REPORT

proofpoint.

PEOPLE-CENTRIC CYBERSECURITY

EINE STUDIE UNTER IT-SICHER-HEITSVERANTWORTLICHEN IN DEUTSCHLAND, ÖSTERREICH UND DER SCHWEIZ (DACH)

Eine Studie von

techconsult
The IT Market Analysts

ZUSAMMENFASSUNG

Die Cyberbedrohungslandschaft im DACH-Raum entwickelt sich rasant weiter. Dabei haben es Cyberkriminelle zunehmend auf Menschen anstatt auf IT-Infrastrukturen abgesehen.

Von E-Mail-basierten Bedrohungen, wie Business Email Compromise (BEC) bis hin zu Phishing von Anmeldeinformationen, kompromittierten Cloud-Konten und Ransomware-Angriffen – Cyberkriminelle sind sich bewusst, dass Mitarbeiter leicht ausgetrickst werden können.

Mit Social-Engineering-Techniken stehlen Angreifer Anmeldeinformationen, greifen sensible Daten ab und erpressen auf betrügerische Weise Gelder. Mitarbeiter auf allen Ebenen der Unternehmenshierarchie und in allen Funktionen können ihr Unternehmen auf vielfältige Weise gefährden. Vom Einsatz schwacher Passwörter über das Teilen von Anmeldeinformationen bis hin zum Klicken auf schädliche Links und dem Herunterladen unerlaubter Anwendungen.

Um diesen Gefahren zu begegnen, müssen Unternehmen wissen, wie oft sie gezielt angegriffen werden, welche Risiken damit verbunden sind und wie gut sie – und vor allem die Belegschaft – auf diese Angriffe vorbereitet sind. Die Aufklärung der Mitarbeiter und das Sicherheitsbewusstsein machen häufig den Unterschied zwischen einem versuchten und einem erfolgreichen Cyberangriff.

Um besser verstehen zu können, wie sich personenbezogene Cyberangriffe auf Unternehmen auswirken, hat Proofpoint eine Umfrage unter CSOs/CISOs im DACH Raum in Auftrag gegeben. Im Rahmen der im Juli und August 2020 vom Beratungsunternehmen techconsult durchgeführten Studie wurden 202 Unternehmen mit 250 oder mehr Mitarbeitern aus verschiedenen Branchen befragt.

Die Studie hat vier Schlüsselbereiche analysiert:

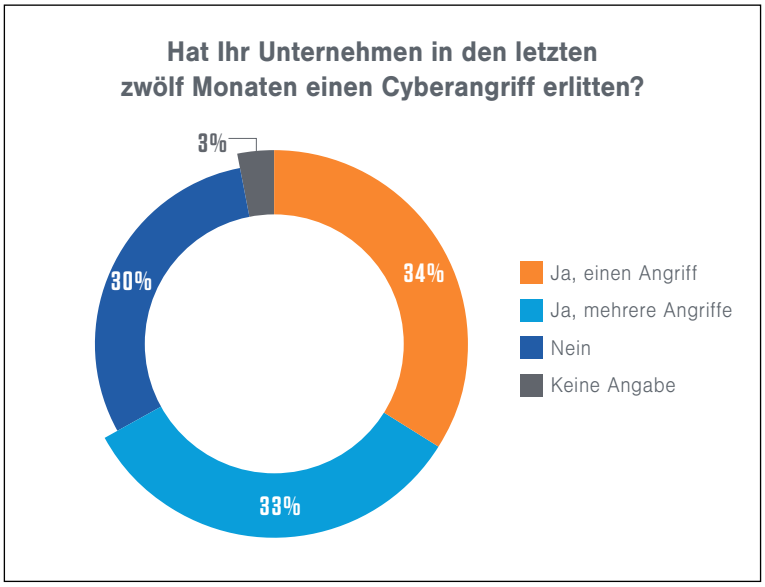
- Häufigkeit von Cyberangriffen
- Mitarbeiter- und Organisationsbereitschaft
- Herausforderungen bei der Umsetzung von Cyberstrategien
- Die Auswirkung der COVID-19-Pandemie auf die Cybersicherheit

Die Studie zeigt, dass die Notwendigkeit, Menschen vor unmittelbar bevorstehenden Bedrohungen zu schützen, nie größer war, da die Mehrheit der Organisationen im DACH-Raum in den letzten zwölf Monaten mindestens einem Cyberangriff ausgesetzt war. Von der Einbindung auf Vorstandsebene bis hin zur Erhöhung des Cybersicherheitsbewusstseins müssen Unternehmen Maßnahmen ergreifen, um ihre Cyberabwehr zu stärken.

Dieser Bericht hebt diese und andere wichtige Erkenntnisse aus der Umfrage hervor.

#1: ORGANISATIONEN IM DACH-RAUM SIND EINER VIELFÄLTIGEN BEDROHUNGSLANDSCHAFT AUSGESETZT

Es besteht kein Zweifel, dass Unternehmen weltweit mit einer sich schnell entwickelnden Bedrohungslandschaft konfrontiert sind. Der deutschsprachige Raum ist dabei keine Ausnahme. Unsere Umfrage ergab, dass 67 Prozent der CSOs/CISOs in den letzten zwölf Monaten mindestens einen Cyberangriff auf ihr Unternehmen erlitten haben*. 33 Prozent gaben an, dass ihr Unternehmen gleich mehrfach ins Visier genommen wurde.

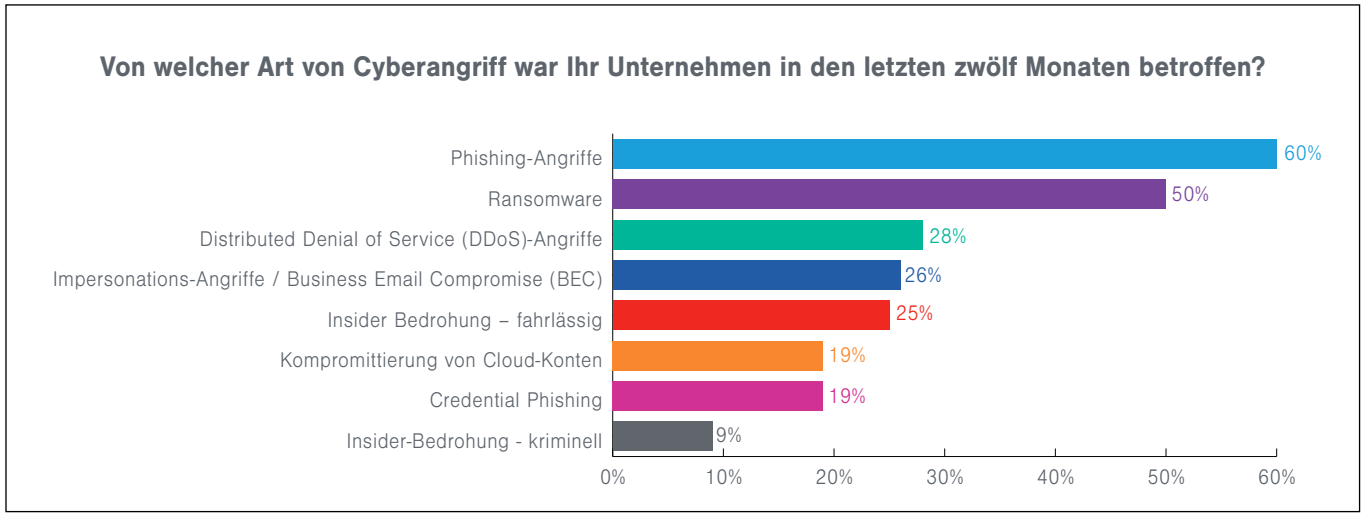


Phishing und Ransomware bleiben die gefährlichsten Bedrohungen, aber Insider-Bedrohungen nehmen zu und werden zum Problem.

Cyberkriminelle nutzen die Unbedarftheit der Mitarbeiter gnadenlos aus, um sich Zugang zu E-Mail-Konten, vertraulichen Informationen und Unternehmenssystemen zu verschaffen. Phishing bildet dabei die Hauptangriffsform für Cyberkriminelle (60 Prozent). Die zweithäufigste Methode in den letzten zwölf Monaten waren Cyberangriffe mit Ransomware (50 Prozent).

Zudem zeigt der 2020 vom Ponemon Institute veröffentlichte „Cost of Insider Threat Report“, dass Insider-Bedrohungen für Unternehmen ein wachsendes Problem darstellen. Die Zahl der Vorfälle stieg in nur zwei Jahren um erstaunliche 47 Prozent.

Dies spiegelt sich auch in dieser Umfrage wider. So gaben 34 Prozent der CSOs/CISOs im DACH-Raum an, dass ihre Unternehmen im vergangenen Jahr Opfer von Insider-Bedrohungen geworden sind. Dabei entfielen 25 Prozent auf Bedrohungen aufgrund von Fahrlässigkeit oder mangelndem Wissen der Mitarbeiter, während 9 Prozent der Bedrohungen durch böswilligen Datenmissbrauch der Mitarbeiter hervorgerufen wurden.



* Kombination von „Ja, ein Angriff“ und „Ja, mehrere Angriffe“

#2: CSOS UND CISOS IN DACH SIND VOR ALLEM BESORGT ÜBER DEN VERLUST SENSIBLER INFORMATIONEN UND STÖRUNGEN DES BETRIEBS AUFGRUND VON CYBERANGRIFFEN

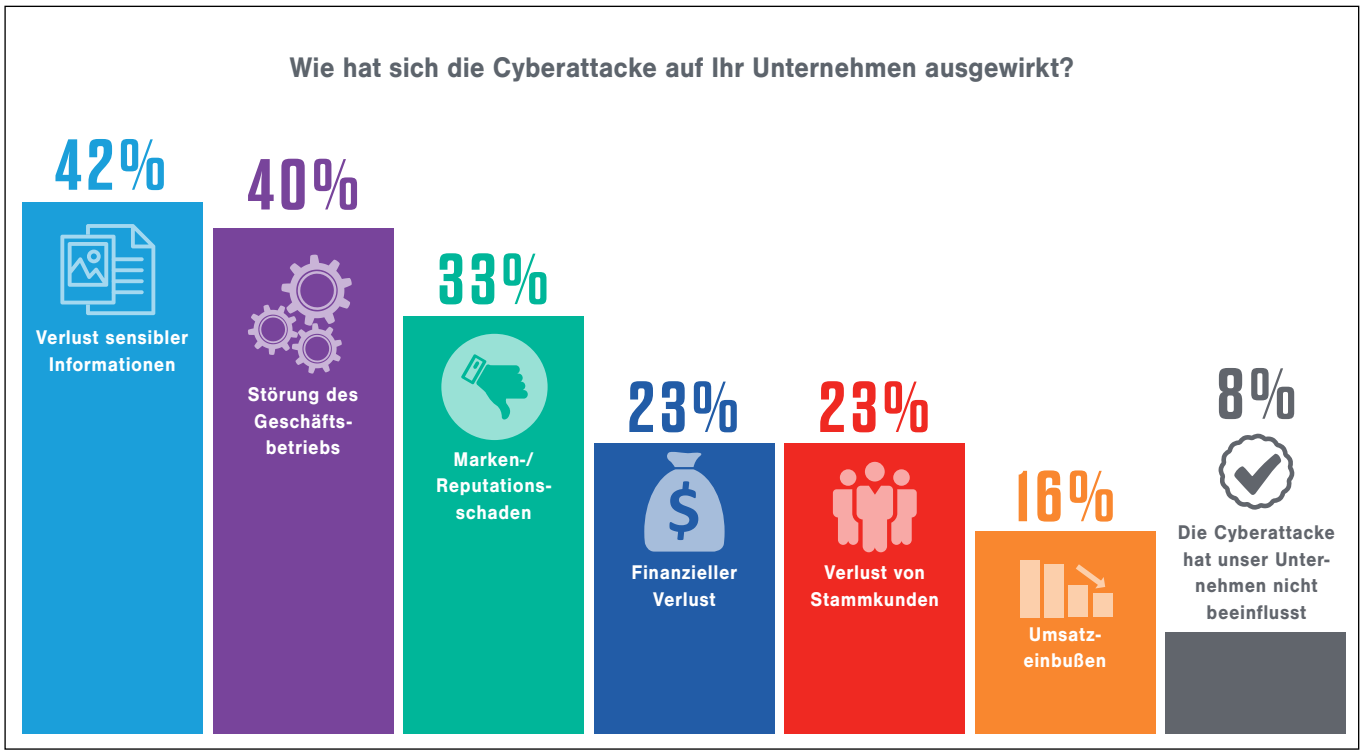
Cyberangriffe jeglicher Art können verheerende Folgen für die beteiligten Organisationen haben.

Das World Economic Forum schätzt, dass zwischen 2019 und 2023 ein globaler Wert von 5,2 Billionen US-Dollar durch böswillige Akteure gefährdet sein wird. Von entgangenen Einnahmen und Reputationsschäden bis hin zu Ausfallzeiten, Anwaltskosten, Entschädigungs- und Sanierungsleistungen, können die finanziellen Auswirkungen solcher Angriffe schnell zu erheblichen Folgen führen.

E-Mail-Betrug über Business Email Compromise (BEC), bei dem ein Angreifer eine falsche Identität annimmt, um den E-Mail Adressaten zu täuschen, nimmt ebenfalls zu – und kann sich als kostspielig erweisen. Der jüngste FBI-Bericht schätzt die weltweiten Gesamtverluste infolge von BEC auf 1,7 Mrd. USD im Jahr 2019.

Unsere Umfrage ergab, dass 42 Prozent der Unternehmen im DACH-Raum den Verlust sensibler Informationen als häufigste Folge eines Cyberangriffs anführte – gefolgt von Geschäfts- und Betriebsstörungen (40 Prozent). Marken- / Reputationsschäden (33 Prozent), der Verlust von Stammkunden (23 Prozent) sowie Umsatzeinbußen (16 Prozent) sind weitere häufig genannte Folgen.

42 Prozent der Unternehmen im DACH-Raum gaben den Verlust sensibler Informationen als größte Folge eines Cyberangriffs an – gefolgt von Geschäfts- und Betriebsstörungen (40 Prozent) und Reputationsschäden (33 Prozent)



#3: ORGANISATIONEN IM DACH-RAUM SIND SICH DER GEFÄHRDUNG BEWUSST – STEHEN JEDOCH VOR HERAUSFORDERUNGEN, UM SICH SELBST ZU SCHÜTZEN

Cyberrisiken und deren Abwehr stehen auf der Tagesordnung der meisten Unternehmen. Die Realität ist aber oft weit vom gewünschten Zustand entfernt: Auf die Frage, ob die Sicherheitsverantwortlichen glauben, dass ihr Unternehmen auf einen Cyberangriff vorbereitet ist, konnten lediglich 24 Prozent der Befragten diese vorbehaltlos bejahen, während 48 Prozent zumindest teilweise zugestimmt haben. Noch bedenklicher scheint es um die größeren Unternehmen (mehr als 5.000 Mitarbeiter) zu stehen, von denen lediglich nur 12 Prozent voll und ganz davon ausgehen, auf Cyberattacken vorbereitet zu sein. Im Branchenvergleich sehen sich vor allem die öffentlichen Verwaltungen eher schlecht gegen Cyberattacken gewappnet, denn nur 46 Prozent dieses Segments können von sich behaupten zumindest annähernd auf Cyberattacken reagieren zu können (insgesamt 72 Prozent der Unternehmen).

Nur 24 Prozent der befragten CSOs / CISOs im DACH-Raum sind sich absolut sicher, dass ihr Unternehmen auf eine Cyberattacke vorbereitet ist.

Bei der Befragung zu den größten Risiken für ihre Organisation führten 70 Prozent der CSOs/CISOs im DACH-Raum menschliche Fehler und ein geringes Sicherheitsbewusstsein als die größten Risikofaktoren für ihr Unternehmen an.

Angesichts der Tatsache, dass Angreifer zunehmend auf die Unternehmensmitarbeiter abzielen, ist es nicht verwunderlich, dass Security-Verantwortliche menschliches Versagen und ein schlechtes Sicherheitsbewusstsein als hohes Risiko betrachten. Was überrascht, ist die mangelnde Besorgnis der Vorstandsmitglieder über die Cybersicherheitslage ihrer Organisationen. Nur 26 Prozent der Befragten stimmten nachdrücklich zu, dass Cybersicherheit im Jahr 2020 ein wesentliches Thema auf Vorstandsebene für ihr Unternehmen darstellt.

Inwieweit stimmen Sie den folgenden Aussagen zum Thema Cybersicherheit in Ihrem Unternehmen zu?

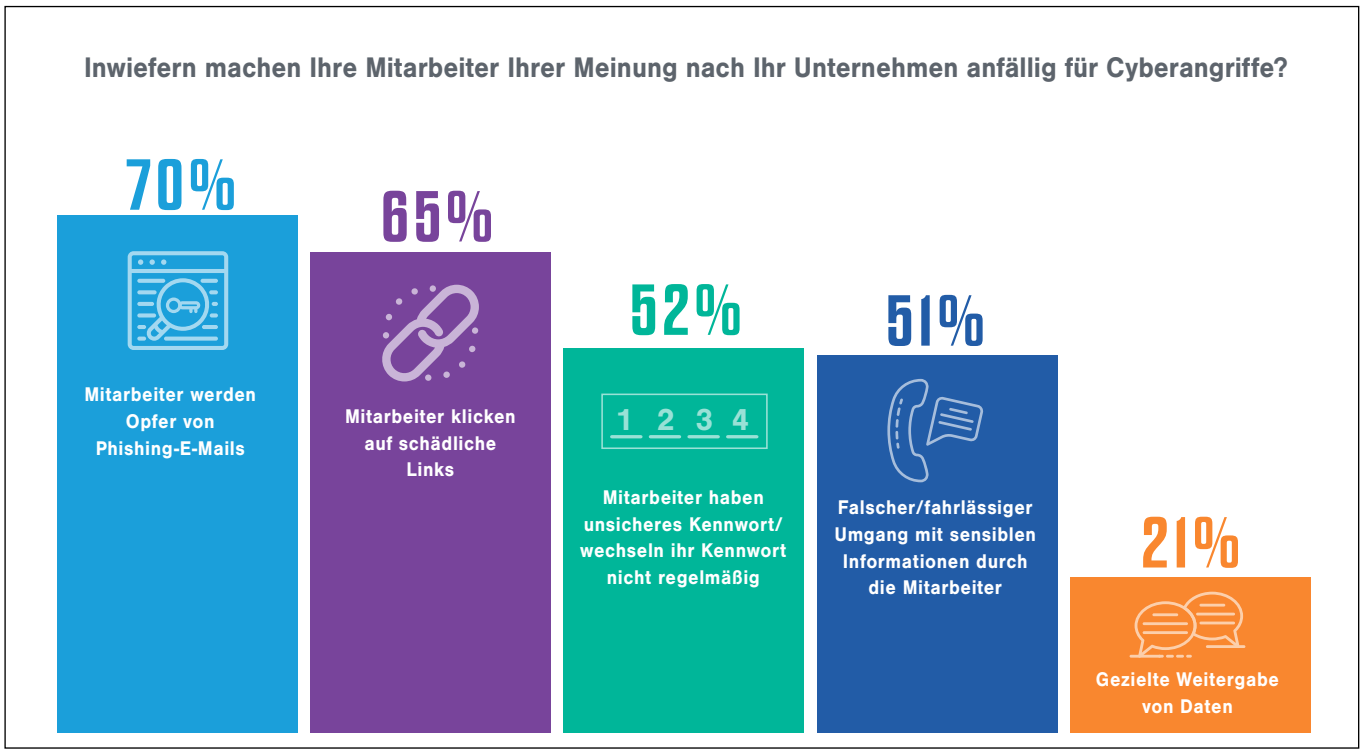
	Stimme voll und ganz zu	Stimme zu	Weder noch	Stimme eher nicht zu	Stimme überhaupt nicht zu
Unser Geschäft ist auf einen Cyberangriff vorbereitet	24%	48%	14%	11%	2%
Cybersicherheit ist für unser Unternehmen in den nächsten 12 Monaten ein Thema auf Vorstandsstandsebene	26%	41%	18%	9%	4%
Menschliches Versagen und mangelndes Sicherheitsbewusstsein ist das größte Risiko für unser Unternehmen	28%	42%	16%	12%	2%

#4: MITARBEITER IM DACH-RAUM MÜSSEN BESSER FÜR DIE BEKÄMPFUNG VON CYBERANGRIFFEN GERÜSTET SEIN

Obwohl die Mitarbeiter die letzte Verteidigungsmöglichkeit gegen Cyberangriffe bilden, muss festgestellt werden, dass es den Arbeitskräften im DACH-Raum häufig an Sicherheitskenntnissen und -bewusstsein mangelt.

Laut Angaben der CSOs und CISOs zählen insbesondere das Hereinfallen auf Phishing-Angriffe (70 Prozent), das Klicken auf schädliche Links (65 Prozent), unsichere Passwörter (52 Prozent) und ein fahrlässiger Umgang mit sensiblen Informationen (51 Prozent) zu den häufigsten Fehlern der Mitarbeiter im Bereich der digitalen Sicherheit im deutschsprachigen Raum.

Weitere Untersuchungen von Proofpoint haben ergeben, dass fast jede vierte Person, die eine Phishing-E-Mail erhält, diese auch öffnet. Mehr als 10 Prozent geben dabei zu, auch auf darin enthaltene schädliche Links zu klicken.



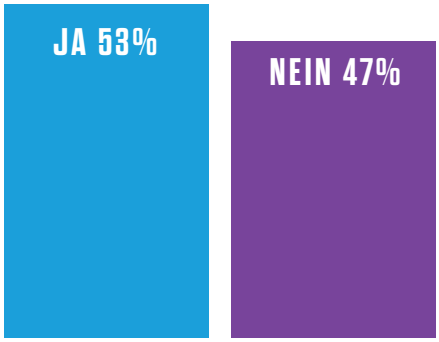
Cyberbewusstsein der Mitarbeiter im Rampenlicht

Angesichts der zunehmenden Cyberangriffe auf Personen ist es durchaus überraschend, dass immerhin knapp die Hälfte (47 Prozent) der CSOs/CISOs im DACH-Raum nicht glauben, dass ihr Unternehmen durch die Mitarbeiter anfällig für einen Cyberangriff ist.

Leider spiegelt sich dieses Gefühl auch in dem vorhandenen Angebot von Schulungsprogrammen vieler Organisationen im DACH-Raum zur Sensibilisierung für Cybersicherheit wider. Trotz der sich schnell entwickelnden Bedrohungslandschaft gaben 77 Prozent der CSOs/CISOs im DACH-Raum an, ihre Mitarbeiter maximal zweimal im Jahr oder weniger in Best Practices für Cybersicherheit zu schulen.

77 Prozent der CSOs/CISOs im DACH-Raum geben an, ihre Mitarbeiter nur zweimal im Jahr oder weniger in Best Practices für Cybersicherheit zu schulen.

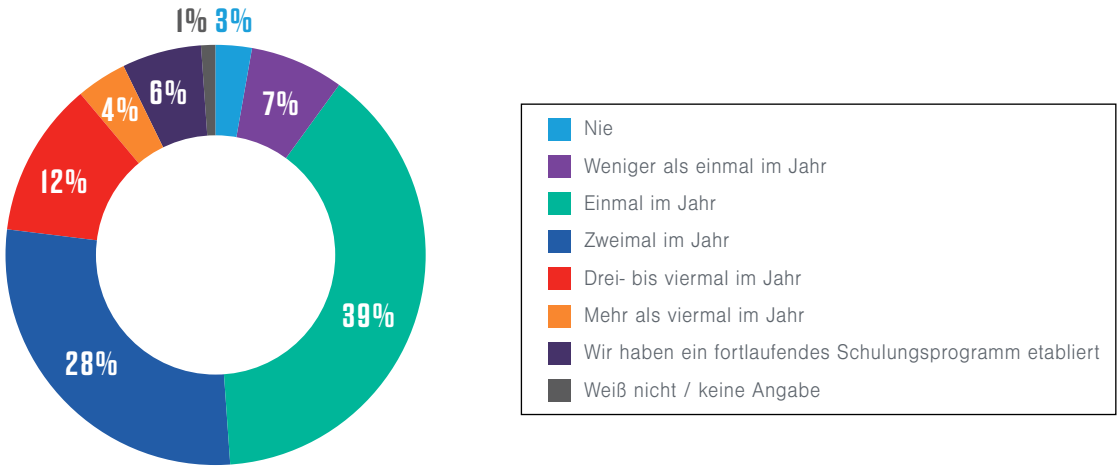
Glauben Sie, dass Ihr Unternehmen durch Ihre Mitarbeiter anfällig für einen Cyberangriff ist?



Auch hier zeigt der öffentliche Sektor deutlichen Nachholbedarf. Zwölf Prozent der CSOs/CISOs in diesem Segment gaben zu Protokoll, ihre Mitarbeiter nie oder weniger als einmal pro Jahr zu schulen. Im Durchschnitt aller Unternehmen liegt dieser Anteil bei knapp vier Prozent. In den befragten Finanz-, Versorgungs-, Transport- und Logistikunternehmen finden dagegen mindestens einmal im Jahr Mitarbeiterschulungen statt.

Regelmäßige und umfassende Schulungen sind für die Gewährleistung der Cybersicherheit jedoch unerlässlich. Alle Programme müssen ständig überprüft werden, um sicherzustellen, dass sie immer aktuell sind und mit der sich entwickelnden Bedrohungslandschaft Schritt halten. Die Aufklärung und das Bewusstsein der Mitarbeiter für die neuesten Bedrohungen sind maßgebliche Faktoren, die über den Erfolg versuchter Cyberangriffe entscheiden. Wenn solche Maßnahmen nicht umgesetzt und fortlaufend überprüft werden, sind Organisationen in gefährlichem Maße bedroht.

Wie oft schulen Sie Ihre Mitarbeiter durchschnittlich in Bezug auf das Bewusstsein für Cybersicherheit und Best Practices?

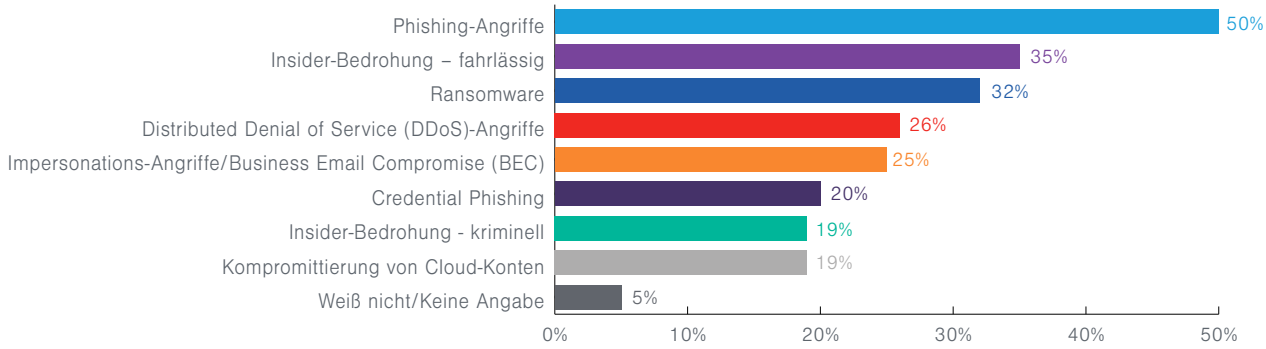


#5: DIE ZUKUNFT DER CYBERRISIKEN IM DACH-RAUM VERSCHIEBT SICH

Entwicklung von Angriffsmethoden und angepassten Cyberstrategien

Mit Blick auf die nächsten drei Jahre, glauben 54 Prozent der CSOs/CISOs im DACH-Raum, dass Bedrohungen von innen (fahrlässig oder kriminell) zukünftig die größte Cyberbedrohung darstellen, dichtgefolgt von Phishing-Attacken (50 Prozent). Auf den weiteren Plätzen folgen Ransomware (32 Prozent), DDoS-Attacken (26 Prozent), Business Email Compromise (25 Prozent), Credential Phishing (20 Prozent) und die Kompromittierung von Cloud-Konten (19 Prozent).

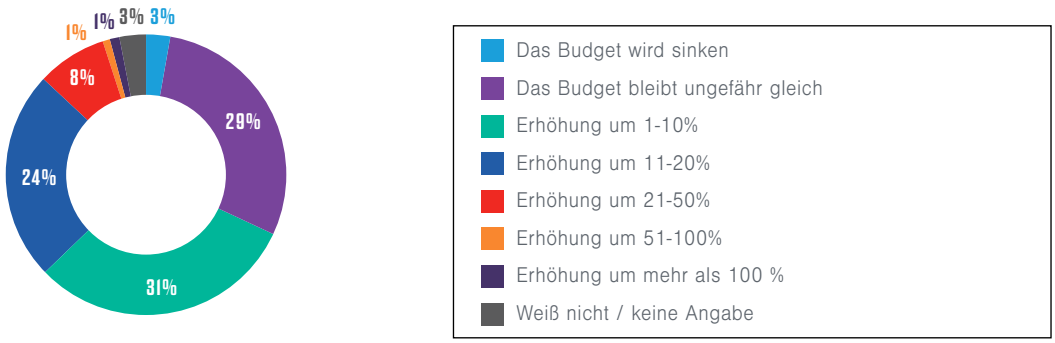
Worin sehen Sie die größten Cybersicherheitsbedrohungen innerhalb Ihrer Branche in den nächsten drei Jahren? (Bitte wählen Sie bis zu drei Bedrohungsarten aus)



Ilm Vergleich zu den tatsächlichen Sicherheitsvorfällen der letzten zwölf Monate, erwarten die Security-Verantwortlichen innerhalb der nächsten drei Jahre eine deutliche Zunahme fahrlässiger oder krimineller Bedrohungen von innen. Waren in den letzten zwölf Monaten 25 Prozent der Unternehmen von fahrlässigen Insiderbedrohungen betroffen, stufen aktuell bereits 35 Prozent (+ 40 Prozent) diese als eine der größten Cybersicherheitsbedrohungen innerhalb der nächsten drei Jahre ein. Gleichzeitig hält jedes fünfte Unternehmen böswilliges Mitarbeiterverhalten für eine der wesentlichsten zukünftigen Gefahren – mehr als doppelt so viel Unternehmen mit entsprechenden Vorfällen im letzten Jahr (9 Prozent).

Diese sich entwickelnde Bedrohungslandschaft erfordert auch Investitionen in die Cyberabwehr. Unsere Umfrage ergab, dass 55 Prozent der CSOs/CISOs im DACH-Raum von einer Erhöhung ihres Cybersecuritybudgets von bis zu 20 Prozent innerhalb der nächsten zwei Jahre ausgehen. Nur zwei Prozent der Befragten erwarten einen Rückgang, während 29 Prozent von gleichbleibenden Budgets ausgehen. Dies ist ein klarer Indikator dafür, dass Unternehmen sich der Notwendigkeit bewusst sind, die Cyberabwehr zu verbessern, um das Risiko zu verringern.

Was erwarten Sie, wie sich Ihr Budget für Cybersicherheit in den nächsten zwei Jahren entwickeln wird?



Transport und Logistik im Fokus von Angriffen mit COVID-19-Bezug

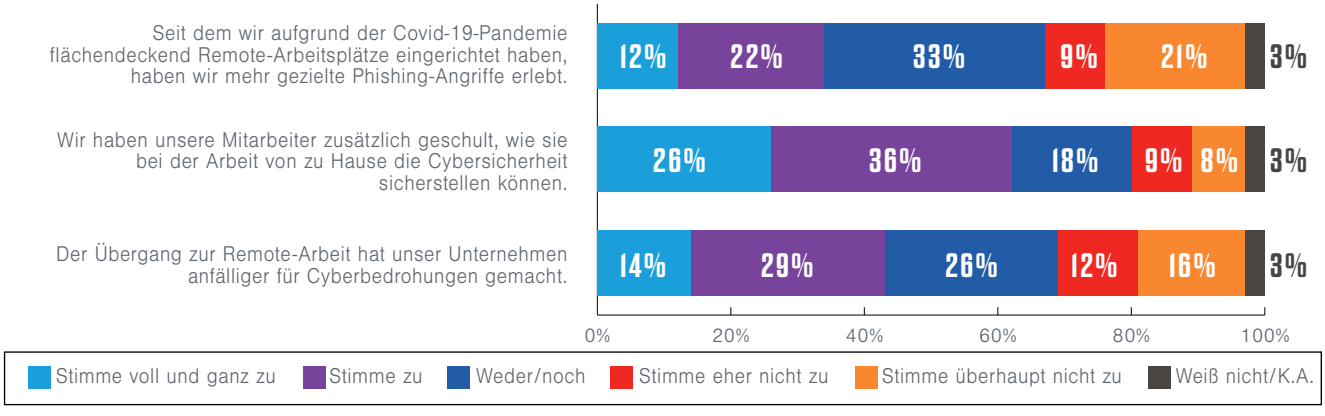
Im Zuge der COVID-19-Pandemie und der damit verbundenen Zunahme von Remote Working, ist auch der Stellenwert von Cyberattacken in den Unternehmen deutlich gestiegen. Über ein Drittel der CSOs/CISOs im DACH-Raum (35 Prozent) gab demnach an, von einem erhöhten Aufkommen von gezielten Phishing-Angriffen betroffen zu sein.

Eine überdurchschnittlich hohe Anzahl von Phishing-Angriffen während der COVID-19-Pandemie scheint insbesondere gegen Unternehmen im Transport-/Logistiksektor durchgeführt worden zu sein, wo 56 Prozent der CSOs/CISOs in diesem Segment einen entsprechenden Anstieg der Angriffe in ihrem Unternehmen verzeichneten. Dies spiegelte sich auch in unserer Bedrohungsanalyse wider, in der Proofpoint-Forscher signifikante Phishing-Aktivitäten im Zusammenhang mit COVID-19 feststellten, die speziell auf diesen Sektor abzielten.

Seit Beginn der Pandemie gab es Hunderte von Phishing-Angriffen im Zusammenhang mit COVID-19, bei denen die Opfer aufgefordert wurden, auf Links zu klicken, Anhänge herunterzuladen und Zugangsdaten auszutauschen. Es reicht bereits ein einziger unaufmerksamer Mitarbeiter, um die Sicherheit der gesamten Organisation zu gefährden. Auf die Frage, ob die Umstellung auf Remote-Arbeit ihr Unternehmen anfälliger für Cyberbedrohungen gemacht habe, waren 43 Prozent der leitenden IT-Sicherheitsverantwortlichen in Deutschland, Österreich und der Schweiz der Meinung, dass das auf ihr Unternehmen zuträfe.

Aber auch andere Bereiche sind betroffen: Cyberkriminelle missbrauchen weltweit die anhaltende COVID-19-Pandemie, um mittels gefälschter Websites Zugangsdaten zu erschleichen. Im Frühling 2020 beobachtete das Threat Research Team von Proofpoint einen deutlichen Anstieg bei der Erstellung von Vorlagen für Phishing-Websites in Zusammenhang mit staatlichen Hilfszahlungen, die im Rahmen der COVID-19-Pandemie gewährt werden. Die Templates der Cyberkriminellen imitierten dabei zahlreiche Websites von Regierungsstellen und bekannten Nichtregierungsorganisationen (NGOs), wie zum Beispiel der Weltgesundheitsorganisation (WHO).

Auswirkungen der Covid-19-Pandemie auf das Thema Remote-Working in den Unternehmen



Weit mehr als die Hälfte der etlichen Hundert Phishing-Kampagnen mit COVID-19-Bezug, die das Proofpoint Threat Research Team seit Januar 2020 erfasst hat, konzentrierten sich auf das Erschleichen von Benutzerdaten. Die Kriminellen hinter den Phishing-Angriffen passten ihre E-Mail-Köder dabei zumeist an aktuellen Themen an. Entsprechend erstellten und verbreiteten cyberkriminelle Gruppen passgenaue Phishing-Vorlagen zu Websites für COVID-19-Hilfszahlungen.

Es ist jedoch ermutigend zu sehen, dass die Mehrheit der Unternehmen im DACH-Raum proaktive Schritte unternommen haben, um das Bewusstsein der Mitarbeiter für diese neue Cyberbedrohungslandschaft zu schärfen: So haben fast zwei Drittel der Unternehmen (62 Prozent) ihren Mitarbeitern spezielle Cybersicherheitsschulungen gegeben, damit sie sicher von zu Hause aus arbeiten können.

FAZIT

Unabhängig von den Angriffsmethoden – E-Mail, Cloud-Anwendungen, Web, Social Media – machen sich Angreifer immer stärker den menschlichen Faktor zunutze.

Ob es sich um Betrüger handelt, die sich als vertrauenswürdige Kollegen ausgeben, oder um immer überzeugendere Phishing-E-Mails und bösartige Links – es sind die Anwender selbst, die im Kampf gegen Cyberkriminelle an vorderster Front stehen.

Nicht erst seit Beginn der COVID-19-Pandemie verbringen Menschen immer weniger Zeit an ihrem festen Büroarbeitsplatz und mehr Zeit damit, aus der Ferne, sei es im Home Office oder von unterwegs, zu arbeiten. Nach wie vor bleiben sie jedoch das Ziel Nr.1 für Angreifer und noch nie war es so wichtig wie heute, sicher und geschützt von entfernten Standorten aus zu arbeiten.

„Cyberkriminelle sind fokussiert und verbessern ihre Fähigkeiten und Techniken ständig. Wenn Sie nicht dasselbe tun, kann es nur einen Gewinner geben."

Michael Heuer, Vice President, DACH bei Proofpoint

Herkömmliche oder veraltete Remote-Zugriffsmethoden lassen sich nur schwer skalieren, sind nicht darauf ausgelegt, moderne cloudbasierte Infrastrukturen zu schützen und führen schnell zu potenziellen Sicherheitsrisiken. Diese erhöhen sich nochmals, wenn Remote-Mitarbeiter nicht den gleichen Sicherheitsstandards unterliegen, wie die Mitarbeiter innerhalb des Unternehmensnetzwerkes. Auf dieser Basis kann nicht sichergestellt werden, dass die gestiegenen Sicherheitsanforderungen und geltenden Vorschriften von den Mitarbeitern auch eingehalten werden.

Wenn es vor 2020 noch nicht klar war, so ist es jetzt mit Sicherheit klar: Die Menschen sind der Perimeter des Unternehmens. Deshalb ist eine auf Menschen ausgerichtete Strategie ein Muss für Unternehmen. Diese beginnt damit, Ihre am stärksten gefährdeten Benutzer zu identifizieren und sicherzustellen, dass sie mit dem Wissen und den Tools ausgestattet sind, um Ihr Unternehmen schützen zu können.

Neben technischen Lösungen und Kontrollen muss ein umfassendes Schulungsprogramm für das Sicherheitsbewusstsein im Mittelpunkt Ihrer Cyberabwehr stehen. Die Schulungen sollten regelmäßig, umfassend und anpassungsfähig sein und eine Reihe von Themen abdecken – von den Beweggründen und Mechanismen von Cyberbedrohungen bis hin dazu, wie sorglose Verhaltensweisen, beispielsweise die Mehrfachverwendung von Passwörtern und unzureichender Datenschutz, die Wahrscheinlichkeit eines erfolgreichen Angriffs erhöhen.

Daten verlieren sich nicht von selbst – es ist immer ein nachlässiger, kompromittierter oder böswilliger Anwender involviert. Ein personenzentrierter Ansatz kann folglich dort erfolgreich sein, wo frühere Lösungen versagt haben, um den notwendigen Cloud-basierten Schutz über alle wichtigen Kanäle unabhängig vom Standort des Benutzers, der Kommunikationsmethode oder den gesetzlichen Anforderungen zu gewährleisten.

Nur durch den Aufbau und die Umsetzung einer übergreifenden Sicherheitsstrategie, die den Menschen in den Mittelpunkt stellt, werden Unternehmen einen großen Schritt in Richtung Verbesserung ihrer IT-Sicherheit machen können.

techconsult
The IT Market Analysts

Alle Daten beziehen sich, sofern nicht anders angegeben, auf die von techconsult durchgeführten Untersuchungen mit 202 CSO/CISOs von Unternehmen mit 250 oder mehr Mitarbeitern im DACH-Raum im Juli 2020.

proofpoint®

Kontaktieren Sie uns unter info-germany@proofpoint.com um Ihr Unternehmen besser zu schützen.

ÜBER PROOFPOINT
Proofpoint, Inc. (NASDAQ: PFPT) ist ein führendes Unternehmen für Cybersicherheit, das die größten Vermögenswerte und Risiken von Unternehmen schützt: ihre Mitarbeiter. Mit einer integrierten Suite von Cloud-basierten Lösungen hilft Proofpoint Unternehmen auf der ganzen Welt, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre Benutzer widerstandsfähiger gegen Cyberangriffe zu machen. Führende Unternehmen jeder Größe, darunter mehr als die Hälfte der Fortune 1000, verlassen sich auf die personenbezogenen Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre wichtigsten Risiken in Bezug auf E-Mail, Cloud, soziale Medien und das Internet zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.com/de**.