkeit. In dieser regionalen Zusammenfassung zeigen wir, dass sie sich meist für Letzteres entscheiden. Auf den nächsten Seiten sehen wir uns die Einstellungen von Sicherheitsexperten und Endnutzern sowie einige wichtige Bedrohungstrends genauer an. Abschließend geben wir Ihnen Empfehlungen, mit welchen Maßnahmen Sie erreichen, dass Ihre Anwender ihr Verhalten ändern und Sicherheit an die erste Stelle rücken.

INHALT

Die wichtigsten Erkenntnisse: Weltweit

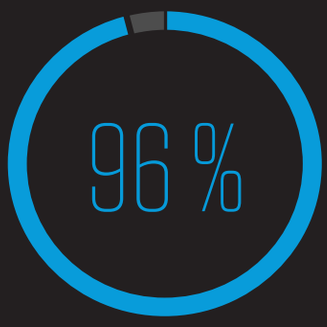
>1 Mio.

Angriffe mit EvilProxy, dem Framework zur MFA-Umgehung, werden jeden Monat verzeichnet, doch 89 % der Sicherheitsexperten glauben immer noch, dass MFA vollständigen Schutz vor Kontoübernahmen bietet.



führten eine riskante Aktion durch

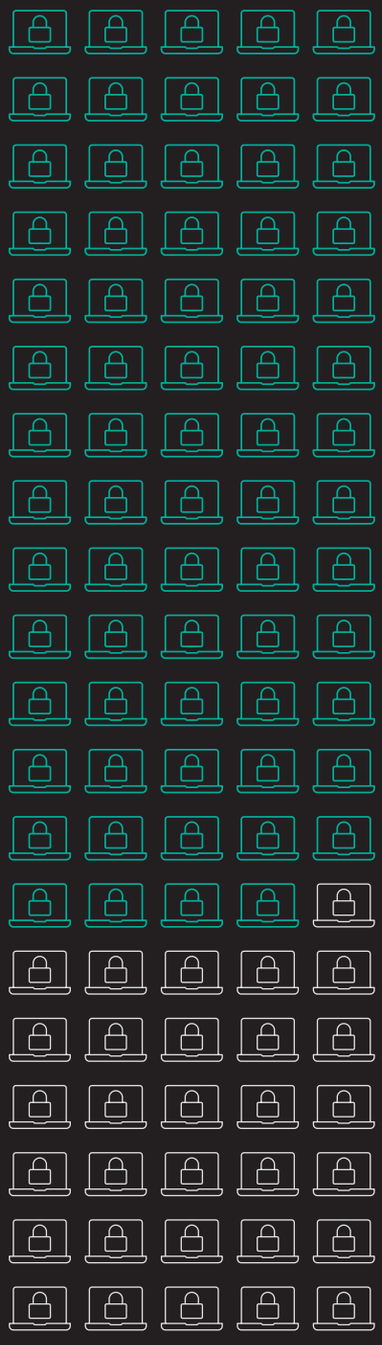
und



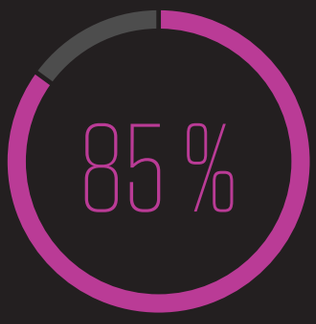
von ihnen waren sich bewusst, dass dies riskant ist.

66 Millionen

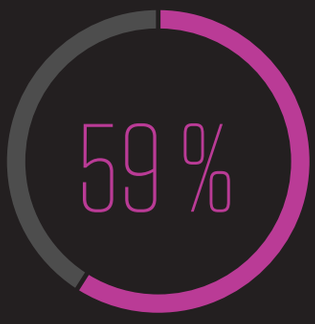
BEC-Angriffe wurden im Durchschnitt pro Monat von Proofpoint erkannt und blockiert.



69 % der Unternehmen wurden mit Ransomware infiziert.



der Sicherheitsexperten waren der Meinung, dass die Arbeitnehmer sich ihrer Verantwortung für die Sicherheit bewusst sind, aber



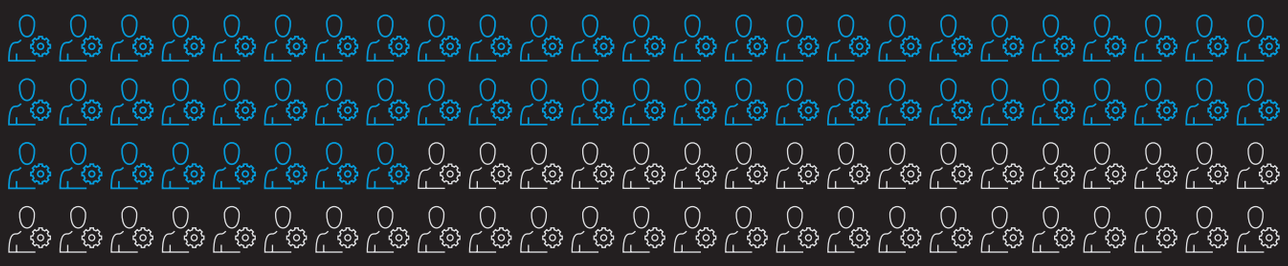
der Anwender waren sich nicht sicher oder gaben an, dass sie die Verantwortung für die Sicherheit nicht bei ihnen liegt.

10 Millionen

TOAD-Nachrichten werden pro Monat verschickt.

68 Millionen

Microsoft ist weiterhin die am häufigsten missbrauchte Marke, d. h. es werden schädliche Nachrichten versendet, die diese Marke oder deren Produkte verwenden.



58 % der Anwender, die riskantes Verhalten gezeigt haben, sind durch ihr Verhalten für gängige Social-Engineering-Taktiken anfällig geworden.

Schlaglicht auf Europa und den Nahen Osten

Für den diesjährigen State of the Phish-Bericht wurden 7.500 Endnutzer und 1.050 Sicherheitsexperten aus 15 Ländern befragt. Diese Zusammenfassung konzentriert sich auf folgende Länder:

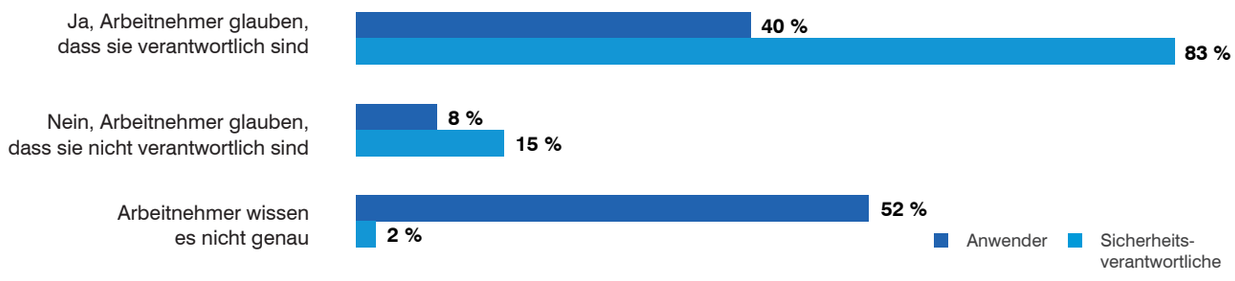
- Frankreich
- Deutschland
- Italien
- Niederlande
- Spanien
- Schweden
- Großbritannien
- Vereinigte Arabische Emirate

Angesichts der unterschiedlichen Sprachen, Kulturen und digitalen Reifegrade stellten wir erhebliche Unterschiede zwischen den Regionen und auch zwischen den acht Ländern fest, auf die sich diese Zusammenfassung konzentriert. Die Region ist in Bezug auf die geografische Lage, die Kulturen und die wirtschaftliche Situation sehr vielseitig, doch in mindestens einer Hinsicht recht homogen: In dieser Region war der Anteil der Anwender, die riskantes Verhalten gezeigt haben, größer als der weltweite Durchschnitt (76 % verglichen mit 71 %). Dabei wich der Anteil der Anwender, die sich bei einer riskanten Aktion des Risikos bewusst waren, nur 1 Prozentpunkt vom weltweiten Durchschnitt ab (95 %).

Nach Ländern betrachtet, sagten 86 % der Umfrageteilnehmer aus den Vereinigten Arabischen Emiraten, dass sie eine riskante Aktion durchgeführt haben. Das war der höchste landesspezifische Wert in unserer Umfrage. Bei Unternehmen in den Vereinigten Arabischen Emiraten werden am häufigsten erfolgreiche Spearphishing-Angriffe verzeichnet. Dies weist auf einen starken Zusammenhang zwischen dem Bewusstsein der Anwender und der Sicherheit von Unternehmen hin. Interessanterweise gab es in diesem Land dennoch die höchste Zahl an Anwendern, die der Meinung sind, dass sie die Verantwortung für Sicherheit tragen (62 % verglichen mit dem weltweiten Durchschnitt von 41 %).

Anwender aus Schweden sagten am seltensten, dass sie für Sicherheit verantwortlich sind. Dies passt zum überdurchschnittlichen Anteil der Anwender, die in Schweden riskantes Verhalten zeigten (82 %).

Verantwortung für Sicherheit (Europa und Naher Osten)

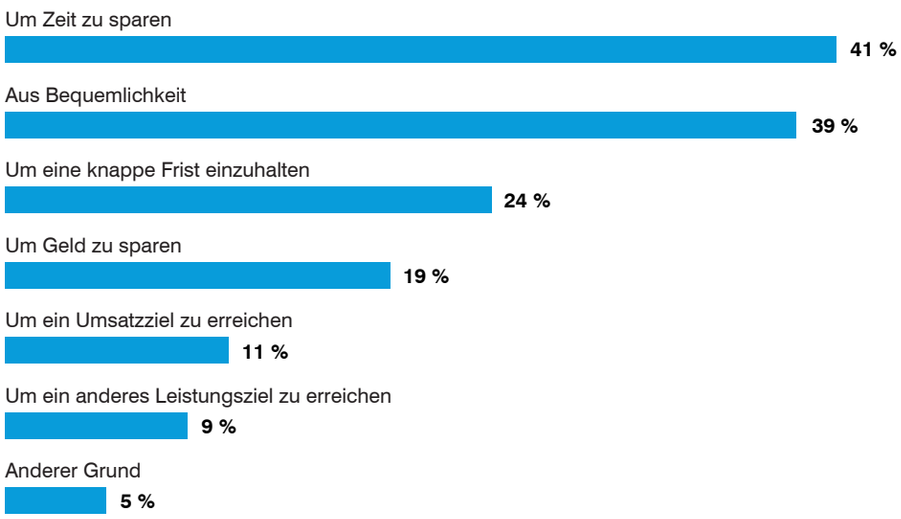


Sicherheitsexperten in der Region stuften mehrfache Kennwortnutzung als riskantestes Verhalten ein. Leider sind die Weitergabe von Kennwörtern und die mehrfache Kennwortnutzung das zweithäufigste riskante Verhalten bei Endnutzern. Doch es gibt auch gute Nachrichten für Sicherheitsteams: Der Zugriff auf unangemessene Websites war die einzige andere von ihnen genannte Aktion, die auch unter den Top 5 der häufigsten riskanten Verhaltensweisen von Anwendern auftauchte.

Rang	Riskantes Verhalten (Ranking laut Sicherheitsexperten)	Riskantes Verhalten (Von Endnutzern gezeigt)
1	Mehrfache Verwendung oder Weitergabe von Kennwörtern	Verwendung unternehmenseigener Geräte für private Aktivitäten
2	Klicken auf Links oder Herunterladen von Anhängen von unbekannten Absendern	Mehrfache Verwendung oder Weitergabe von Kennwörtern
3	Hochladen vertraulicher Daten in externe Cloud	Herstellung einer Verbindung ohne VPN an einem öffentlichen Ort
4	Eingabe von Anmeldedaten auf einer nicht vertrauenswürdigen Seite	Antworten auf eine Nachricht (E-Mail oder Textnachricht) von einem unbekannten Absender
5	Zugriff auf unangemessene Websites	Zugriff auf unangemessene Websites

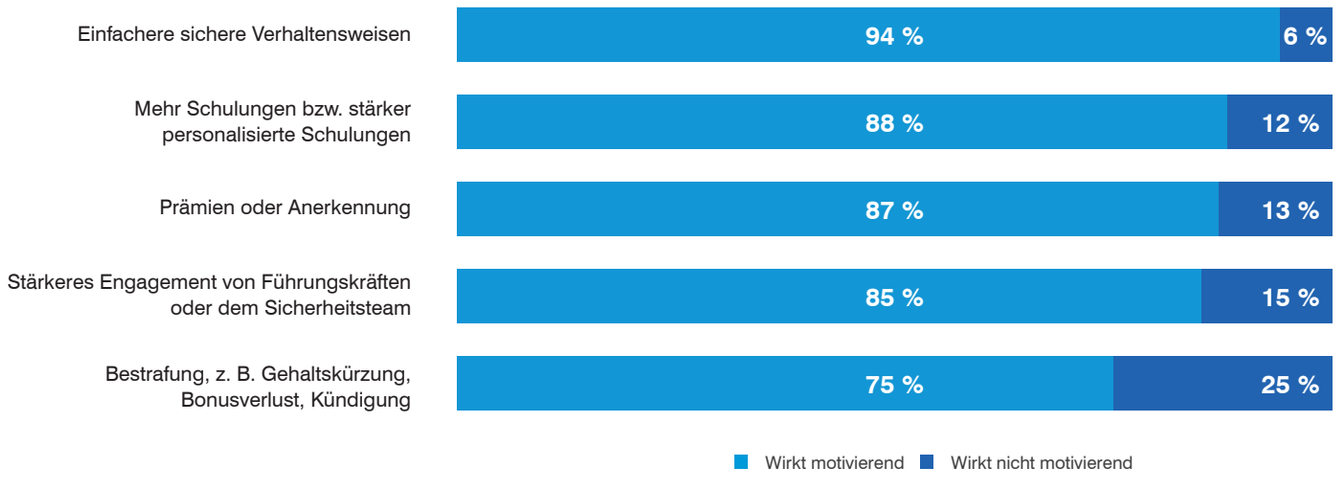
Doch warum handeln Anwender riskant? Die häufigste Antwort auf diese Frage lautete Zeitersparnis, dicht gefolgt von Bequemlichkeit. In Großbritannien war die Reihenfolge umgekehrt, d. h. britische Umfrageteilnehmer nannten häufiger als alle anderen Bequemlichkeit als Grund.

Warum handeln Anwender riskant?



Anwender in Europa und im Nahen Osten sind sich bewusst, warum sie riskant handeln. Doch was würde sie motivieren, Sicherheit zu priorisieren? Ebenso wie bei unseren weltweiten Ergebnissen antworteten die meisten, dass einfachere sichere Verhaltensweisen am stärksten motivieren – und Bestrafung am wenigsten.

Wie wird Sicherheit zur Priorität für Endnutzer?



78 %

der deutschen Unternehmen verzeichneten TOAD-Angriffe, doch nur

21 %

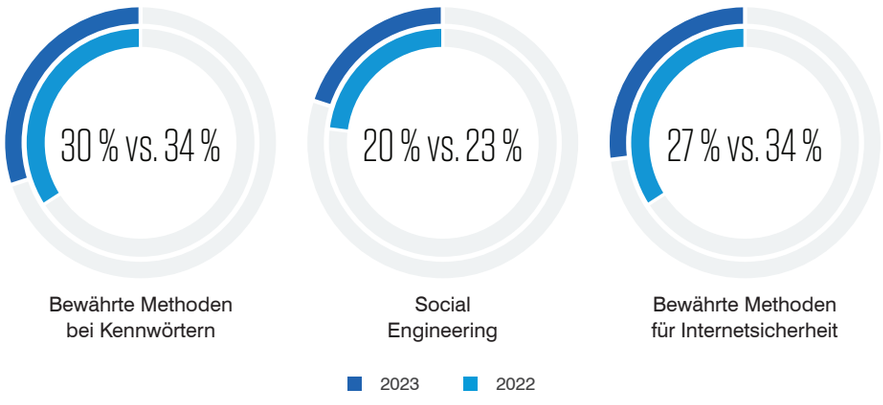
thematisieren sie bei Schulungen.

Verbesserungsmöglichkeiten

95 % der Unternehmen in Europa und im Nahen Osten nutzen bereits Bedrohungsdaten, um ihre Security-Awareness-Schulungsprogramme zu optimieren. Es gibt jedoch noch erhebliche Lücken. Obwohl die meisten Unternehmen angaben, dass sie per Telefon (TOADs) angegriffen werden, berücksichtigt weniger als ein Drittel diese Taktik bei Schulungen. In Deutschland verzeichneten 78 % der Unternehmen TOAD-Angriffe, doch nur 21 % thematisierten sie bei Schulungen. Das ist eine der größten Differenzen zwischen täglichen Angriffen und Schulungsthemen.

Insgesamt wendeten die Unternehmen in dieser Region mehr Zeit für Security-Awareness-Schulungen auf. In Spanien war der Anstieg am größten. Hier nahm die Zahl der Unternehmen, die ihre Mitarbeiter mindestens drei Stunden pro Jahr schulen, um 120 % zu.

Allerdings scheinen immer weniger Unternehmen zu grundlegenden Themen zu schulen:



Diese drei Sicherheitsthemen sind unverzichtbare Grundlagen. Wenn weniger Anwender wissen, wie sie sichere Kennwörter festlegen, häufige Köder vermeiden und sich sicher im Internet bewegen, werden Cyberkriminelle dies zweifellos ausnutzen.

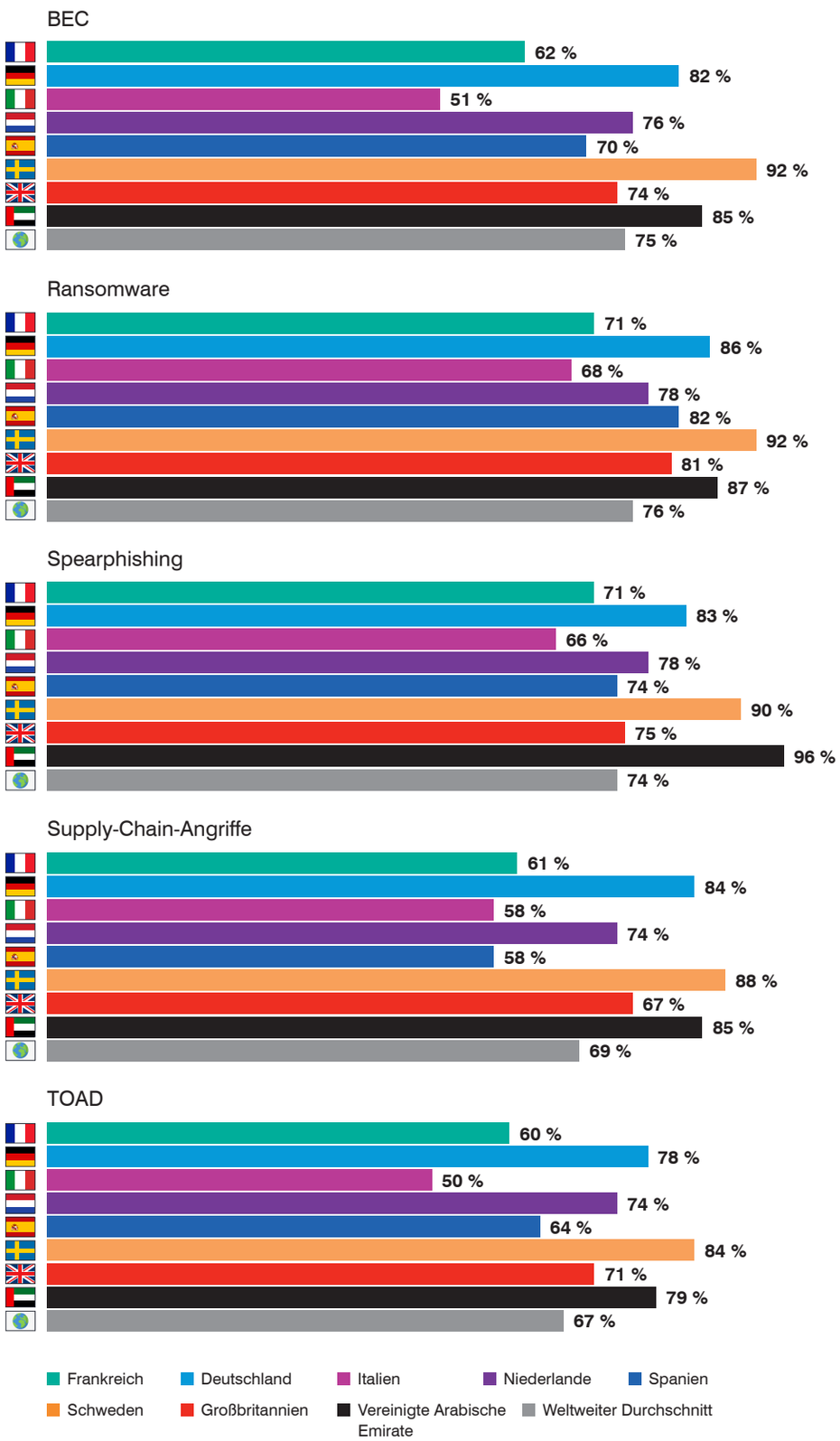
Die Bedrohungslandschaft in Europa und im Nahen Osten

Die regionale Bedrohungslandschaft folgte im letzten Jahr im großen und ganzen den weltweiten Trends. Business Email Compromise (BEC) ging insgesamt zurück, doch in nicht englischsprachigen Ländern ging die Zahl nach oben. Dies könnte eine Folge der zunehmenden Nutzung von KI-Tools wie ChatGPT sein, mit denen sich in mehreren Sprachen überzeugende E-Mail-Köder verfassen lassen. Ähnliche Trends wurden weltweit in anderen nicht englischsprachigen Ländern festgestellt. Insgesamt verzeichneten 75 % aller Unternehmen mindestens einen erfolgreichen Phishing-Angriff, während es 2022 noch 88 % waren.

In Europa und im Nahen Osten gab es etwas mehr TOAD-Angriffe – 70 % verglichen mit dem weltweiten Durchschnitt von 67 %. 84 % der schwedischen Unternehmen verzeichneten einen TOAD-Angriff, der höchste Wert in dieser Region.

Ebenso wie bei unseren weltweiten Zahlen wurde in Europa und im Nahen Osten eine Zunahme der negativen Auswirkungen erfolgreicher Angriffe gemeldet. Die Geldstrafen stiegen um 122 % und damit etwas weniger als im weltweiten Durchschnitt. Das kann daran liegen, dass in den vorherigen Jahren bereits Strafen entsprechend der DSGVO verhängt wurden.

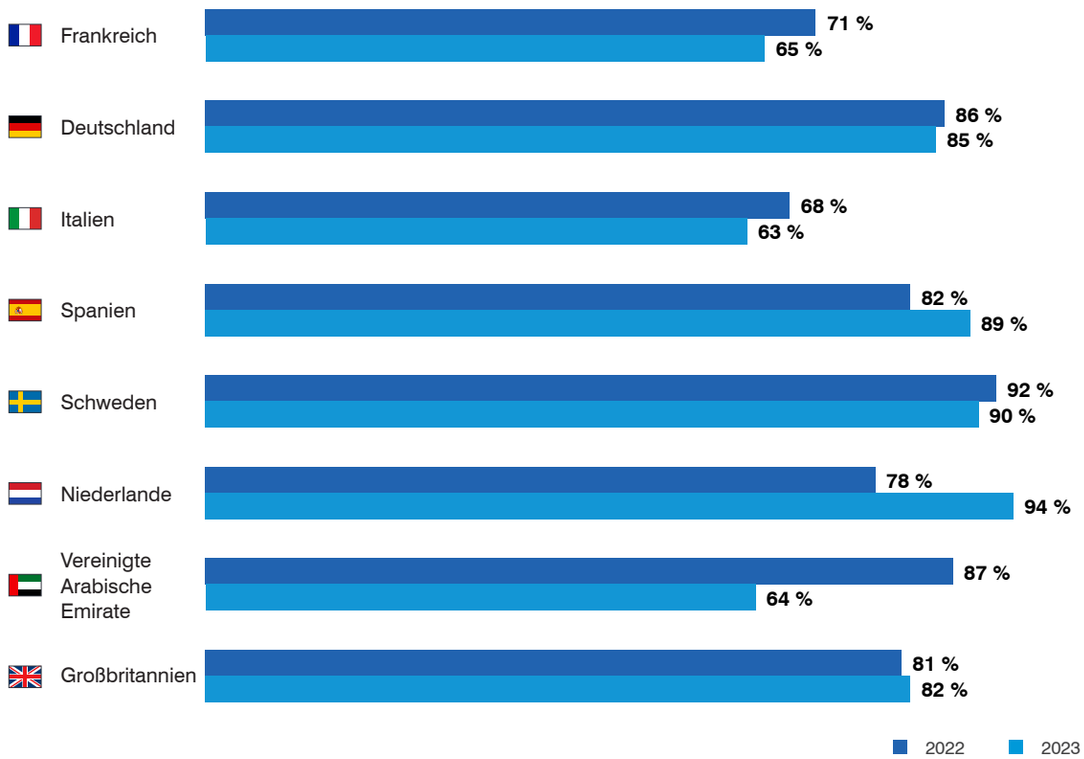
Anteil der Unternehmen mit gezielten Angriffen



Ransomware

Ransomware stellt in Europa und im Nahen Osten weiterhin eine schwerwiegende Bedrohung dar. Sowohl die Zahl der Angriffe und als auch die der Infektionen ist im vergangenen Jahr gestiegen. Es gibt jedoch Unterschiede zwischen den Ländern.

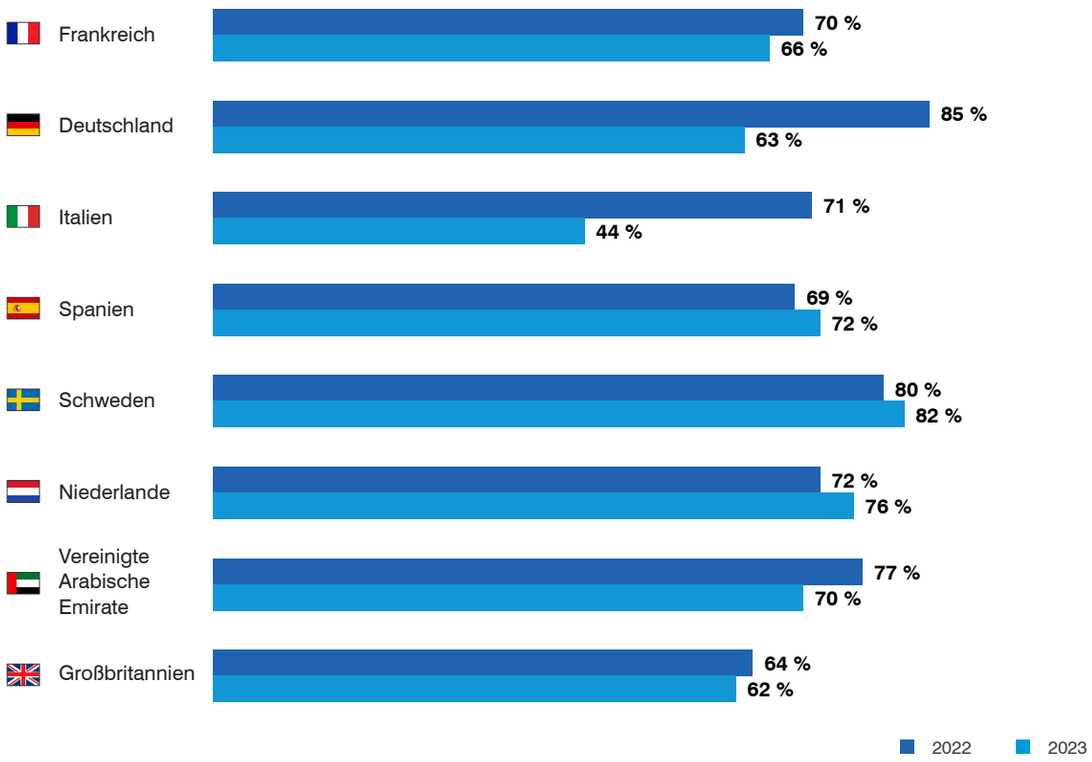
Trends bei E-Mail-basierten Ransomware-Angriffen



Zum Beispiel ist die Zahl der erfolgreichen Ransomware-Angriffe in Italien von 44 % im Jahr 2022 auf 71 % im Jahr 2023 stark gestiegen – wobei die Zahl der Angriffe selbst mit anderen Ländern vergleichbar war. Die starke Zunahme veranlasste die italienischen Behörden im Juni, eine Warnung vor Ransomware-Angriffen über einen VMware-Fehler herauszugeben.

Schwedische Unternehmen verzeichneten weltweit am häufigsten Ransomware-Angriffsversuche – hier wurden 92 % der Unternehmen attackiert. Dies kann damit zusammenhängen, dass bei einer früheren Umfrage 74 % der schwedischen Umfrageteilnehmer Anmeldedatendiebstahl als häufigste Ursache für Datenschutzverletzungen nannten. Wenn Maßnahmen zum Schutz vor solchen Angriffen Priorität eingeräumt wird, kann die Wahrscheinlichkeit nachfolgender Aktivitäten, wie zum Beispiel Ransomware, reduziert werden.

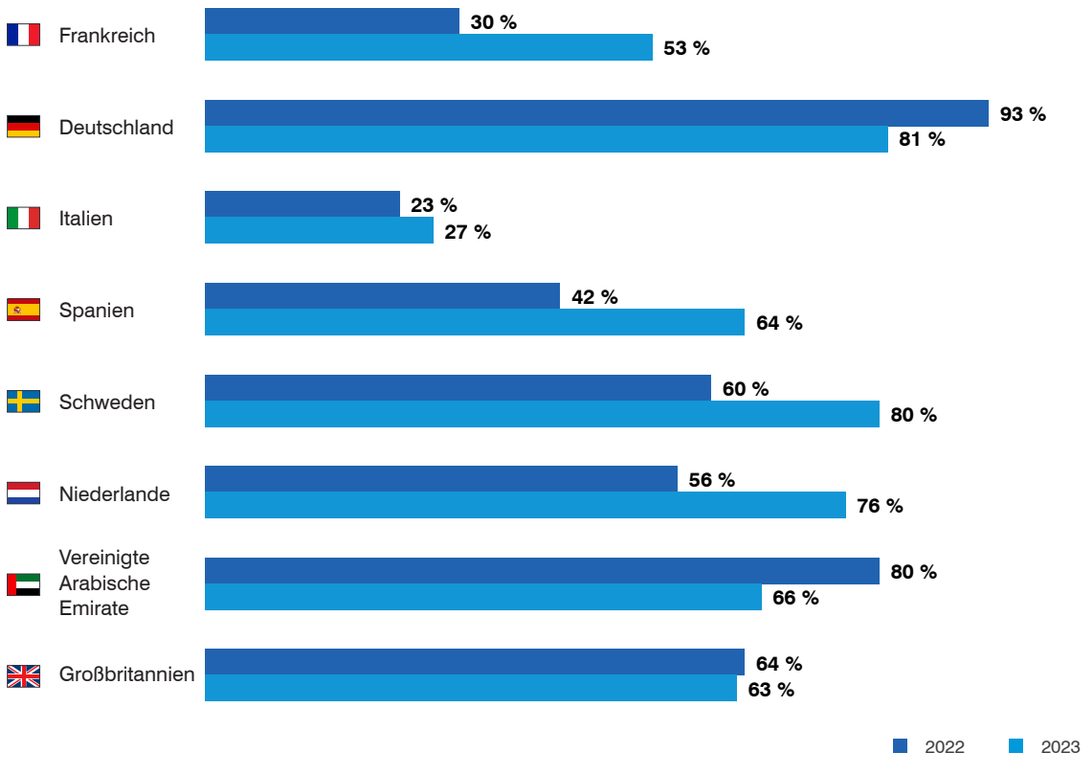
Trend bei Ransomware-Infektionen



Andererseits zeigten nur drei Länder – Deutschland, die Vereinigten Arabischen Emirate und Großbritannien – eine größere Bereitschaft, auf Lösegeldforderungen einzugehen. In Deutschland war auch der Anteil der Unternehmen, die ein Lösegeld gezahlt haben, am höchsten (93 % verglichen mit dem weltweiten Durchschnitt von 54 %).

Diese Strategie scheint in Deutschland und in den Vereinigten Arabischen Emiraten aufzugehen, da hier deutlich mehr Unternehmen berichteten, dass sie nach einer einzigen Zahlung ihre Systeme und Daten wiederherstellen konnten. Der Nachteil: 85 % der deutschen Unternehmen verzeichneten eine erfolgreiche Ransomware-Infektion – der höchste Wert in dieser Region. Das deutet darauf hin, dass es möglicherweise einen Zusammenhang zwischen der Zahlungsbereitschaft und der Angriffsintensität gibt.

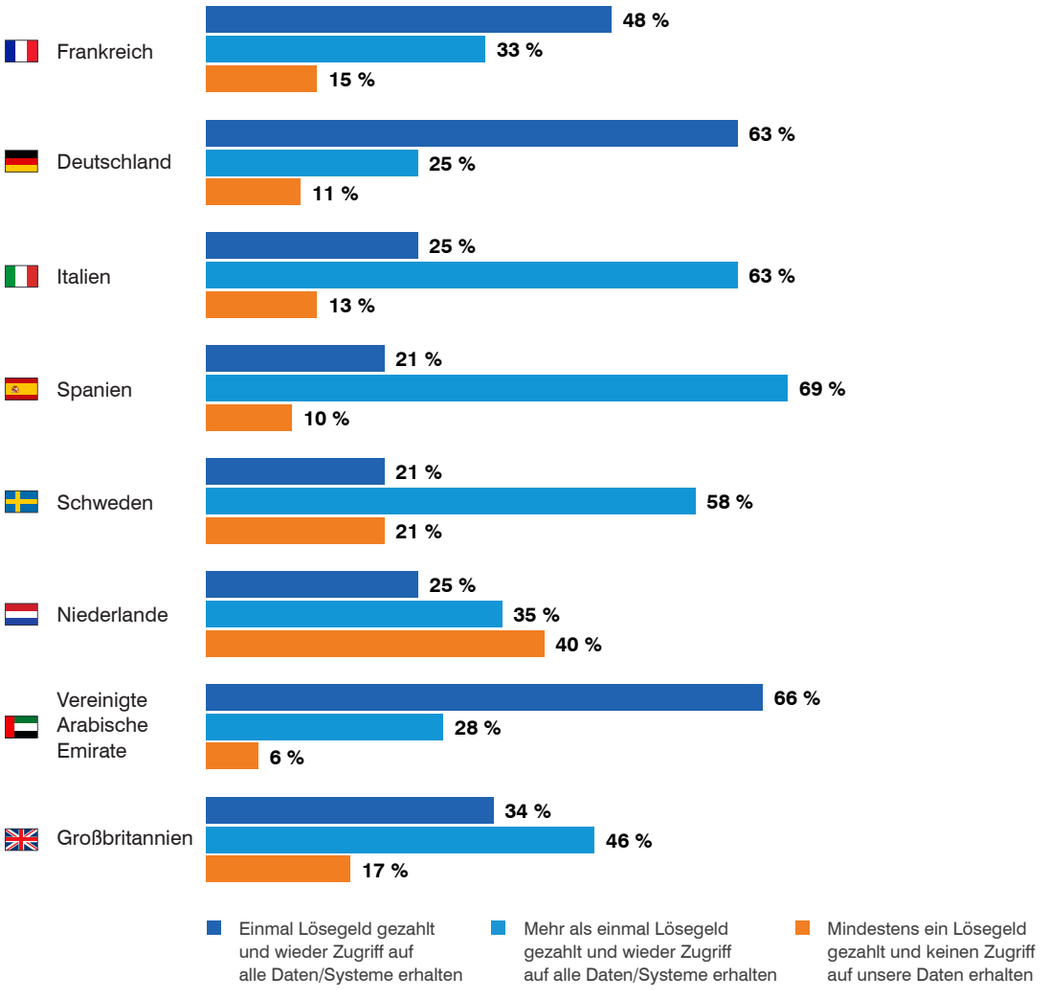
Anteil der Unternehmen, die Lösegeld gezahlt haben



Britische Unternehmen schnitten dagegen nicht so gut ab. Sie verzeichneten die höchste Anzahl wiederholter Infektionen, d. h. 14 % berichteten von mindestens 10 Infektionen, verglichen mit einem weltweiten Durchschnitt von 5 %. Dies zeigt, dass die Zahlung des Lösegelds keine Immunität gegen zukünftige Angriffe bietet. Im Gegenteil kann dies sogar zu weiteren Angriffen motivieren.

Bei niederländischen Unternehmen wurde am seltensten ein positives Ergebnis erreicht: Während weltweit betrachtet nur 16 % nicht wieder Zugriff auf die eigenen Daten erlangen konnten, galt dies in den Niederlanden für 40 % der Unternehmen. Dies deutet darauf hin, dass einige Ransomware-Gruppen ihre Versprechen nicht einhalten oder nicht immer in der Lage sind, die Daten wiederherzustellen.

Ergebnis der Lösegeldzahlung



Positiv zu bewerten ist, dass die Leistungen von Cyberversicherungen sich verbessert haben, sodass sie eine gewisse finanzielle Entlastung darstellen. Die einzige Ausnahme hierbei ist Frankreich, wo der Anteil der vollständig oder teilweise versicherten Unternehmen von 87 % im Jahr 2022 auf 76 % im Jahr 2023 gesunken ist. Dies liegt wahrscheinlich daran, dass der größte französische Versicherer angekündigt hat, Ransomware-Angriffe zukünftig vom Versicherungsschutz auszunehmen.

Empfehlungen

Unsere Umfrage hat gezeigt, dass Anwender in Europa und im Nahen Osten sich bewusst sind, dass ihr Verhalten zu Risiken führen kann. Häufig motiviert sie dieses Wissen jedoch nicht, Sicherheit zu priorisieren, sei es aus Bequemlichkeit, weil sie Zeit sparen wollen oder weil sie einfach nicht wissen, dass die Verantwortung für IT-Sicherheit bei ihnen liegt.

Wenn Ihre Anwender bereits verstehen, dass sie die Verantwortung für Sicherheit tragen:

- Stellen Sie Tools zur Verfügung, die Ihre Anwender dabei unterstützen, proaktiv zu werden. Dazu gehören zum Beispiel Schaltflächen, über die verdächtige E-Mails gemeldet werden können, und Warnhinweise in E-Mails, die zum Handeln auffordern. Erwägen Sie auch die Einrichtung eines Netzwerks aus Fürsprechern sowie ein Prämiensystem, um diese Anwender zu motivieren, als Vorbild für richtiges Verhalten zu dienen.

Wenn Ihre Anwender noch unsicher sind oder nicht der Meinung sind, dass sie die Verantwortung für Sicherheit tragen:

- Personalisieren Sie Schulungen und zeigen Sie, warum jeder einzelne für die Sicherheit im Unternehmen verantwortlich ist. Verbessern Sie die Kommunikation vonseiten der Unternehmensleitung und von Sicherheitsverantwortlichen, damit sich die Anwender ihrer Verantwortung stärker bewusst werden und verstehen, welche Bedeutung ihr Verhalten für das Unternehmen hat.

Außerdem ist es wichtig, erstklassige Sicherheitsschulungen sowie Maßnahmen zur Prävention, Erkennung und Reaktion zu implementieren. Erweiterte Lösungen können helfen, ein besseres Gleichgewicht zwischen strikteren Sicherheitskontrollen und der Produktivität zu finden, indem Anwender mit weniger Bedrohungen konfrontiert werden. Wenn Sie zum Beispiel eine E-Mail-Sicherheitslösung mit einer Effektivität von 99,9 % einsetzen, müssen sich die meisten Anwender nie entscheiden, wie sie auf einen verdächtigen Link reagieren sollen.

Arbeiten Sie außerdem mit den Verantwortlichen im Unternehmen zusammen, um zu gewährleisten, dass die implementierten Sicherheitsrichtlinien benutzerfreundlich sind. Anwender sind weniger geneigt, bestehende Systeme zu umgehen, wenn die Sicherheitsmaßnahmen ihren Zielen nicht im Weg stehen. Und sie werden die Kontrollen mit größerer Wahrscheinlichkeit nutzen, wenn sie intuitiv sind und keine Schulungen erfordern.

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 **www.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 85 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.

0402-001-04-01