2024 / 2025

CYBERSICHERHEIT IN ZAHLEN

Lernen. Wissen. Handeln.

Liebe Leserinnen und Leser,

seit der Veröffentlichung von ChatGPT vergeht eigentlich kein Tag mehr, an dem ich nicht um eine Einschätzung zu künstlicher Intelligenz (KI) gebeten werde. Klar ist: Unternehmen profitieren davon auf vielfältige Weise und verbessern die Effizienz und Qualität etwa in der Produktion. Gleichzeitig können sie auch Risiken minimieren. Aber klar ist auch: Noch sind keine selbstdenkenden Maschinen im Einsatz. Es braucht Menschen, die ein tiefes Verständnis für diese digitalen Tools besitzen. Und die gleichzeitig eine Vorstellung davon haben, welches Ergebnis am Ende herauskommen soll.

Auch Cyberkriminelle greifen immer mehr auf künstliche Intelligenz zurück und gestalten ihre Angriffe effizienter. Nicht nur bei Phishing-Mails, die authentischer und schwerer zu erkennen sind. Auch beim sogenannten Fuzzing kommt KI zum Einsatz, um automatisiert Schwachstellen in Netzwerken und Programmen zu suchen und auszunutzen. Kriminelle Hacker setzen nicht zuletzt auch bei der Vorbereitung auf KI. Durch die Analyse sozialer Medien und anderer öffentlicher Informationen können sie zielgerichteter angreifen und verbessern damit die Wahrscheinlichkeit eines erfolgreichen Angriffs.

Zum vierten Mal haben wir mit brand eins und Statista zentrale Zahlen zu allen Aspekten der Sicherheit in der digitalen Welt für dieses Magazin zusammengetragen. Und traditionell steht am Anfang dieses Heftes unsere exklusive Umfrage. Sie widmet sich unter anderem dem Thema künstlicher Intelligenz. Mehr als 5.000 Menschen in Deutschland haben uns Fragen zu ihrem Wissensstand und ihren Bedenken bezüglich des Einsatzes von KI beantwortet.

Neben dem umfangreichen Zahlenwerk gibt es wieder spannende Reportagen über interessante Menschen aus der Cybersicherheit. Ein Bericht geht dabei der Frage nach, was Hacker sind und wie sie ihr Können sowohl in guter als auch böser Absicht einsetzen.

Ich lade Sie herzlich auf eine spannende Lektüre ein und freue mich auf den Austausch mit Ihnen.

Mit herzlichem Gruß

Ihr Andreas Lüning
Vorstand und Mitgründer G DATA CyberDefense AG

Auf Abwehr

Es stimmt schon: Künstliche Intelligenzen können uns eine Reihe formaler, auch diffiziler Aufgaben abnehmen. Wir werden mit ihrer Hilfe schneller, gründlicher, effizienter. Aber dadurch wird das menschliche Wissen nicht unwichtig. Im Gegenteil: Je mehr uns KIs bei unserer Arbeit unterstützen, desto mehr neue Fähigkeiten werden wir brauchen, um unsere Daten, unsere Systeme und unsere kritischen Infrastrukturen zu schützen.

Wir haben für diese Ausgabe Menschen getroffen, deren Job es ist, für Sicherheit zu sorgen. Sandra Heger zum Beispiel, die als Chief Information Security Officer an der Hochschule Ruhr West für den Schutz der IT-Systeme und aller physischen Räume und Dokumente zuständig war (*Seite 24*). Was im Falle eines Angriffs zu tun ist, hat Heger nicht nur in Übungen simuliert: Anfang 2023 konnte sie mit ihrem Team einen schweren Hackerangriff abwehren. Im neuen Netzwerk Informationssicherheit der Hochschulen Nordrhein-Westfalens hilft die studierte Informatikerin heute, landesweit Daten und IT der Wissenschaftsbetriebe zu schützen.

Das versucht auch die Grünen-Politikerin Tabea Rößner, die im Deutschen Bundestag den Ausschuss für Digitales leitet (*Seite 78*). Die frühere Journalistin fordert eine Kehrtwende im Bereich der IT-Sicherheitspolitik. „Es braucht neue Rechtsgrundlagen, zum Beispiel für den Schutz unserer kritischen Infrastrukturen“, sagt sie im Gespräch und verweist auf das Wettrennen zwischen Kriminellen und denjenigen, die versuchen, deren Angriffe abzuwehren, was noch viel zu wenig in unser aller Bewusstsein sei.

Das würde wohl auch Henrik Hohenlohe unterschreiben, der im sächsischen Landeskriminalamt die größte Abteilung zum Schutz gegen Cyberkriminalität leitet (*Seite 56*). Er und sein Team haben gut zu tun, die Zahl der Cyberverbrechen steigt von Jahr zu Jahr. Es wächst aber auch die Kompetenz derer, die für Schutz sorgen. „Wir stellen den internationalen Systemen der Täter ein internationales System der Strafverfolgung gegenüber“, sagt Kriminaloberrat Hohenlohe.

Ein Wettrennen wird es bleiben, das weiß kaum jemand besser als Lukas, der als Hacker beim Bundesnachrichtendienst (BND) arbeitet (*Seite 30*). Hacking hat ihn schon als Schüler fasziniert, ihn erst in eine Pentesting-Firma und dann zum Geheimdienst geführt. Lukas dringt legal in Netze im Ausland ein, um für die Bundesregierung Informationen zu beschaffen. Das Wichtigste in seinem Job: die Technik zu beherrschen, immer auf dem neuesten Stand zu sein, Trends zu kennen und zu wissen, was gerade benutzt wird.

Das könnte für uns Laien auch eine gute Idee sein. Denn das wird sich mit technologischen Entwicklungen und jeder neuen KI eher verschärfen: Cybersicherheit lässt sich nicht komplett an Aufpasser und Systeme delegieren. Sie bleibt Aufgabe von uns allen.

Susanne Risch
Chefredakteurin

Inhalt

Nachgefragt

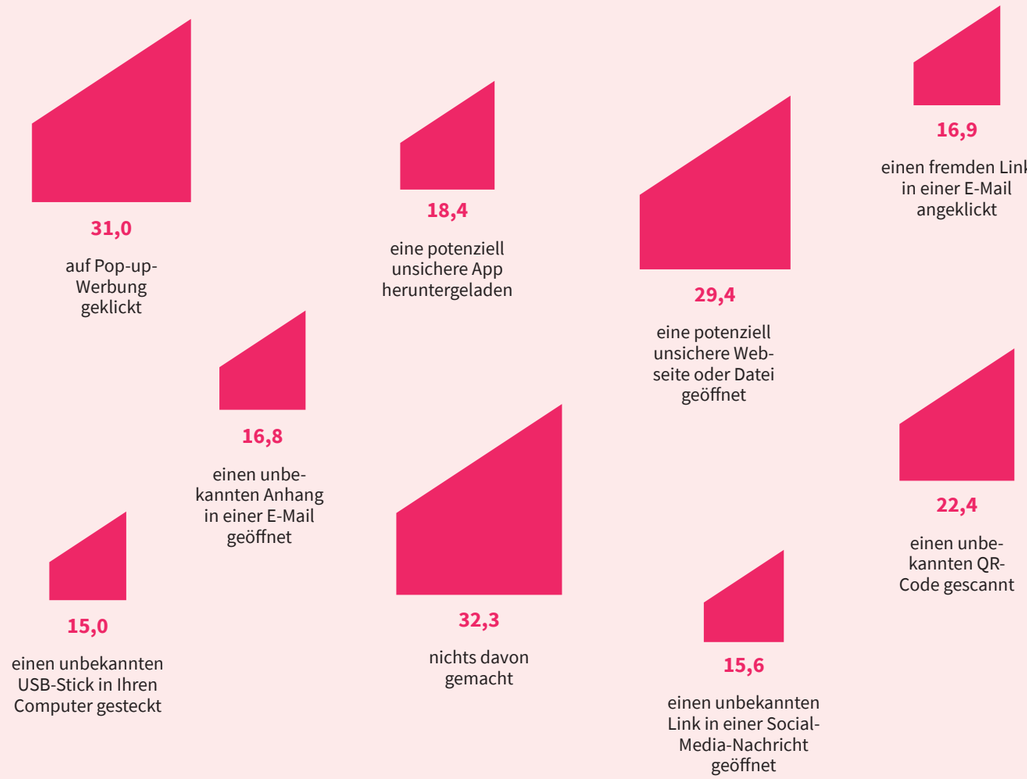
Wie sicher fühlen wir uns in unserem Berufsalltag? Mehr als 5 000 Beschäftigte in Deutschland zwischen 16 und 70 Jahren aus Unternehmen aller Branchen und Größen gaben im März und April 2024 Auskunft – über ihr Wissen, ihre Einschätzungen und Erfahrungen im Umgang mit IT. Die repräsentative Umfrage zeigt das aktuelle Stimmungsbild.

Neugierig – und überheblich

Neugierbedingte Handlungen mit Blick auf Cyberkriminalität; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2024; in Prozent *

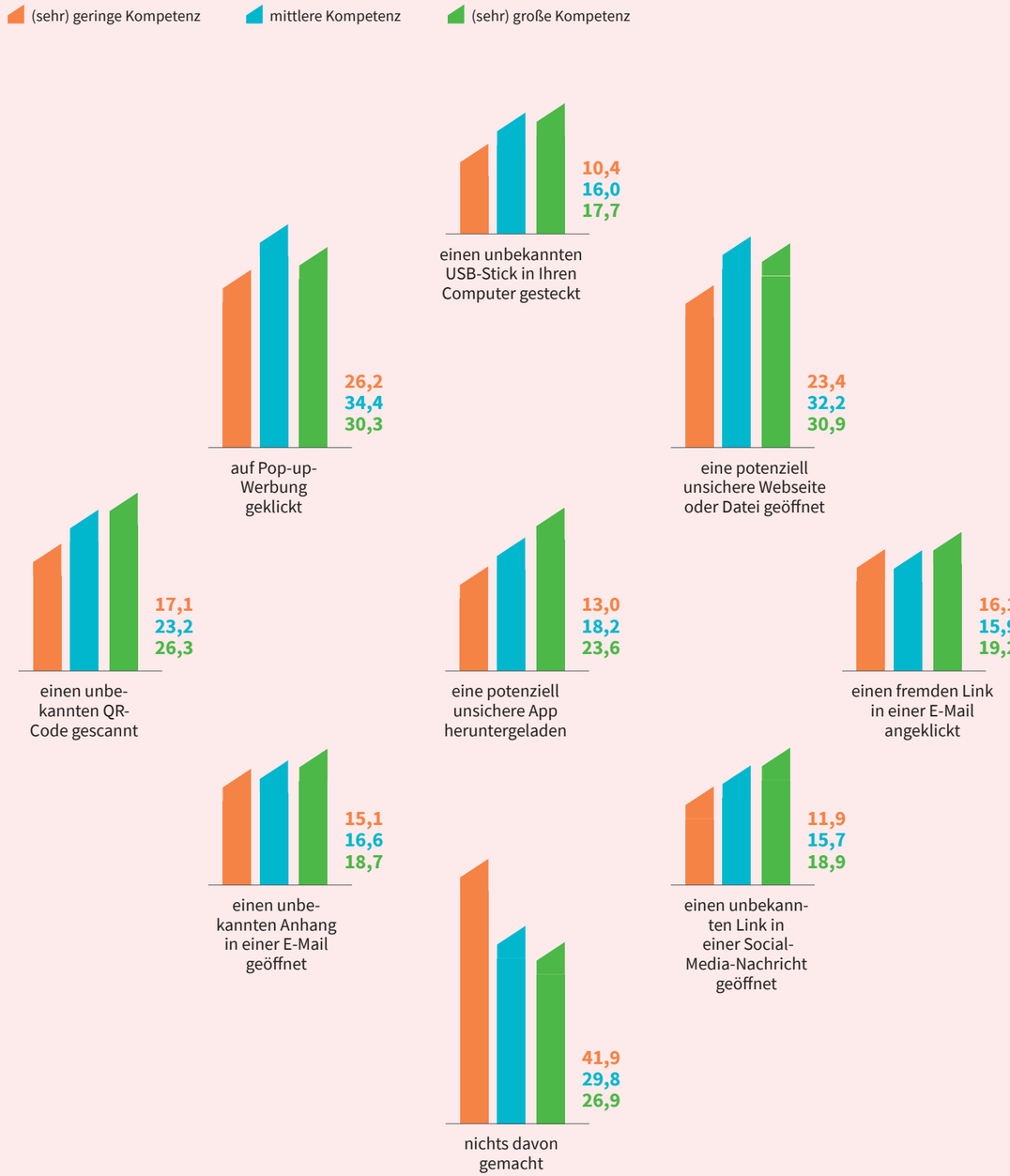
Haben Sie schon mal aus Neugier folgende Dinge gemacht?

insgesamt



* Mehrfachnennungen möglich. Quelle: Statista im Auftrag von G DATA

nach persönlicher Kompetenz im Bereich IT-Sicherheit



Glossar der Cyberbegriffe auf Seite 100 – 103

Überschätzt?

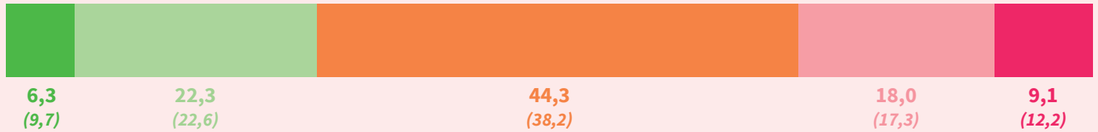
Einschätzung der persönlichen Kompetenz zum Thema IT-Sicherheit; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2024; in Prozent

Wie schätzen Sie Ihre persönliche Kompetenz beim Thema IT-Sicherheit ein?

sehr große Kompetenz | große Kompetenz | mittlere Kompetenz | geringe Kompetenz | sehr geringe Kompetenz

(Vergleichswert aus dem Vorjahr)

insgesamt



nach Abteilungen

* exklusive IT-Security. Quelle: Statista im Auftrag von G DATA

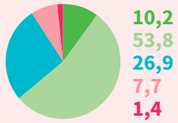
Unterschätzt?

Schutzgefühl durch IT-Sicherheitsmaßnahmen im beruflichen und privaten Umfeld; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2024; in Prozent

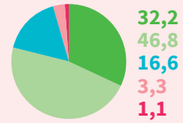
Wie gut fühlen Sie sich durch die Sicherheits- und Schutzmaßnahmen in Ihrem privaten und beruflichen Umfeld geschützt?

sehr gut | gut | weder noch | schlecht | sehr schlecht

insgesamt

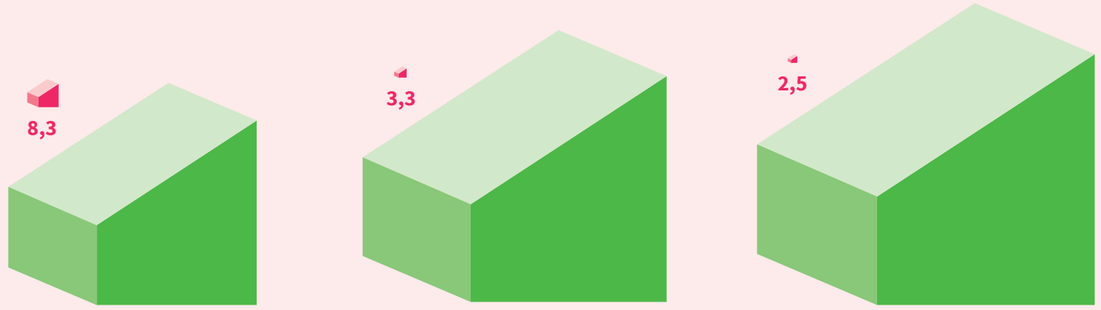


im privaten Umfeld

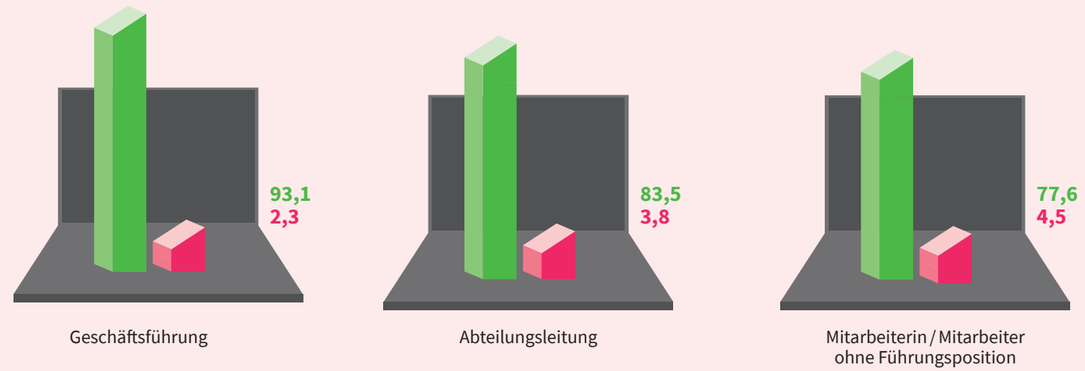


im beruflichen Umfeld

(sehr) gut / (sehr) schlecht nach persönlicher Kompetenz im Bereich IT-Sicherheit, im beruflichen Umfeld



(sehr) gut / (sehr) schlecht nach Positionen



Quelle: Statista im Auftrag von G DATA

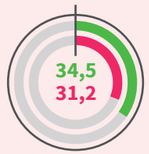
Sorglos

Risikoeinschätzung zum Thema Cyberkriminalität im privaten und beruflichen Umfeld; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2024; in Prozent

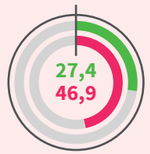
Wie hoch schätzen Sie das Risiko ein, dass Sie Opfer von Cyberkriminalität oder Datenklau werden?

(sehr) hoch (sehr) gering

insgesamt

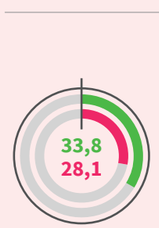


im privaten Umfeld

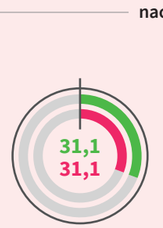


im beruflichen Umfeld

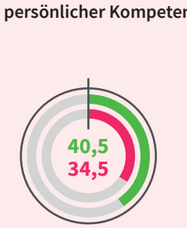
nach persönlicher Kompetenz im Bereich IT-Sicherheit



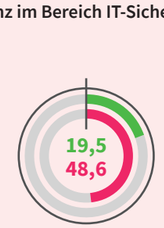
(sehr) geringe Kompetenz



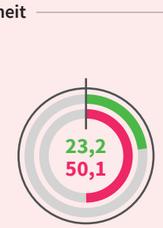
mittlere Kompetenz



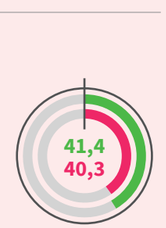
(sehr) große Kompetenz



(sehr) geringe Kompetenz



mittlere Kompetenz

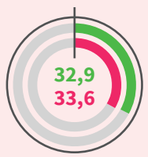


(sehr) große Kompetenz

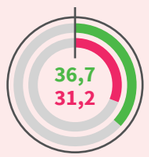
im privaten Umfeld

im beruflichen Umfeld

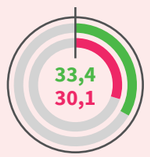
nach Unternehmensgröße



100 bis 249 Mitarbeiterinnen und Mitarbeiter

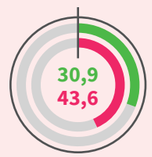


250 bis 999 Mitarbeiterinnen und Mitarbeiter

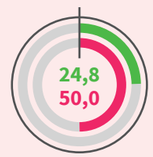


1000 und mehr Mitarbeiterinnen und Mitarbeiter

100 bis 249 Mitarbeiterinnen und Mitarbeiter



250 bis 999 Mitarbeiterinnen und Mitarbeiter



1000 und mehr Mitarbeiterinnen und Mitarbeiter

im privaten Umfeld

im beruflichen Umfeld

Quelle: Statista im Auftrag von G DATA

Ahnungslos

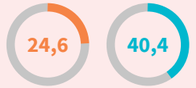
Frequenz, in der Befragte sich zu bestimmten Sicherheitsthemen informieren; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2024; in Prozent

Wie oft informieren Sie sich über folgende Themen?

(sehr) häufig selten / nie

insgesamt

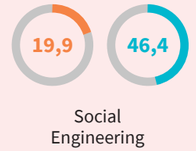
Datenschutzrichtlinien von Webseiten vor der Eingabe persönlicher Daten



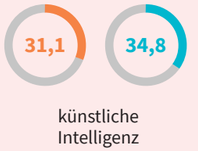
Malware / Ransomware

Phishing / Datendiebstahl

Umgang mit Passwörtern



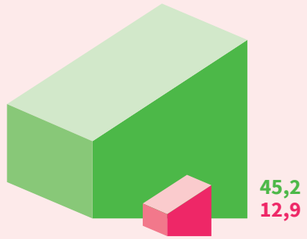
Social Engineering



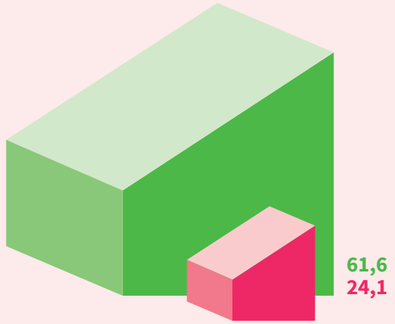
künstliche Intelligenz

nach persönlicher Kompetenz im Bereich IT-Sicherheit

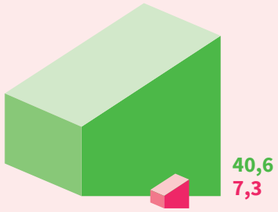
(sehr) große Kompetenz (sehr) geringe Kompetenz



Arbeitnehmerinnen und Arbeitnehmer, die sich zu Datenschutzrichtlinien von Webseiten (sehr) häufig informieren, bevor sie persönliche Daten eingeben



Arbeitnehmerinnen und Arbeitnehmer, die sich über den Umgang mit Passwörtern (sehr) häufig informieren



Arbeitnehmerinnen und Arbeitnehmer, die sich über Social Engineering (sehr) häufig informieren

Quelle: Statista im Auftrag von G DATA

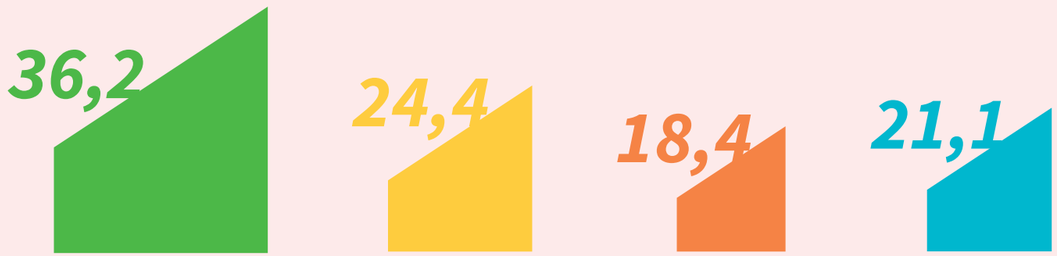
Zu unregelmäßig

Angebot an Cybersicherheitsschulungen und -trainings im Unternehmen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2024; in Prozent

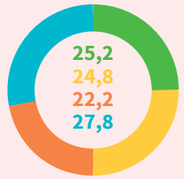
Bietet Ihr Unternehmen für alle Mitarbeiterinnen und Mitarbeiter (Online-)Schulungen / Veranstaltungen / Trainings rund um das Thema Cybersicherheit an?

ja, regelmäßig | ja, aber eher unregelmäßig | nein, nur für ausgewählte Abteilungen | Nein, ich habe noch nie von so einem Angebot in unserem Unternehmen gehört.

insgesamt

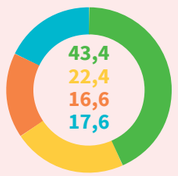


nach Unternehmensgröße



100 bis 249 Mitarbeiterinnen und Mitarbeiter

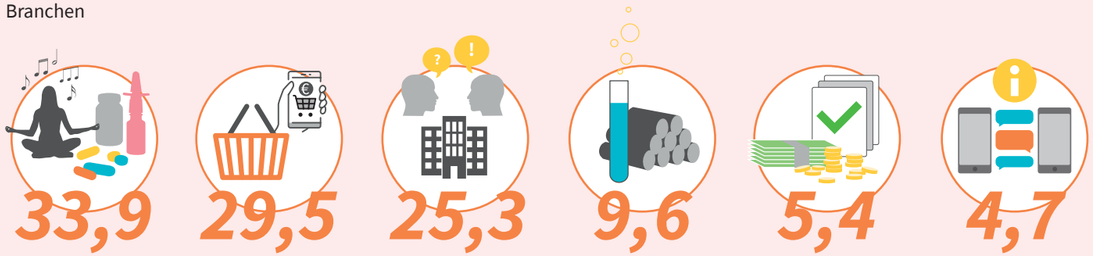
250 bis 999 Mitarbeiterinnen und Mitarbeiter



1000 und mehr Mitarbeiterinnen und Mitarbeiter

nach Branchen

Anteil der Arbeitnehmerinnen und Arbeitnehmer, die noch nie von so einem Angebot in ihrem Unternehmen gehört haben nach Branchen



Gesundheit & Soziales | Handel | öffentlicher Dienst | Chemie & Rohstoffe | Finanzen & Versicherungen | Telekommunikation & Information

Quelle: Statista im Auftrag von G DATA

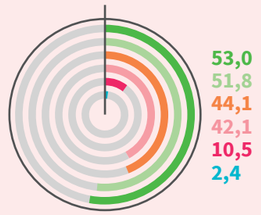
Zu halbherzig

Maßnahmen zur Förderung der Security Awareness ; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2024; in Prozent *

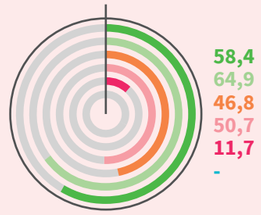
Welche Maßnahmen werden zur Förderung der Security Awareness eingesetzt?

kontinuierliche E-Learnings zur Sensibilisierung | jährliche Vor-Ort Schulung durch die eigene IT-Leiterin oder den eigenen IT-Leiter | Durchführung von Phishing-Simulationen | Präsenzschulungen mit externen Anbietern | sonstige Maßnahmen | keine

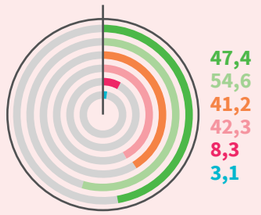
nach Positionen



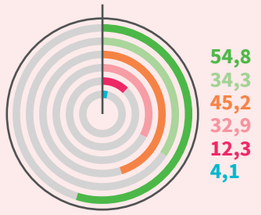
insgesamt



Bereichsleitung

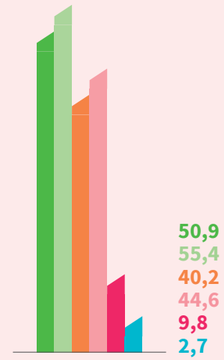


Abteilungsleitung

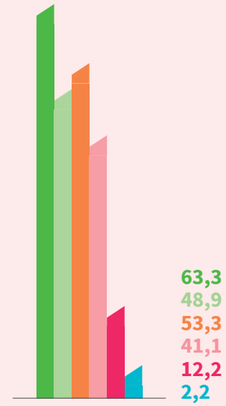


Teamleitung

nach Unternehmensgröße



250 bis 999 Mitarbeiterinnen und Mitarbeiter



1000 und mehr Mitarbeiterinnen und Mitarbeiter

* Mehrfachnennungen möglich. Quelle: Statista im Auftrag von G DATA

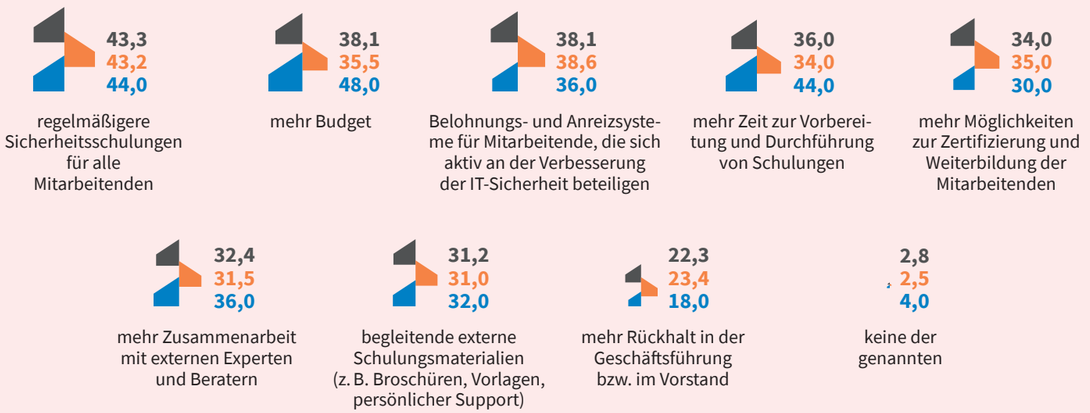
Mehr Unterstützung

Gewünschte Unterstützung für die Schulung von Mitarbeitenden; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2024; in Prozent *

Welche Art von Unterstützung wünschen Sie sich in Bezug auf die Mitarbeiterinnen- und Mitarbeiter-Schulung zu IT-Sicherheit?

nach Abteilungen

insgesamt | IT und EDV** | IT-Security

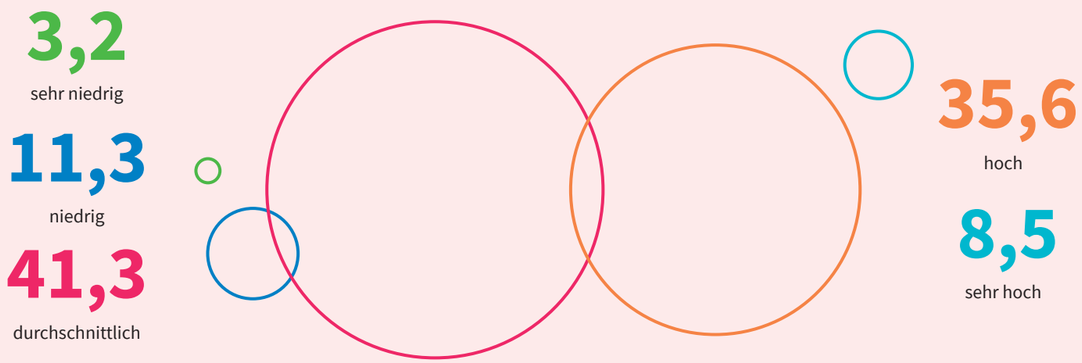


* Mehrfachnennungen möglich. ** exklusive IT-Security. Quelle: Statista im Auftrag von G DATA

Mehr Fachkräfte

Einschätzung des Fachkräftemangels im Bereich IT-Sicherheit; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2024; in Prozent

Wie schätzen Sie den Fachkräftemangel im Bereich IT-Sicherheit in Ihrem Unternehmen ein?



Quelle: Statista im Auftrag von G DATA

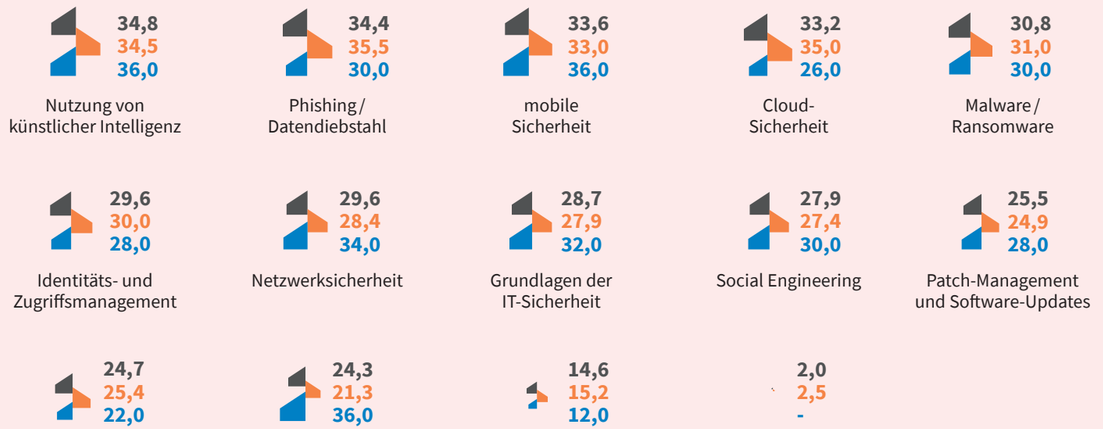
Mehr Wissen

Wissenslücken bei Kolleginnen und Kollegen in Bezug auf IT-Sicherheit; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2024; in Prozent *

In welchen Bereichen bestehen bei Ihren Kolleginnen und Kollegen die größten Wissenslücken in Bezug auf IT-Sicherheit?

nach Abteilungen

insgesamt | IT und EDV** | IT-Security



* Mehrfachnennungen möglich. ** exklusive IT-Security. Quelle: Statista im Auftrag von G DATA

Mehr Informationen, mehr Zeit und mehr Ressourcen

Probleme durch einen Mangel an Cybersicherheits-Personal; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die als Bereichsleitung, Abteilungsleitung oder Teamleitung in der IT-Security oder IT / EDV arbeiten und die den Fachkräftemangel als hoch oder sehr hoch einschätzen; 2024; in Prozent *

Welche der folgenden Probleme haben Sie erlebt, die Ihrer Meinung nach durch eine ausreichende Zahl von Cybersicherheits-Mitarbeiterinnen und -Mitarbeitern hätten gemildert werden können?

unzureichende Auswertung von Informationen (z. B. Meldungen von der Anti-Virus-Software)	43,1
nicht genug Zeit, um jedes Mitglied des Cybersicherheits-Teams angemessen zu schulen	41,3
nicht genügend Ressourcen, um Personal angemessen zu schulen	37,6
langsames Patchen von kritischen Systemen	36,7
Versäumnisse in Prozessen und Verfahren	33,9
nicht genug Zeit für eine angemessene Risikobewertung und -management	33,0
falsch konfigurierte Systeme	26,6
keine der genannten	4,6

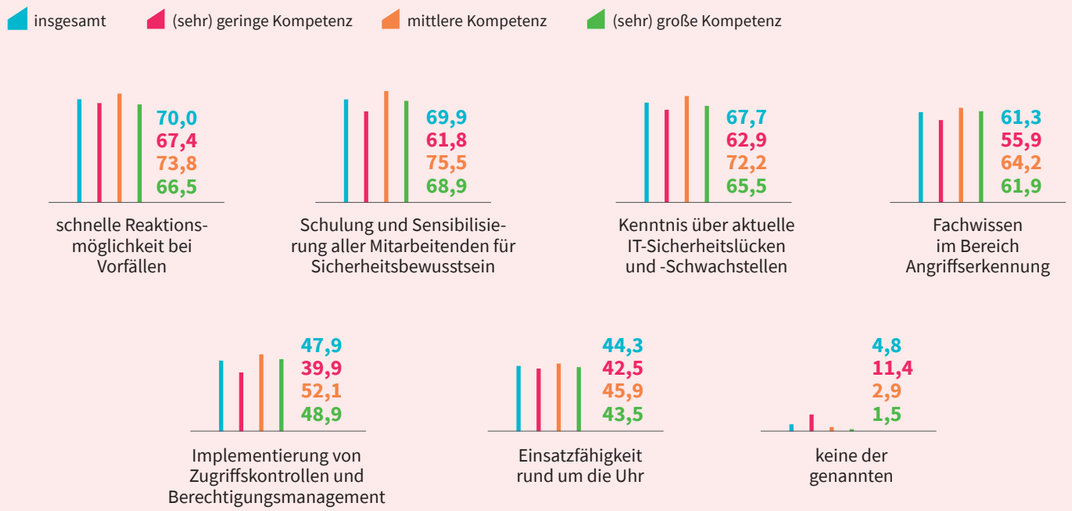
* Mehrfachnennungen möglich. Quelle: Statista im Auftrag von G DATA

Gut eingeschätzt?

Anforderungen an eine effektive IT-Sicherheit im Unternehmen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2024; in Prozent *

Was sind Ihrer Ansicht nach die aktuellen Anforderungen an eine effektive IT-Sicherheit?

nach persönlicher Kompetenz im Bereich IT-Sicherheit



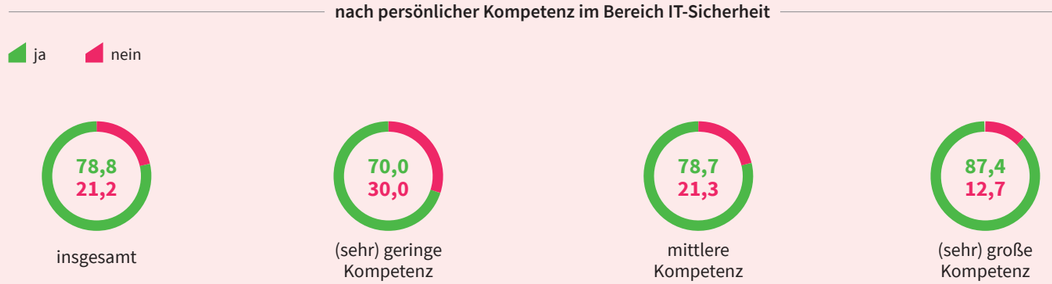
* Mehrfachnennungen möglich. Quelle: Statista im Auftrag von G DATA

Gut aufgestellt?

Einschätzung der Fähigkeit der IT-Abteilung; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2024; in Prozent

Sind Sie der Ansicht, dass Ihre IT-Abteilung den aktuellen Anforderungen an eine effektive IT-Sicherheit gewachsen ist?

nach persönlicher Kompetenz im Bereich IT-Sicherheit



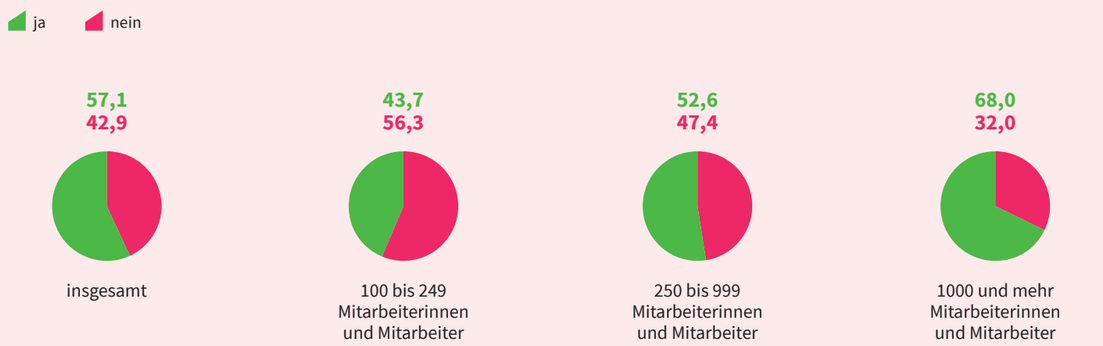
Quelle: Statista im Auftrag von G DATA

Zu unbekümmert

Einschätzung des eigenen Unternehmens als potenzielles Angriffsziel für Cyberkriminelle; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2024; in Prozent

Ist Ihr Unternehmen aus Ihrer Sicht ein interessantes Angriffsziel für Cyberkriminelle?

nach Unternehmensgröße

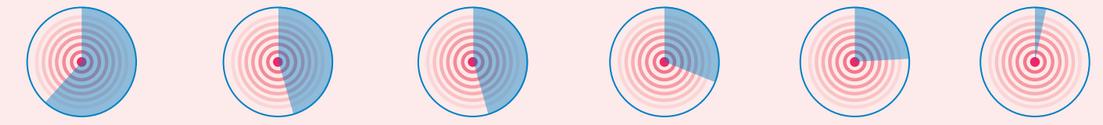


Quelle: Statista im Auftrag von G DATA

Zu naiv

Gründe für das Interesse von Cyberkriminellen am Unternehmen als Angriffsziel; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2024; in Prozent *

Warum ist Ihr Unternehmen aus Ihrer Sicht ein interessantes Angriffsziel für Cyberkriminelle? Unser Unternehmen …



* Mehrfachnennungen möglich. Quelle: Statista im Auftrag von G DATA

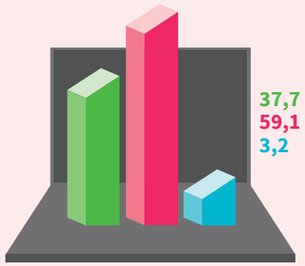
Erfahrungen

Erfahrungen mit Cyberangriffen innerhalb der vergangenen 2 Jahre; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2024; in Prozent

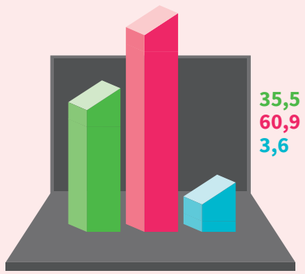
War Ihr Unternehmen in den vergangenen 2 Jahren von einem Cyberangriff betroffen?

nach Abteilungen

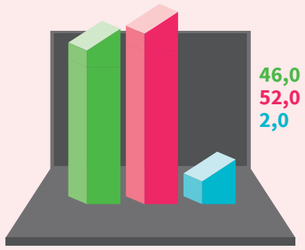
ja | nein | Ich weiß es nicht



insgesamt



IT und EDV*



IT-Security

* exklusive IT-Security. Quelle: Statista im Auftrag von G DATA

Maßnahmen

Ergriffene Maßnahmen zur Abwehr potenzieller Cyberangriffe; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die als Bereichsleitung, Abteilungsleitung oder Teamleitung in der IT-Security oder IT / EDV arbeiten; 2024; in Prozent *

Welche Maßnahmen haben Sie ergriffen, um sich auf potenzielle Cyberangriffe vorzubereiten?

59,1 Anti-Viren-Software

49,4 Multi-Faktor-Authentifizierung

49,0 Notfallplan und -übungen

46,2 Angriffs-Simulationen zur Überprüfung der Reaktion der Mitarbeiterinnen und Mitarbeiter

42,9 regelmäßige Penetrationstests

42,5 Durchführung von Security-Awareness-Trainings

35,2 Managed Security Services

30,8 Rahmenvereinbarung mit Incident-Response-Team

0,8 keine der genannten

* Mehrfachnennungen möglich. Quelle: Statista im Auftrag von G DATA

Auswahlkriterien

Kriterien bei der Auswahl von Dienstleistern bei IT-Sicherheitsvorfällen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die als Bereichsleitung, Abteilungsleitung oder Teamleitung in der IT-Security oder IT / EDV arbeiten; 2024; in Prozent *

Nach welchen Kriterien wählen Sie Ihre Dienstleister zur Behebung eines IT-Sicherheitsvorfalls aus?

53,0 Standort Deutschland

45,3 ISO-Zertifizierung

44,9 Verfügbarkeit eines 24/7-Supports für schnelle Reaktionszeiten

42,9 Qualifizierung der Mitarbeiterinnen und Mitarbeiter

41,7 ganzheitliches Angebot und umfassende Lösungen

33,6 Preis

28,3 Dienstleister steht auf der Liste der qualifizierten APT-Response-Dienstleister vom BSI.

25,9 Garantie, Daten nur im deutschen Rechtsraum zu verarbeiten

25,5 Empfehlung

1,6 keine der genannten

* Mehrfachnennungen möglich. Quelle: Statista im Auftrag von G DATA

Standortentscheidungen

Wichtigkeit des Standorts von Anbietern für IT-Sicherheitslösungen und für Managed Security Services; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die IT-Admin in der IT-Security oder IT / EDV sind oder die als Bereichsleitung, Abteilungsleitung oder Teamleitung in der IT-Security oder IT / EDV arbeiten; 2024; in Prozent

Wie wichtig ist es Ihnen, wo folgende Anbieter ihren Standort haben?

(sehr) wichtig | weniger / überhaupt nicht wichtig

Anbieter von IT-Sicherheitslösungen

59,7 | **13,3**

Anbieter von Managed Security Services

66,7 | **12,6**

Quelle: Statista im Auftrag von G DATA

Welchen IT-Sicherheitsanbieter würden Sie * bevorzugen?

51,8 einen deutschen IT-Sicherheitsanbieter

4,1 einen außereuropäischen IT-Sicherheitsanbieter

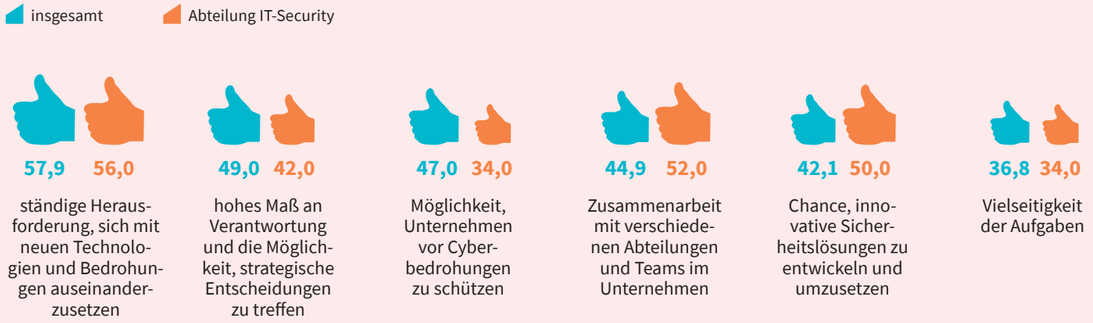
44,1 einen europäischen IT-Sicherheitsanbieter (ausgenommen Deutschland)

* Befragte, die IT-Admin in der IT-Security oder IT / EDV sind oder die als Bereichsleitung, Abteilungsleitung oder Teamleitung in der IT-Security oder IT / EDV , arbeiten und denen der Standort von Anbietern von IT-Sicherheitslösungen sehr wichtig oder wichtig ist. Quelle: Statista im Auftrag von G DATA

Das freut

Positives am Job eines IT-Security-Verantwortlichen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die als Bereichsleitung, Abteilungsleitung oder Teamleitung in der IT-Security oder IT / EDV arbeiten; 2024; in Prozent *

Was ist aus Ihrer Sicht das Beste am Job eines IT-Security-Verantwortlichen?

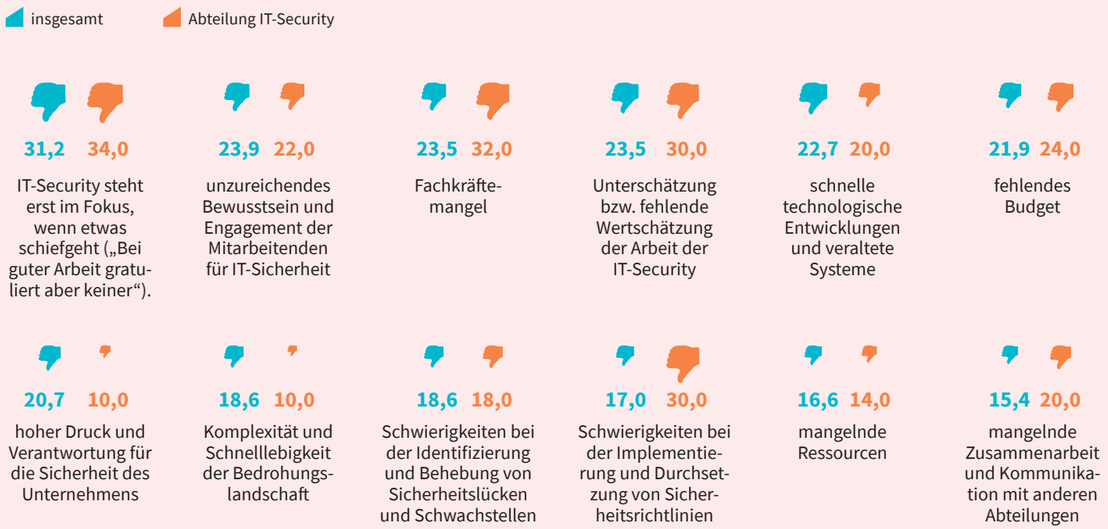


* Mehrfachnennungen möglich. Quelle: Statista im Auftrag von G DATA

Das ärgert

Herausforderungen und Ärgernisse im Job eines IT-Security-Verantwortlichen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die als Bereichsleitung, Abteilungsleitung oder Teamleitung in der IT-Security oder IT / EDV arbeiten; 2024; in Prozent *

Was sind aus Ihrer Sicht die größten Ärgernisse im Job eines IT-Security-Verantwortlichen?

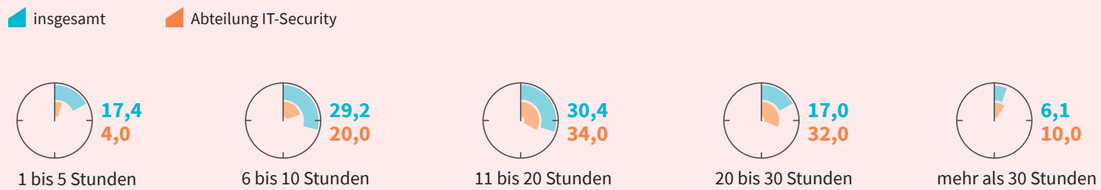


* Mehrfachnennungen möglich (max. 3 Antworten). Quelle: Statista im Auftrag von G DATA

Das braucht

Aufgewendete Arbeitszeit pro Woche für Tätigkeiten im Bereich IT-Sicherheit; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die als Bereichsleitung, Abteilungsleitung oder Teamleitung in der IT-Security oder IT / EDV arbeiten; 2024; in Prozent

Wie viel Ihrer Arbeitszeit wenden Sie pro Woche für den Bereich IT-Security auf?

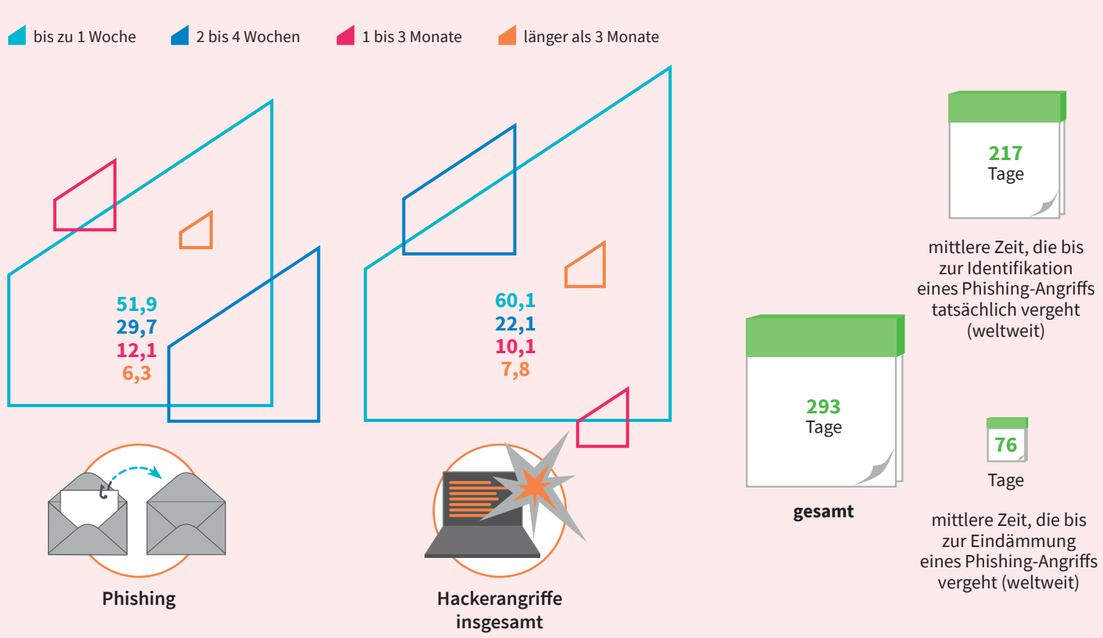


Quelle: Statista im Auftrag von G DATA

Das dauert

Einschätzung der Zeit zwischen einem Cyberangriff und dessen spürbaren Auswirkungen in Unternehmen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2024; in Prozent

Zwischen einem Hackerangriff und den spürbaren Auswirkungen vergeht einige Zeit. Was glauben Sie, wie lange die folgenden Dinge in Unternehmen im Durchschnitt unbemerkt bleiben?



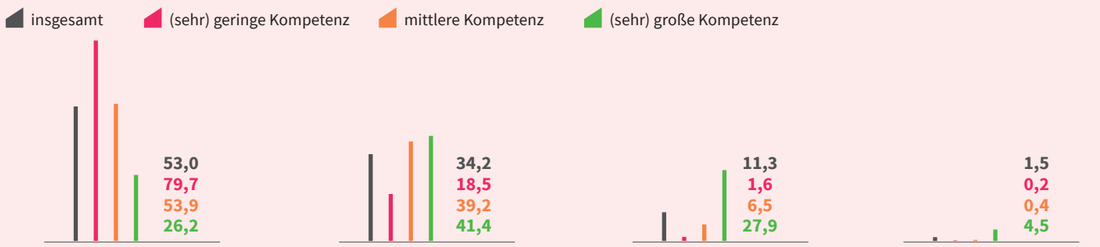
Quellen: Statista im Auftrag von G DATA, IBM

KI-Kompetenzen

Wissensstand zu künstlicher Intelligenz; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2024; in Prozent

Wie bewerten Sie Ihren Wissensstand zu künstlicher Intelligenz und deren Nutzungsmöglichkeiten in Ihrem Unternehmen?

nach persönlicher Kompetenz im Bereich IT-Sicherheit



Grundlegend: Ich habe ein grundlegendes Verständnis, bin aber noch nicht aktiv in Projekten oder der Entwicklung von KI-Lösungen involviert.

Durchschnittlich: Mein Wissen ist begrenzt, aber ich arbeite aktiv daran, Möglichkeiten für den KI-Einsatz in unserem Unternehmen zu entwickeln.

Fortgeschritten: Ich habe umfangreiche Erfahrungen und konnte bereits an Projekten mitarbeiten und KI-basierte Lösungen einsetzen.

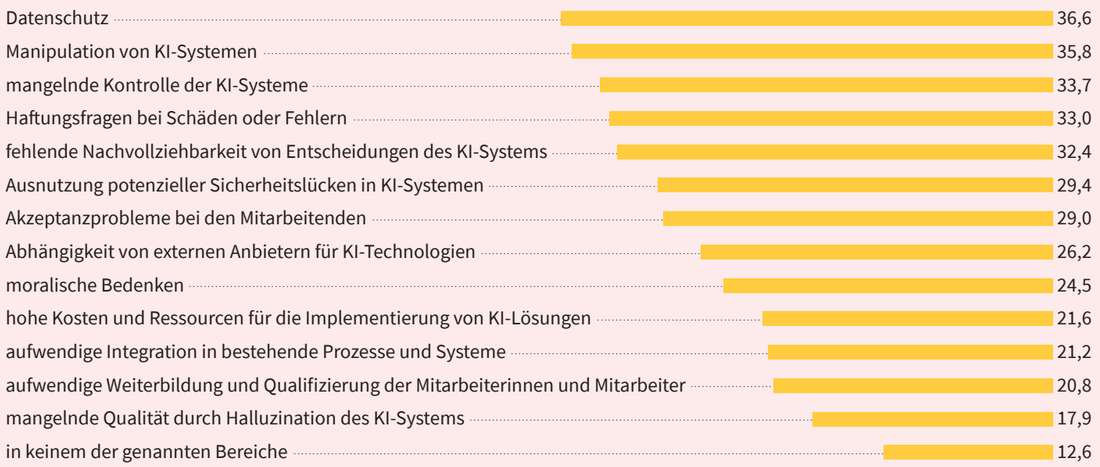
Experte: Ich habe tiefgreifendes Fachwissen und leite oder führe KI-Projekte in unserem Unternehmen.

Quelle: Statista im Auftrag von G DATA

KI-Bedenken

Bedenken bezüglich des KI-Einsatzes; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2024; in Prozent *

In welchen Bereichen haben beziehungsweise hätten Sie Bedenken bezüglich des KI-Einsatzes in Ihrem Unternehmen?

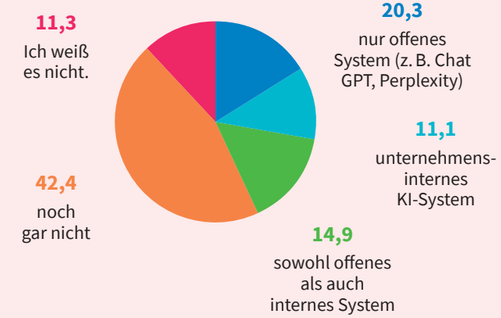


* Mehrfachnennungen möglich. Quelle: Statista im Auftrag von G DATA

KI-Anwendungen

Anwendung von KI in der täglichen Arbeit; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2024; in Prozent

In welcher Form wenden Sie KI für Ihre tägliche Arbeit an?

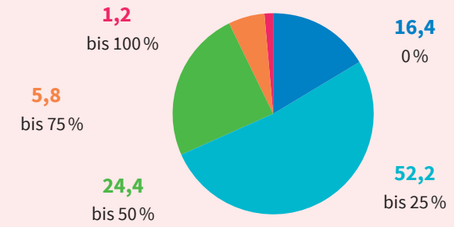


Quelle: Statista im Auftrag von G DATA

KI-Entwicklungen

Anteil der Arbeit, der in den nächsten 5 Jahren von einer KI übernommen werden könnte; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2024; in Prozent

Wie viel Prozent Ihrer täglichen Arbeit könnte in den nächsten 5 Jahren von einer KI übernommen werden?

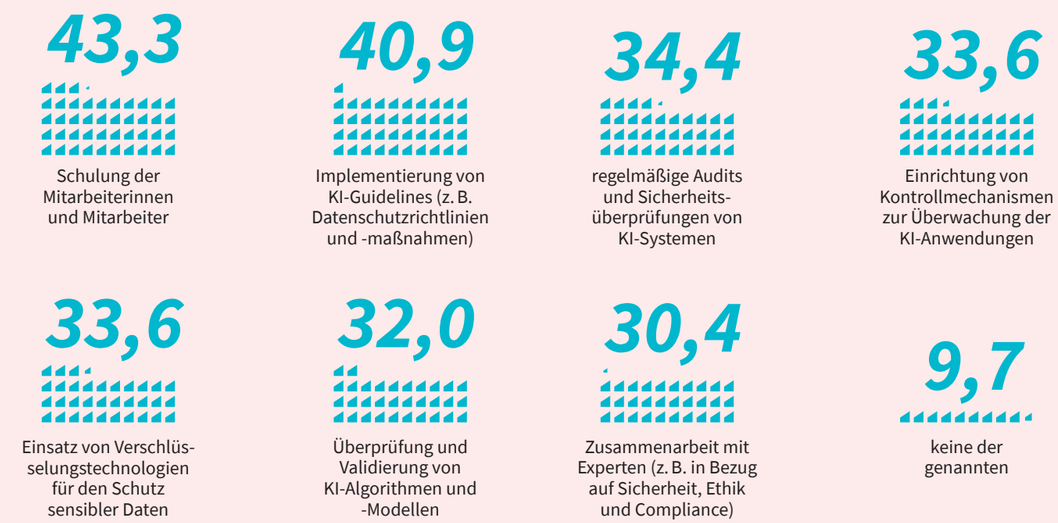


Quelle: Statista im Auftrag von G DATA

KI-Sicherheitsmaßnahmen

Maßnahmen zur sicheren Anwendung von KI; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die als Bereichsleitung, Abteilungsleitung oder Teamleitung in der IT-Security oder IT / EDV arbeiten; 2024; in Prozent *

Welche Maßnahmen zur sicheren Anwendung von KI werden in Ihrem Unternehmen angewendet?



* Mehrfachnennungen möglich. Quelle: Statista im Auftrag von G DATA

Eher ahnungslos

Betroffenheit von NIS-2-Richtlinie; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2024; in Prozent

Voraussichtlich ab Ende 2024 gilt für viele Unternehmen und Organisationen die NIS-2-Richtlinie (Network-and-Information-Security-Richtlinie) und damit verpflichtende Sicherheitsmaßnahmen und Meldepflichten, die auf ein besseres gemeinsames Cybersicherheitsniveau in der EU abzielen sollen. Ist Ihr Unternehmen davon betroffen?

Quelle: Statista im Auftrag von G DATA

Eher uninformiert

Gründe für Nichtbetroffenheit von der NIS-2-Richtlinie; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die von der NIS-2-Richtlinie nicht betroffen sind; 2024; in Prozent *

Warum denken Sie, dass Sie nicht von der NIS-2-Richtlinie betroffen sind?

* Mehrfachnennungen möglich. Quelle: Statista im Auftrag von G DATA

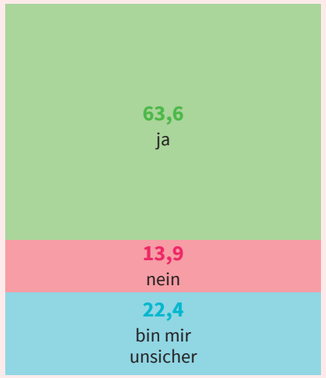
Eher zuversichtlich

Umsetzung der NIS-2-Richtlinie im Unternehmen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die von der NIS-2-Richtlinie betroffen sind; 2024; in Prozent

Wie gestaltet sich die Umsetzung der NIS-2-Richtlinie in Ihrem Unternehmen bisher?

Sehr herausfordernd: Es gibt noch viele offene Fragen bezüglich der konkreten Umsetzung der Richtlinie in unserem Unternehmen.	5,1
Herausfordernd: Es erfordert eine umfassende Überarbeitung unserer IT-Sicherheitsmaßnahmen und Prozesse.	16,5
Eher herausfordernd: Wir müssen zusätzliche Ressourcen und Expertise einsetzen, um den Anforderungen der NIS-2-Richtlinie gerecht zu werden.	36,6
Nicht besonders herausfordernd: Wir haben bereits robuste IT-Sicherheitsmaßnahmen implementiert, die weitgehend den Anforderungen der Richtlinie entsprechen.	30,3
Überhaupt nicht herausfordernd: Die Umsetzung der NIS-2-Richtlinie ist für uns unkompliziert, da wir bereits über die nötigen Strukturen und Prozesse verfügen.	11,4

Was schätzen Sie: Wird Ihr Unternehmen bis Ende des Jahres alle Kriterien der NIS-2-Richtlinie erfüllt haben?

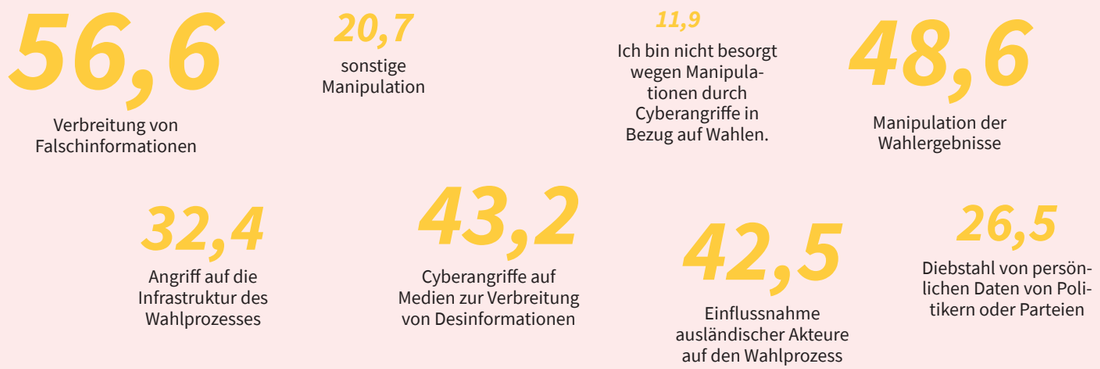


Quelle: Statista im Auftrag von G DATA

Eher besorgt

Sorgen bezüglich Manipulationen bei Wahlen durch Cyberangriffe; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2024; in Prozent *

Welche Art von Manipulationen durch Cyberangriffe bereitet Ihnen die größten Sorgen in Bezug auf Wahlen?



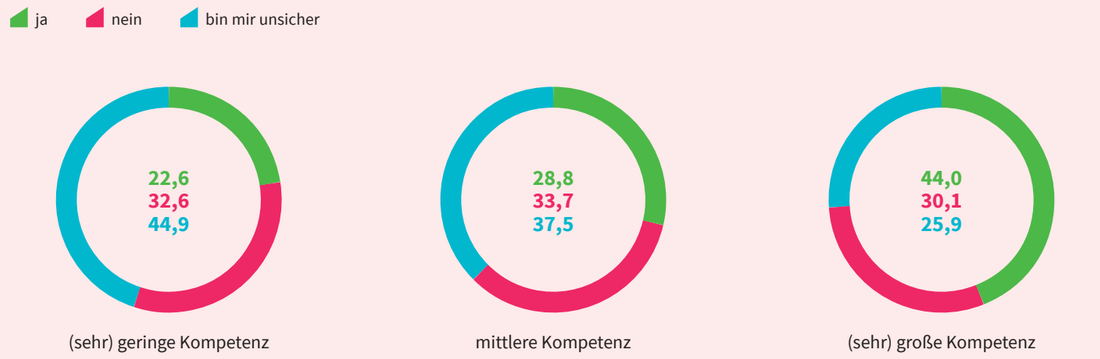
* Mehrfachnennungen möglich. Quelle: Statista im Auftrag von G DATA

Eher vertrauensvoll

Vertrauen in Sicherheitsmaßnahmen durch deutsche Behörden; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2024; in Prozent *

Haben Sie Vertrauen in die Sicherheitsmaßnahmen, die von den deutschen Behörden ergriffen werden, um z. B. Bundestagswahlen vor Cyberangriffen zu schützen?

nach persönlicher Kompetenz im Bereich IT-Sicherheit



* exklusive IT-Security. Quelle: Statista im Auftrag von G DATA

Die Hüterin

Sandra Heger ist eine CISO – Chief Information Security Officer. Im neuen Netzwerk Informationssicherheit der Hochschulen Nordrhein-Westfalens hilft sie, landesweit Daten und IT der Wissenschaftsbetriebe zu schützen. Zuvor verantwortlich an der Hochschule Ruhr West hat sie erfahren, wie wichtig das ist: Anfang 2023 konnten sie und ihr Team einen schweren Hackerangriff abwehren.

Text: Christoph Koch

„Genauer möchte ich es nicht sagen" – nämlich wie die Angreifer am 31. Januar 2023 in die IT der Hochschule Ruhr West eingedrungen sind. Sicherheitsmanagerin Sandra Heger will niemanden auf Ideen bringen. Und erst recht nichts über ihre erfolgreiche Abwehrstrategie preisgeben.

Als ich einen Interviewtermin mit Sandra Heger vereinbaren möchte, bekomme ich sehr schnell einen Eindruck von dem speziellen Mindset einer CISO: Obwohl ich mit meiner Mailadresse von brand eins anfrage und wir einen Tag später auch per Mobilnummer telefonieren, ruft sie noch einmal im Verlag in Hamburg an. Ob ein Beitrag über sie geplant sei und meine Anfrage tatsächlich von der Redaktion stamme? „Vertrauen ist gut, Kontrolle ist besser", sagt eine Redensart. Sie wird meist dem russischen Revolutionär Lenin zugeschrieben. Nach dem ersten Kontakt mit Sandra Heger bin ich mir ziemlich sicher, dass Lenin den Satz während der Oktoberrevolution von seinem Chief Information Security Officer aufgeschnappt hat.

„Es mag überskeptisch oder sogar leicht paranoid wirken, dass ich noch einmal nachgefragt habe", sagt Sandra Heger, 34, mit einem vergnügten Lächeln, als wir uns ein paar Wochen später auf dem Campus der Hochschule Ruhr West in Mülheim treffen. „Aber wenn jemand hier persönlich vorbeikommen und mich ausfragen möchte, könnte das theoretisch auch dazu dienen, eventuelle Schwachstellen auszuspähen." Mail-Absender lassen sich tatsächlich fälschen, und ein paar Informationen über einen legitim klingenden Rechercheauftrag wären von jemandem, der Böses will, auch schnell zusammengegoogelt. So gesehen also keine Paranoia, sondern eine sinnvolle zusätzliche Sicherheitsstufe. Die man vielleicht viel öfter einziehen sollte. „Viele Phishing- oder Scam-Versuche ließen sich mit einem einzigen Anruf verhindern", sagt Heger. „Einfach bei der Bank anrufen, die angeblich kurz davor ist, das Girokonto zu sperren. Natürlich nicht unter der Nummer, die in der Mail steht, sondern unter der von der Webseite der Bank."

Einen offenen Campus effektiv einhegen

Das Berufsbild des Chief Information Security Officers ist vergleichsweise neu. Erst in den vergangenen zwei bis drei Jahrzehnten hat sich der Job zu einer zentralen Führungsaufgabe entwickelt, die weit über rein technische Aspekte hinausgeht. Meist denkt man an die Entwicklung und Implementierung von IT-Sicherheitsvorkehrungen, wenn von CISOs die Rede ist. An Schulungen, Firewalls (siehe Glossar) und nervende Erinnerungen, sein Passwort bitte nicht auf einem Post-it an den Büro-Monitor zu kleben. Aber den CISOs obliegt auch der Schutz physischer Dokumente und die generelle Frage, wie Räumlichkeiten abzusichern sind, in denen sich Dokumente befinden – ganz egal ob auf Papier oder auf Festplatten.

Sandra Heger muss sich als CISO für Hochschulen beispielsweise auch um Klausuren Gedanken machen, die auf Papier geschrieben und aufbewahrt werden. Oder um den Zugang zu Hörsälen, Labors oder Archiven. „Eine Hochschule mit Studierenden, die kommen und gehen, ist ein sehr offenes Umfeld", sagt sie. „Zumindest verglichen mit Firmen, die häufig gleich am Eingang eine Rezeption haben, die niemanden ohne Hausausweis oder bestätigten Termin reinlässt." Gleichzeitig gibt es aber auch Bereiche, in denen das Kommen und Gehen sehr streng geregelt werden muss: Labors beispielsweise, in denen hochsensible Forschung stattfindet oder ein leistungsstarker Laser herumsteht.

Die CISO einer Hochschule ist also nicht nur dafür zuständig, nach welchem Standard die digitalen Backups verschlüsselt werden – sondern auch ganz banal dafür, wer welchen Schlüssel für welche Türen bekommt. Wenn sie Kindern erklären will, was sie beruflich macht, fragt sie die stets, ob sie Geheimnisse hätten. „Und Kinder haben natürlich alle Geheimnisse", weiß Heger. „Ich erkläre ihnen dann, dass es mein Beruf ist, diese Geheimnisse von Menschen zu schützen und zu bewahren. Auch wenn das nur ein Teilbereich meiner Arbeit ist."

Schlüssel und Verschlüsselung

Da der digitale Anteil unserer Geheimnisse ständig größer wird, haben die meisten CISOs einen IT-Hintergrund. Auch Sandra Heger hat Informatik studiert – und war damals in vielen Vorlesungen und Seminaren die einzige Frau. „Frauen sind in der Informatik immer noch eine große Ausnahme", sagt sie. „Bei mir war ein Informatiklehrer in der Schule entscheidend. Er nahm mein Interesse an dem Fach ernst und ermutigte mich, es zu studieren." Sie startete ihre Karriere an der Hochschule Ruhr West zunächst im Campus-Management, „aber immer schon an den Schnittstellen von IT zu anderen Themen". Informationssicherheit war damals – wie in vielen Organisationen – noch eine von mehreren Unteraufgaben der regulären IT-Administration. Als 2022 feststand, dass die Menge der Arbeit eine dezidierte CISO-Stelle rechtfertigt, fiel die Wahl auf Heger.

„Als CISO hat man vor allem strategische Aufgaben", sagt sie. „Wie setzen wir welche Sicherheitsstandards um, wie priorisieren und steuern wir einzelne Themen?" Um die klassische Phishing-Mail oder die Rechner im PC-Pool der Hochschule kümmert sich nach wie vor die IT-Abteilung. Ihr Beruf erfordere vor allem gute Kommunikationsfähigkeiten und Fingerspitzengefühl: „An einer Hochschule, aber auch in Unternehmen hat man es als CISO mit extrem unterschiedlichen Gruppen zu tun, die teilweise ganz unterschiedliches Hintergrundwissen mitbringen." Alle gilt es mitzunehmen. Man muss von der Notwendigkeit von Schulungen also ebenso überzeugen können wie von wichtigen, aber häufig als umständlich wahrgenommenen Vorkehrungen wie der Zwei-Faktor-Authentifizierung.

„Natürlich sind grundlegende IT-Kenntnisse wichtig", sagt Heger, und das Informatik-Studium schade sicher nicht – es sei aber nicht zwingend Voraussetzung für die Position. „Gerade wenn es darum geht, Sicherheitsstandards umzusetzen, wie sie etwa vom Bundesamt für Sicherheit in der Informationstechnik (BSI) oder anderen Stellen kommen, hat die Position auch schnell etwas von klassischem Projektmanagement."

Denn eines ist klar: Die Angriffe werden häufiger und ausgebuffter. Und sie sind längst nicht mehr hoch spezialisierten Hackern vorbehalten. Im Darknet kann man sich sofort einsatzfähige Ransomware-Sets bestellen, mit denen sich fremde Daten verschlüsseln lassen, wenn sie nicht gut genug abgesichert sind. Entschlüsselung dann nur gegen entsprechendes Lösegeld, gern in Bitcoin, beehren Sie uns bald wieder! ›

Mit generativer KI lassen sich Phishing-Mails in einem Bruchteil der Zeit verfassen, und das ohne die üblichen verräterischen Fehler. Eine der neuesten Angriffsarten: Mithilfe von KI-Werkzeugen lässt sich die Stimme des CEOs oder eines Kollegen schon mit relativ wenig Ausgangsmaterial klonen. Dann folgt ein Anruf bei der Buchhaltung, bitte diesen oder jenen Betrag schnell anzuweisen. Oder die IT wird instruiert, die Firewall oder die Zwei-Faktor-Identifizierung für ein bestimmtes Gerät kurzzeitig zu deaktivieren, es gebe da ein kleines technisches Problem.

Vertraute Stimme, künstlicher Zeitdruck – wer denkt, er würde darauf unter gar keinen Umständen hereinfallen, sollte sich besser nicht zu sicher sein. 2023 lagen die direkt durch Cyberangriffe verursachten gesamtwirtschaftlichen Schäden laut Erhebung des Branchenverbandes Bitkom bei 148 Milliarden Euro. 58 Prozent der deutschen Unternehmen gaben 2023 an, in den vorangegangenen zwölf Monaten Ziel eines Angriffs gewesen zu sein. Und: Mittlerweile ist bereits jede Hochschule in Nordrhein-Westfalen Opfer einer Cyberattacke geworden. Zwar ist nicht jeder Angriff erfolgreich, aber Hoffnung allein reicht als Verteidigungsmaßnahme ebenso wenig aus wie der Glaube, man sei als kleine Organisation doch gar nicht interessant genug für kriminelle Hacker.

Alarm im War Room

Wie schnell es gehen kann, erfuhr Sandra Heger am 31. Januar 2023. Das Datum kommt wie aus der Glasfaserleitung geschossen, als ich sie danach frage. „Den Tag vergesse ich so schnell nicht mehr“, sagt sie. Ein Mitarbeiter habe „verdächtiges Verhalten“ im System bemerkt. Dass das so vage klingt, ist Absicht. „Genauer möchte ich es nicht sagen“, sagt Heger diplomatisch. Sie will niemanden auf Ideen bringen – vor allem aber auch keine Einblicke gewähren, wie eine IT-Verteidigungsriege in solchen Fällen vorgeht. Was sie sagen kann: „Wir haben das Netzwerk der Hochschule vom Internet getrennt und begonnen, den Vorfall zu untersuchen“ – was keine Maßnahme sei, die man mal eben so ergreift, weil ein Drucker sich eigenartig verhält. Sie beauftragten dafür das „Incident Response Team“ von G DATA Advanced Analytics. Während die Spezialisten sofort mit der IT-Forensik begannen, passierten gleichzeitig sofort andere Dinge, erzählt Heger: „Der Krisenstab trat zusammen. Wir informierten die Hochschulangehörigen über den Vorfall und natürlich die Ermittlungsbehörden.“

Der Raum, in dem wir das Gespräch führen, ein Konferenzzimmer im dritten Stock mit Blick auf ein begrüntes Flachdach, wurde zum War Room umfunktioniert. „Hier saßen sechs bis acht Kolleginnen und Kollegen aus der IT, und es sah aus wie früher bei einer LAN-Party mit den ganzen Kabeln auf dem Tisch.“ Ein Gebäude weiter tagte unterdessen der Krisenstab mit Abgesandten aller Hochschulgruppen. Dort wurden zum einen Prioritäten gesetzt, also welche Systeme beispielsweise zuerst wieder in Betrieb genommen werden sollten. Zum anderen fand dort auch die Krisenkommunikation nach außen hin statt. Denn spätestens, als sich Hegers Team entschied, die Hochschule vom Netz zu nehmen, war klar, dass sich der Vorfall nicht diskret und im Hintergrund lösen ließ. Studierende, Belegschaft, Kooperationspartner, Kultusministerium – alle wollten und mussten wissen, was los war. „Die Präsidentin gab beispielsweise jeden Tag per Videobotschaft ein kurzes Update“, sagt Heger. „Das kam sehr gut an. Hier wiederum saß die IT, konnte die Tür zumachen und sagen: Stört uns einfach nicht bei unserer Arbeit.“

Es dauerte Tage, bis Hegers Team das Geschehen komplett rekonstruiert hatte und wirklich sicher war, den Angriff erfolgreich abgewehrt zu haben. Ein kompletter Reset aller Passwörter läutete danach so etwas wie eine erste Stufe der wiederhergestellten Normalität ein. Bis dahin vergingen jedoch Wochen. Das hing auch damit zusammen, dass das Team die Gelegenheit nutzte, ein paar grundsätzliche Änderungen in der IT-Infrastruktur vorzunehmen, die ohnehin geplant waren. „Ich kann natürlich nicht laut sagen, dass mir die Sache letztlich auch Spaß gemacht hat“, sagt Heger und sieht so aus, als sei genau das der Fall gewesen. „Aber es war auf jeden Fall eine interessante Zeit.“

Weil der Vorfall schnell entdeckt wurde und die Hochschule entschlossen gehandelt hatte, konnte Sandra Heger am Ende aufatmen, dass keine Daten „abgeflossen“ waren, wie man in der Branche sagt. Von den Tätern wurde nichts verschlüsselt, es gab keine Erpressungsversuche. „Aber es deutete alles darauf hin, dass es auf einen Ransomware-Angriff hinausgelaufen wäre“, sagt die CISO.

Andere Hochschulen hatten weniger Glück: Die Universität Gießen beziffert den Schaden eines Angriffs im Jahr 2019 auf 1,7 Millionen Euro. Wenn eine Datenschutzverletzung vorliegt und Organisations- und Nutzerdaten im Darknet landen wie bei der Universität Duisburg-Essen Ende 2022 (siehe Kasten), ist der Schaden kaum noch zu beziffern.

Ein Vorteil der Hochschule Ruhr West bei dem Angriff war ihre vergleichsweise zentralisierte IT-Architektur: „Je größer und älter eine Hochschule ist, desto dezentraler ist meist die IT organisiert“, sagt Heger. „Dann gibt es hier ein Rechenzentrum, da die Verwaltungs-IT, dort haben die Mathematiker ihr eigenes System und so weiter und so fort. Da ist teilweise über Jahrzehnte eine dezentrale Struktur entstanden, die es schwieriger macht, schnell und geschlossen zu reagieren.“ Auch Unternehmen hätten oft den Vorteil einer zentralisierten Architektur.

Routinen gegen den Ernstfall

Doch egal wie dramatisch solche Tage im Krisenmodus sein mögen – sie sind die Ausnahme für CISOs. Vieles ist Routine, Vorbereitung, Beratung, um zu verhindern, dass es überhaupt zum Ernstfall kommt. Einen typischen Tagesablauf hat es dennoch nicht gegeben, so Heger. Sie hat regelmäßig beobachtet, welche Software-Schwachstellen die InfoSec-Community entdeckte und wofür es bereits „Patches“ gab: Vor welchen Angriffswellen warnt das Bundesamt für Sicherheit in der Informationstechnik (BSI)? Wie könnte das die Hochschule betreffen? Sie hat sich regelmäßig mit anderen CISOs ausgetauscht. Auf NRW-Ebene gibt es die Landesarbeitsgruppe Informationssicherheit, in der alle CISOs der NRW-Hochschulen mitwirken. „Hochschulen konkurrieren tendenziell weniger miteinander als Unternehmen aus einer Branche. Deshalb tauschen wir uns intensiv aus: Was funktioniert bei euch, was können wir übernehmen?“

Jetzt Netzwerkerin für ganz Nordrhein-Westfalen

Ihr Engagement als Mitglied im dort gewählten Sprecherteam dürfte sie auch auf ihren neuen Posten geführt haben: Seit Kurzem ist Heger aufgestiegen zur stellvertretenden Leiterin des Netzwerks Informationssicherheit der Hochschulen in NRW (NISHS.nrw). Ziel des Netzwerks, das gerade neu aufgebaut wird, ist es, die Informationssicherheit und den Datenschutz aller Hochschulen im Bundesland zu stärken. Dazu übernimmt es die Funktion einer Beratungs- und Koordinierungsstelle, um den Austausch zwischen den Wissenschaftsbetrieben zu fördern und gemeinsame Projekte voranzubringen.

Nordrhein-Westfalen folgt damit dem Vorbild anderer Bundesländer wie Bayern und Baden-Württemberg, die bereits zentrale Stellen für Cybersicherheit an Hochschulen aufgebaut haben. Sie werden von den Landesregierungen finanziert und unterstützen im Fall von Attacken. Sie halten zentrale Sicherheits-Tools bereit und koordinieren Rahmenverträge mit IT-Dienstleistenden. Zusätzlich baut das Deutsche Forschungsnetz (DFN), über dessen Glasfasernetz die meisten deutschen Hochschulen ihren Internetzugang beziehen, seine Sicherheitsdienstleistungen für Hochschulen nach und nach weiter aus.

„Man darf als CISO nicht darauf hoffen, irgendwann fertig zu sein“, sagt Sandra Heger, nach wichtigen Eigenschaften gefragt, die man für den Beruf mitbringen sollte. „Selbst wenn man ein Sicherheitsproblem gut gelöst hat – die Gegebenheiten ändern sich ständig, und es kommen immer wieder neue Angriffsvektoren dazu.“ Unter anderem darüber tauscht sie sich im bundesweiten Arbeitskreis Informationssicherheit der „Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung“ aus.

Und man müsse damit umgehen können, große Verantwortung zu tragen, sagt Heger. Zwar liege die formal am Ende bei den Hochschulleitungen, „aber natürlich fühle ich mich dafür verantwortlich, dass unsere Informationen sicher sind“.

Manche CISO-Kolleginnen und -Kollegen beklagen, mit ihren Warnungen (an denen oft auch die Budgets hängen), nicht ernst genommen zu werden. Das klassische Präventionsparadox: Solange alles gut abgesichert ist und nichts passiert, lässt sich der Schutz als Kostenfaktor leicht infrage stellen – genau deshalb, weil nichts passiert. Sandra Heger hatte dieses Problem mit ihrem früheren Arbeitgeber nicht. „Die Hochschulleitung hatte auch schon vor dem Angriff 2023 ein offenes Ohr für die Informationssicherheit“, sagt sie. „Wirklich darum kämpfen, sinnvolle Maßnahmen umsetzen zu können, musste ich zum Glück nie.“

GROSSANGRIFFE AUF HOCHSCHULEN

Hochschulen sind ein beliebtes Ziel von Cyberangriffen. Einige Beispiele aus den vergangenen Jahren.

Mai 2020
Die Ruhr-Universität Bochum wird Ziel eines Cyberangriffs, bei dem rund 60 Serversysteme verschlüsselt werden. Große Teile des Campus und der Verwaltung sind arbeitsunfähig, E-Mail-Kommunikation, Terminierung und Dateizugriffe sind nicht verfügbar. Auch zentrale Systeme der Personal-, Studierenden- und Finanzverwaltung sind betroffen.

Juni 2020
Einem Hacker gelingt es, die Server der School of Medicine der University of California San Francisco mit Ransomware zu verschlüsseln. Die Universität zahlt 1,14 Millionen Dollar Lösegeld, um wieder Zugriff auf ihre Daten zu erhalten.

April 2021
Aufgrund eines Angriffs auf die Systeme der Technischen Universität Berlin muss das komplette Netzwerk vorsorglich heruntergefahren werden.

September 2021
Bei einem Angriff mit Ransomware werden Festplatten des Leipziger Instituts für Medizinische Informatik, Statistik und Epidemiologie (IMISE) verschlüsselt.

November 2022
Angreifer legen mithilfe von Schadsoftware das komplette Telefon- und IT-System der Universität Duisburg-Essen lahm. Zudem werden Daten verschlüsselt und für die Entschlüsselung ein Lösegeld gefordert. Als die Universität nicht zahlt, werden einige der privaten Daten im Darknet veröffentlicht.

August 2023
Die University of Michigan wird Opfer eines Diebstahls von sensiblen persönlichen Daten von rund 230.000 Studierenden, Alumni, Patienten, Studienteilnehmenden und Mitarbeitenden – darunter Finanzinformationen und Gesundheitsdaten.

Februar 2024
Die Universitäten Manchester und Cambridge werden Opfer einer Denial-of-Service (DoS)-Attacke der Hackergruppe „Anonymous Sudan“. Die Gruppe hat bereits zahlreiche erfolgreiche Angriffe in aller Welt verübt und wird mit Russland in Verbindung gebracht.

März 2024
Die E-Klausuren-Plattform der Heinrich-Heine-Universität Düsseldorf wird gehackt. Neben Prüfungsfragen und -antworten werden 15.000 Datensätze von Studierenden sowie aus einem anderen Datensatz weitere 60.000 Nutzerdaten von Universitätsangestellten und Gästen erbeutet. Bereits im März 2023 waren rund 4.500 persönliche Datensätze durch unbefugten Zugriff gehackt worden.

G DATA INDEX – CYBERSICHERHEIT

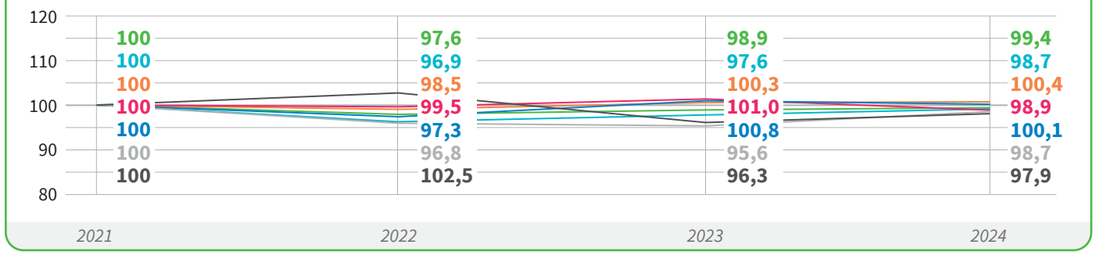
Die Bedrohung durch Cybercrime steigt seit Jahren und verursacht massive wirtschaftliche und gesellschaftliche Schäden. Kein Tag ohne neue Meldungen zu Hackerangriffen und Cyberattacken. Wie wirkt sich das aus? Wie sicher fühlen wir uns angesichts der latenten Bedrohung – beruflich und privat? Der G DATA Index gibt Auskunft.

Insgesamt eher unsicher – und wenig Gefühl für die Risiken

Index-Veränderung gegenüber dem Basisjahr 2021; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2024

Deutschland | männlich | weiblich | unter 30 Jahre | 30 bis 49 Jahre | 50 bis 64 Jahre | 65 Jahre und älter

Index



Lesehilfe:
Der Wert des Index im Jahr 2021 beträgt 100.
Ein Indexwert von mehr als 100 entspricht einem Anstieg gegenüber dem Wert des Jahres 2021 (z. B.: 103 = ein Anstieg um 3 %).
Ein Indexwert von unter 100 entspricht einem Rückgang gegenüber dem Wert des Jahres 2021 (z. B.: 98 = ein Rückgang um 2 %)

Was der Index bedeutet
Skala 0 bis 100:
100 = hohes Sicherheitsgefühl, hohe Wissenskompetenz und ein geringes Risikoempfinden
0 = geringes Sicherheitsgefühl, geringe Wissenskompetenz und hohes Risikoempfinden

Wonach wir fragen

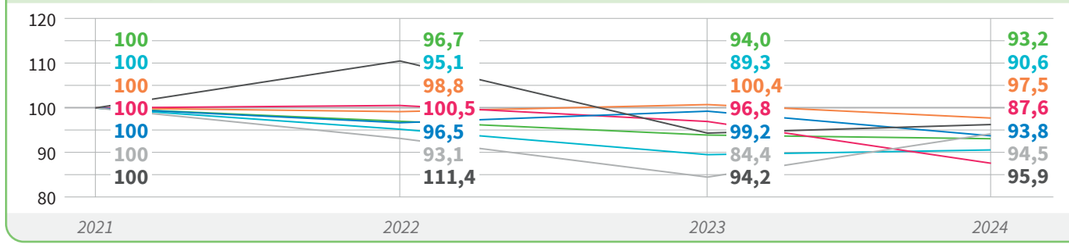
Wissen:
Wie schätzen Sie Ihre Kompetenz / Ihren Wissensstand zum Thema IT-Sicherheit ein?
Antworten auf einer Skala:
1 = sehr geringe Kompetenz,
5 = sehr große Kompetenz

Sicherheit:
Zu Hause und im Büro werden teils unterschiedliche IT-Sicherheits- und Schutzmaßnahmen angewendet. Wie gut fühlen Sie sich durch die angewendeten Sicherheits- und Schutzmaßnahmen in den beiden Lebensbereichen geschützt?
Antworten auf einer Skala:
1 = sehr schlecht, 5 = sehr gut

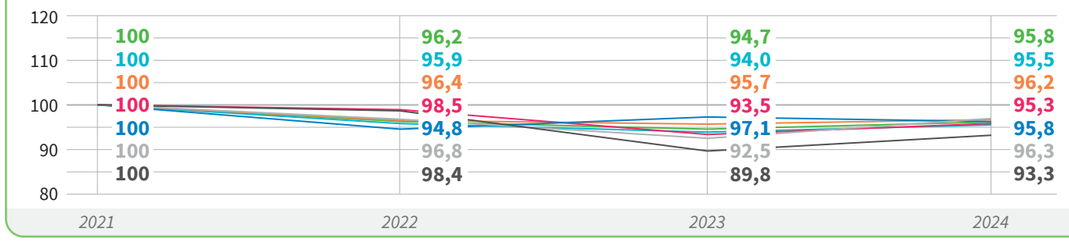
Risiko:
Wie hoch schätzen Sie das Risiko ein, Opfer von Cyberkriminalität oder Datenklau zu werden? (persönlich / beruflich)
Antworten auf einer Skala:
1 = sehr gering, 5 = sehr hoch

Quelle: Statista im Auftrag von G DATA

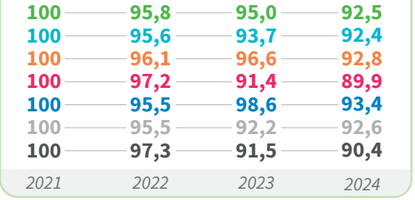
1 Wissenskompetenz Je höher der Wert, desto höher ist die empfundene Wissenskompetenz.



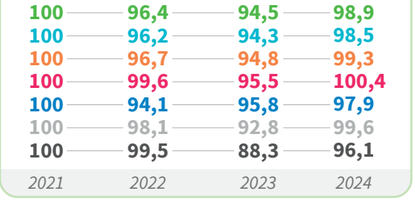
2 Sicherheitsgefühl gesamt Je höher der Wert, desto höher ist das Sicherheitsgefühl.



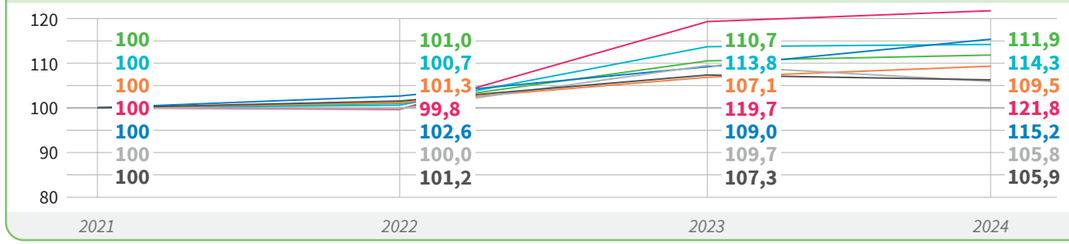
Sicherheitsgefühl privates Umfeld



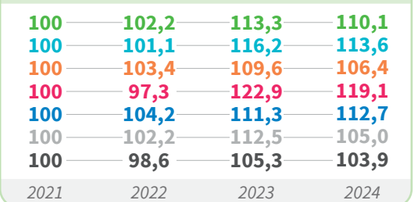
Sicherheitsgefühl berufliches Umfeld



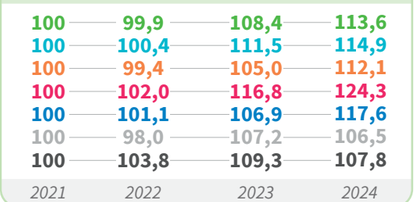
3 Risikoempfinden gesamt Je höher der Wert, desto geringer ist das Risikoempfinden.



Risikoempfinden privates Umfeld



Risikoempfinden berufliches Umfeld



What, the Hack!

Hacker können vieles:
Probleme machen, Probleme finden, Probleme lösen.
Ja, sie bringen auch Schlechtes –
aber vor allen Dingen bringen sie die Welt voran.

Text: Peter Lau


```
users = {
    „user1“: {„password“: „pass1“, „balance“: 1000},
    „user2“: {„password“: „pass2“, „balance“: 1500},
    „ccc“: {„password“: „cccpassword“, „balance“: 0}  # CCC-Konto
}

# Funktion zur Anmeldung
def login(username, password):
    if username in users and users[username][„password“] == password:
        return True
    return False

# Funktion zur Überweisung
def transfer_funds(sender, recipient, amount):
    if sender in users and recipient in users:
        if users[sender][„balance“] >= amount:
            users[sender][„balance“] -= amount
            users[recipient][„balance“] += amount
            return True
    return False

# Hauptprogramm
def main():
    print(„Willkommen beim Bildschirmtext-System (BTX)“)

    # Anmelden
    username = input(„Benutzername: „)
    password = input(„Passwort: „)

    if login(username, password):
        print(f“Willkommen, {username}!“)
        print(f“Ihr Kontostand: {users[username][‚balance‘]} DM“)

        # Überweisung
        recipient = input(„Empfänger: „)
        amount = float(input(„Betrag: „))

        if transfer_funds(username, recipient, amount):
            print(„Überweisung erfolgreich!“)
            print(f“Neuer Kontostand: {users[username][‚balance‘]} DM“)
        else:
            print(„Überweisung fehlgeschlagen. Überprüfen Sie die Empfängerdaten
und Ihren Kontostand.“)
    else:
        print(„Ungültige Anmeldedaten. Zugriff verweigert.“)

# Programm ausführen
if __name__ == „__main__“:
    main()
```

Quellcode: Chat GPT

Was ist ein Hacker? Da gibt es Menschen, die in Computer eindringen, weil sie Daten suchen, die sie stehlen können. Oder die Wege finden, um den Rechner zu verschlüsseln oder sein Netzwerk außer Betrieb zu setzen, um damit Lösegeld zu erpressen – das sind Hacker. Ebenso passend wäre zu sagen: Kriminelle.

Dann gibt es Menschen, die in Computer eindringen, um Sicherheitslücken zu finden und zu schließen, die Kriminelle nutzen könnten – auch das sind Hacker. Beziehungsweise: IT-Schützer.

Einige Menschen dringen in Computer ein, um Daten zu finden, mit denen sie Menschen schützen können, etwa im Kampf gegen Kriminelle oder in Kriegen, auch sie sind – Hacker. Und oftmals Beamte.

Und schließlich gibt es noch hackende Modelleisenbahner. Die haben das Hacking sogar erfunden.

Das war Anfang der Sechzigerjahre am Massachusetts Institute of Technology (MIT), als die Mitglieder des universitären Modelleisenbahn-Vereins Tech Model Railroad Club (TMRC) einen Weg suchten, um ihre gigantische Anlage zu automatisieren – es war zu mühselig, die vielen Züge und Signale von Hand zu bedienen. Mit dem Computer der Universität wäre das ein Klacks gewesen, aber Rechner waren damals nicht nur riesig, sondern auch selten, teuer und begehrt. Zeit an den Maschinen bekamen deshalb nur wichtige Projekte. Also mussten sich die jungen Männer etwas anderes einfallen lassen. Und das nannten sie „Hacks“. So wurden sie zu den ersten Hackern der Welt.

Sie waren also ganz normale Studenten, doch mit den Jahren entwickelten sich viele von ihnen zu Erbauern, Entwicklern und Innovatoren der digitalen Welt: Alan Kotok wurde Mitglied des „World Wide Web Consortium“, das bis heute die Standards des Internets entwickelt. John McCarthy war ein Begründer des Forschungszweigs künstliche Intelligenz. Sein Kommilitone Steve Russell entwickelte das erste professionell vertriebene Videospiel „Spacewar!“. Und Richard Greenblatt, der das erste Schachprogramm entwarf, das Turniere spielte, gilt als ein Begründer der Hacker-Community. Im Rückblick scheint es, als hätte sich zufällig eine Gruppe Hochbegabter getroffen und dabei das Hacking erfunden. Aber vielleicht ist es genau umgekehrt – und diese Männer und diverse andere Kommilitonen wurden zu IT-Innovatoren, gerade weil sie Hacker waren. Denn Hacking ist zuerst einmal eine Art des Denkens.

Frühwarnung vom Urvater

Ein Hacker sei jemand, der Würstchen in der Kaffeemaschine warm macht, wenn er keinen Topf hat, soll Wau Holland gesagt haben, der Urvater der deutschen Hackerszene. Holland und andere Hacker seiner Generation waren nicht nur einfallsreich, sondern in den Achtzigern die ersten kritischen Beobachter der fortschreitenden Digitalisierung. Sie warnten schon damals vor den Gefahren für die Datensicherheit und durch die Datenfreiheit. Heute würden sie Hacktivisten genannt werden.

Um ihren Argumenten Gewicht zu verleihen, verübten sie selber Hacks, die zeigen sollten, wie anfällig viele Systeme waren: 1984 drangen Holland und sein Kollege Steffen Wernéry in das Bildschirmtext-System (BTX) ein, jenes ersten Online-Angebots der staatlichen Bundespost, das Telefon und Fernsehen interaktiv vernetzt hatte. Damit zeigten sie zum ersten Mal öffentlich in Deutschland, wie anfällig Daten in Netzwerken sein können.

Klone, Trojaner und ein Einbruch bei der Nasa

Solche Aktionen gab es hierzulande immer wieder: 1987 drangen deutsche Hacker in ein von der Nasa betriebenes System ein. 1997 zeigten sie, wie sich Mobilfunkkarten klonen lassen. 2006 demonstrierten sie, dass sich Wahlcomputer manipulieren lassen. 2011 veröffentlichten sie den „Staatstrojaner“, eine staatliche Spionagesoftware.

Die meisten dieser Aktionen münden in eine „Responsible Disclosure“: Werden Schwachstellen gefunden, informieren die Hacker den Hersteller und geben ihm eine gewisse Frist, um das Problem zu beheben oder zumindest darauf zu reagieren. Im Gegensatz dazu steht die „Full Disclosure“, wo alle Funde sofort veröffentlicht werden. Das kann ethisch und juristisch allerdings sehr heikel sein, zum Beispiel wenn es um potenziell gefährliche Maschinen wie Waffen geht. Oder um weitverbreitete Systeme und Programme, deren Ausfall bei einem Angriff massive Schäden verursachen kann.

Hacker, die ohne Erlaubnis in ein System eindringen, aber grundsätzlich gute Absichten hegen, werden „Grey Hats“ genannt, Grauhüte. Daneben gibt es „White Hats“, Hacker, die im Auftrag von Unternehmen und Organisationen in Computer eindringen, um die Systemsicherheit zu überprüfen. Und Cyberkriminelle heißen „Black Hats“. Lange war das Bild des Hackers vor allem von den „Grey Hats“ geprägt – und von Kids, die aus Spaß irgendwo eindringen, ohne zu wissen, was sie tun. Der Hollywood-Film „War Games“, in dem ein jugendlicher Hacker fast einen Atomkrieg auslöst, hinterließ dabei im kollektiven Bewusstsein eine tiefe Spur.

Inzwischen aber stehen die „Black Hats“ im Fokus, was auch ein Symptom für den durchschlagenden Erfolg der Digitalisierung ist. Ihre kriminellen Raubzüge sind nur deshalb möglich, weil die Welt vernetzt, der Geldverkehr weitgehend digitalisiert und Unternehmen von Daten abhängig sind, beziehungsweise Daten den Kern ihres Geschäftsmodells bilden. Es heißt, jede größere kriminelle Vereinigung, von der Mafia bis zu den Triaden, betreibt inzwischen Cyberkriminalität. Das ist nicht überprüfbar, aber realistisch, denn der Bereich ist lukrativ: Betrug der Umsatz im Drogenhandel 2023 weltweit rund 500 Milliarden Dollar, lag – allein in Deutschland – der Schaden durch Cyberkriminalität 2023 bei 148 Milliarden Euro! Ein erheblicher Teil dieser Summe beziffert zwar Betriebsausfälle, die Kriminellen kein Geld einbringen, aber auch sie nützen ihnen – als der Wirtschaft angsteinflößende Beispiele.

Zudem stehen dem Versprechen eines potenziell hohen Gewinns Investitionen gegenüber, die sich im Vergleich zu anderen Verbrechen in Grenzen halten: Wer Drogen schmuggeln will, braucht eine Lieferkette, an der zahllose Menschen

Foto: Wikipedia / Computer History Museum

Oben: Konsolen aus der Cybersteinzeit: Gordon Bell (l.) und Alan Kotok spielen 1964 am PDP-6 ihr eigenes Spiel. Unten spielen Dan Edwards (l.) und Peter Samson 1962 „Spacewar!“, eines der ersten Videospiele für Computer.

mitverdienen, von den Kurieren bis hin zu korrupten Staatsdienern. Für Cyberverbrechen hingegen sind neben der technischen Ausrüstung nur gute Hacker nötig. Und die werden oft in Ländern rekrutiert, in denen selbst für hochbegabte IT-Spezialisten mit ehrlicher Arbeit wenig zu holen ist. Allein in der Ransomware-Gruppe, die Anfang des Jahres Ziel der internationalen Polizeiaktion „Operation Endgame“ (siehe Seite 56) war, kamen sieben der acht Mitglieder aus Russland. Wer solche Leute anheuern will, muss zumindest anfangs nicht viel bezahlen. Und ist erst mal jemand Teil der Mafia oder ähnlicher Organisationen geworden, ist der Ausstieg fast unmöglich.

Kriminelle im Staatsdienst

Das gilt erst recht für kriminelle Hacker im Staatsdienst. Nordkorea etwa ist bekannt für Hacks bei Kryptowährungen; 2022 soll die Diktatur damit 1,7 Milliarden Dollar eingenommen haben. Mit Konsequenzen muss dort niemand rechnen: Wo der Staat Auftraggeber ist, haben Black Hats nichts zu befürchten. Das gilt in gewissem Rahmen allerdings auch für die Organisierte Kriminalität, deren Attraktivität nicht zuletzt auf dem Versprechen von Schutz beruht. Wer in der Lage ist, Leute zu schützen, die auf offener Straße Koks verkaufen, kriegt das erst recht bei Personen hin, die ständig am Rechner sitzen und nie das Haus verlassen.

Jedenfalls steigen die polizeilich erfassten Fälle von Cyberkriminalität stetig. Waren es 2007 in Deutschland noch rund 34.000 Fälle, sind es 2023 schon rund 134.000 gewesen. Ein bescheidener Anstieg? Nur von Weitem betrachtet: Der Branchenverband Bitkom geht davon aus, dass gerade mal 14 Prozent der Geschädigten zur Polizei gehen. Stimmt das, liegt die Zahl der Geschädigten bei rund einer Million.

Die steigende Cyberkriminalität ließ in den vergangenen Jahren auch die Nachfrage für Cybersecurity wachsen, zu der unter anderem die Einsätze von Hackern gehören, die Systeme auf ihre Lücken überprüfen und Schachstellen suchen – das sogenannte Pentesting.

Die EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS2), die in Deutschland ab Oktober 2024 umgesetzt wird und Organisationen wie Unternehmen zu Sicherheitsmaßnahmen gegen Cyberattacken verpflichtet, wird diesen Bedarf noch verstärken. Die zuständigen Behörden rüsten in dem Bereich ebenfalls seit Jahren auf – und so ist Hacker mittlerweile ein Berufsbild mit hohem Marktwert.

Für die allgemeine Sicherheit ist das gut, für staatliche Stellen allerdings ein echtes Problem. Denn sie müssen auch Hacker nach Tarif bezahlen und können deshalb nicht annähernd Gehälter wie in der freien Wirtschaft bieten. Was also zieht mehr als viel Geld? Commitment. Wirksamkeit. Und ein bisschen der Thrill.

Das erfährt man von Lukas, der anders heißt, aber als Hacker des Bundesnachrichtendienstes (BND) anonym bleiben muss. Lukas ist ein Staatshacker des Geheimdienstes. Im Gespräch wirkt er ruhig und überlegt, vielleicht ein wenig emotionslos. Doch das trügt: ›

„Ich habe mich schon zu Schulzeiten fürs Hacken interessiert. Später habe ich an ‚Capture The Flags' teilgenommen, also diesen offiziellen Hacker-Wettbewerben. Bei denen müssen Schwachstellen gefunden und andere Aufgaben gelöst werden. Um was zu lernen, muss man es üben, und da konnte ich hacken, ohne illegal zu sein. Außerdem hat das einen sportlichen Charakter. Denn es kommt unter anderem auf Zeit an: Wer schafft es am schnellsten? Das war cool. Da hat mich auch mein erster Arbeitgeber gescoutet, eine Pentesting-Firma, wo ich quasi professionell nutzen konnte, was ich vorher sportlich gemacht habe.

Mir ging es bei den Wettbewerben vor allem darum, mir selbst zu beweisen, dass ich etwas schaffe, selbst wenn ich vorher tausendmal gescheitert bin. Das ist etwas, das ich auch von Freunden kenne, die ebenfalls Hacker sind. Dieser Erfolgsmoment ist ein großer Motivator. Und der zieht sich auch bei unseren Hackern beim BND durch. Es gibt sicherlich Leute, die das machen, weil sie damit viel Geld verdienen können. Aber bei denen, die ich kenne, ist die Motivation eher: Das macht Spaß, ich habe Lust darauf, es ist irgendwie interessant.

Bei uns ist es sehr, sehr wichtig, die Technik wirklich zu beherrschen und immer auf dem neuesten Stand zu sein, zu wissen, was gerade benutzt wird, Trends zu kennen. Außerdem braucht man in unserem Bereich ein leicht abgeändertes Mindset. Anders als bei den Pentests. Die sind am Ende Aufträge, um die Sicherheit eines Systems zu überprüfen. Sie haben einen festen zeitlichen Rahmen, und es gibt bestimmte Sachen, die erlaubt sind oder eben nicht. Das ist mit unseren Operationen nicht vergleichbar.

Ich sage es mal provokant: Wir machen das echte Hacking. Wir dringen in Netze im Ausland ein, zur Informationsbeschaffung für die Bundesregierung. Und das Eindringen darf ebenso wenig bemerkt werden wie der Export von Daten. Wir wollen dort möglichst lange drinbleiben. Deshalb kommen bestimmte Skills zum Tragen: Wie sorge ich dafür, dass ich nicht entdeckt werde? Wie halte ich mich in Netzwerken länger auf? Wie schaffe ich unsichtbar Daten raus? Das sind alles Dinge, die man im Pentesting nicht so intensiv hat. Ein einfaches Beispiel: Ich sitze bei einem Einsatz auf keinen Fall am Rechner, tippe und drücke Enter. Ich bereite die Befehle vor, kopiere sie rein und drücke dann Enter, um Tippfehler zu vermeiden.

Das alles ist wirklich sehr spannend. Und das ist genau der Punkt, warum ich gewechselt habe. Als Pentester war immer klar, wenn ich auffalle, sage ich, wer ich bin, und es ist erledigt. Jetzt führe ich echte Operationen durch mit echter Informationsbeschaffung. Und wenn ich hinterher sehe, was der Auswerter geschrieben hat, habe ich das gute Gefühl, dass meine Arbeit einen Effekt hat. Sie hat einen Wert.

Also, die Leute kommen nicht wegen des Gehalts zu uns, sondern weil sie hier geilen Scheiß machen. Zwar wird jeder im Bereich Hacking, der möchte, nach einer Wartezeit verbeamtet. Aber man muss ehrlich sagen, das Tarifrecht ist für Hacker nicht so attraktiv. Wir zahlen eine Zulage, brutto etwa 1.000 Euro, was den Schmerz ein bisschen lindert. Es ist eben nur nicht konkurrenzfähig mit Google.

Privat über meinen Job reden kann ich natürlich nicht. Meine engste Familie, Eltern, Geschwister und so, wissen, wo ich arbeite. Die fragen nicht nach Details. Im Freundeskreis ist es unterschiedlich. Ich habe zwei sehr enge Freunde, die auch Hacker sind und meinen Werdegang kennen. Denen kann ich nicht sagen: Ich mache im Finanzamt Schöneberg die IT. Denen habe ich die Wahrheit gesagt. Aber wenn mich sonst jemand fragt, was ich mache, antworte ich: ‚Ich bin Beamter, ich richte die Drucker in einer Verwaltungsbehörde ein.' Da will garantiert keiner mehr Genaueres wissen."

Foto: Wikipedia

Um jemanden zur Freigabe sensibler Daten zu bewegen, sind die schwarzen Schafe unter den Hackern raffinierter geworden im Ausnutzen von Hilfsbereitschaft und Empathie.

Wenn man so will, arbeiten amtliche Hacker wie Lukas für die Vorwärtsverteidigung moderner Staaten. Sie werden gebraucht, solange es Autokraten, Diktatoren, Oligarchen gibt, die für ihr Ego, ihre Macht, ihren Reichtum die Welt bedrohen.

Dagegen ist landläufige Cyberkriminalität so etwas wie der Gradmesser für den Entwicklungsstand der Digitalisierung. Am Anfang gab es solche Verbrecher nicht, weil es schlicht nichts zu holen gab. Heute gleicht die Situation eher dem Wilden Westen: Noch haben Datenräuber und -hehler allzu gute Chancen, nach ihren Beutezügen unbehelligt davonzukommen.

Immer wieder bieten Banden Hacking als „Service" an: Für kleines Geld, oft wohl weniger als 1.000 Dollar, werden entsprechende Schadprogramme plus Web-Adressen potenzieller Opfer verkauft. Doch vermutlich haben es viele Möchtegern-Diebe bei einem Versuch belassen. Denn kriminelles Hacken erfordert Geduld, Geschick, Einfallsreichtum und Organisation. Allein die nötige Geldwäsche, die in der Regel über die Konten ansonsten unbeteiligter Menschen läuft, ist immens aufwendig – und nichts für Amateure.

Es sind nur wenige Fälle bekannt, in denen ein Einzeltäter ein populäres, weitverbreitetes Programm mit einer illegalen „Hintertür" versehen hat, die es ermöglicht, über lange Zeit in unzählige Computer einzudringen und dort Schaden anzurichten.

Für das Gros der Angriffe braucht es Opfer, die ahnungslos oder leichtsinnig in die Fallen der Täter tappen. Denn die weitaus meisten Cyberstraftaten fußen auf der unfreiwilligen Mitarbeit der Opfer – ob es nun um Schadprogramme geht, den Aufbau von Botnetzen oder den Identitätsdiebstahl durch Doxing. So nennt man das Sammeln personenbezogener Daten im Internet, die zu einer Art Fake-Profil zusammengeführt werden. Immer braucht es jemanden, der gedankenlos Daten hinterlässt, auf fragwürdige Links klickt, dubiose Anhänge öffnet oder einen Datenstick in den Computer steckt, den er auf der Straße gefunden hat. Passiert tatsächlich.

Hacking ist schlau und ansteckend

Um jemanden zur Freigabe sensibler Daten zu bewegen, sind die schwarzen Schafe unter den Hackern zunehmend raffinierter geworden im Ausnutzen von Hilfsbereitschaft und Empathie. Ein beliebte Betrugsmasche war vor einigen Jahren ein E-Mail-Scam, bei dem häufig „nigerianische Prinzen" behaupteten, sie hätten ganz viel Geld, bräuchten aber Hilfe (also echtes Geld), um es zu nutzen. Auch heute versuchen vorgeblich wohlhabende Menschen noch, mit dieser Masche Beute zu machden. Es sind aber auch gefakte Hilfsaufrufe zum Schließen vermeintlicher Sicherheitslücken, die zum Desaster führen: ein Klick – und ganze Stadtverwaltungen werden lahmgelegt.

Doch die Gesellschaft lernt dazu. Wer einmal verstanden hat, dass unangekündigte E-Mails von fragwürdigen Absendern nicht vertrauenswürdig sind, klickt nicht mehr drauf. Der Wilde Westen wird gezähmt.

Denn die gute Nachricht ist: Hacking ist schlau und ansteckend. Gute Hacker sind Menschen, die fragen: Wie funktioniert das? Wie komme ich damit weiter als angenommen? Die andere Art zu denken – sie ist ein Erfolgsmodell, und die ganze Geschichte der Digitalisierung ließe sich als permanenter Hack erzählen, der äußerst gut funktioniert.

Übrigens, der Computer, den die MIT-Studenten Anfang der Sechziger ersetzen wollten, um ihre Modelleisenbahn zu automatisieren, hatte nur einen Bruchteil der Kapazität jener Geräte in unseren Taschen, die wir nur noch aus Gewohnheit Telefone nennen. ◢

WELT

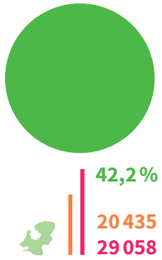
Uns steht ein Super-Wahljahr bevor. Die Regierungen weltweit wappnen sich, schließlich werden Wahlen heute auch im Internet gewonnen oder verloren. Desinformation, Hackerangriffe auf Partei-Netzwerke und Hack-and-Leak-Kampagnen sind inzwischen an der Tagesordnung. Wir sind angreifbar geworden – immer und überall.

Gefährliche Lücken

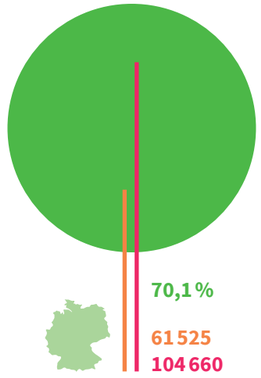
Fehlende Fachkräfte im Bereich Cybersicherheit; ausgewählte Länder

2020 · 2023 · Veränderung 2020 – 2023

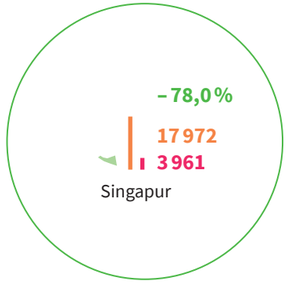
Australien
2,1 %
27 192
27 756



Niederlande
42,2 %
20 435
29 058

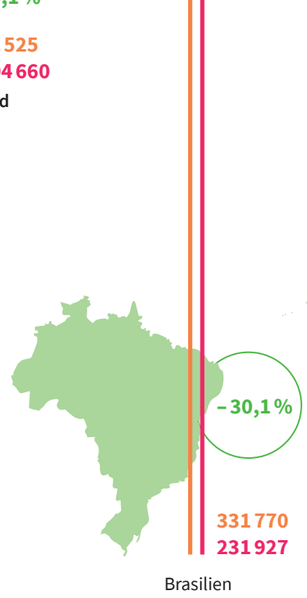


Deutschland
70,1 %
61 525
104 660

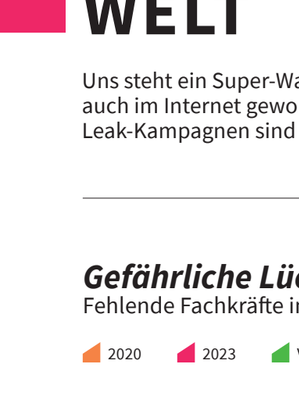


Singapur
– 78,0 %
17 972
3 961

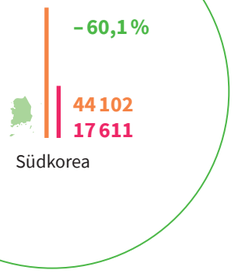
Japan
19,2 %
92 466
110 254



Brasilien
– 30,1 %
331 770
231 927

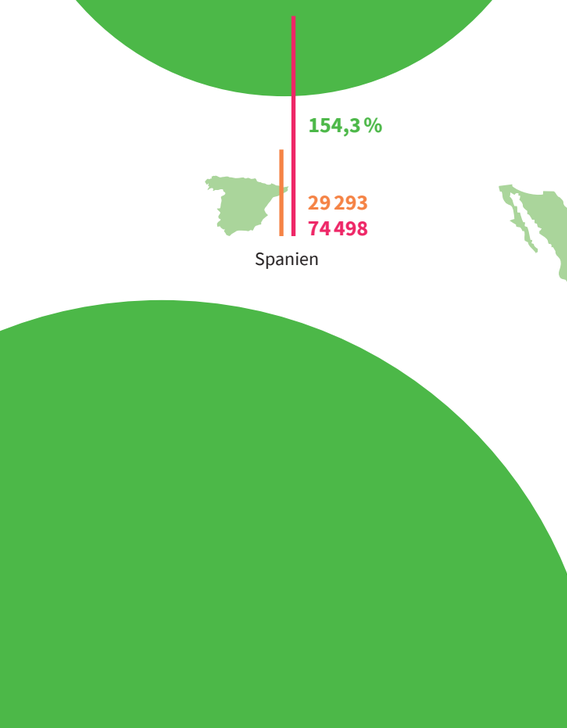


Frankreich
114,5 %
27 562
59 117

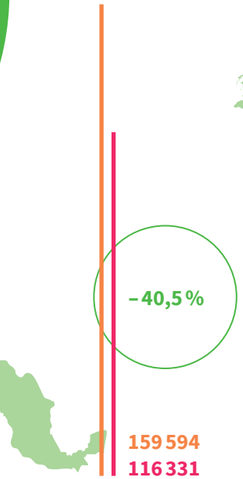


Südkorea
– 60,1 %
44 102
17 611

Kanada
134,7 %
16 552
38 842

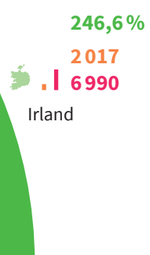


Spanien
154,3 %
29 293
74 498



Mexiko
– 40,5 %
159 594
116 331

Vereinigtes Königreich
167,9 %
27 408
73 439



Irland
246,6 %
2 017
6 990

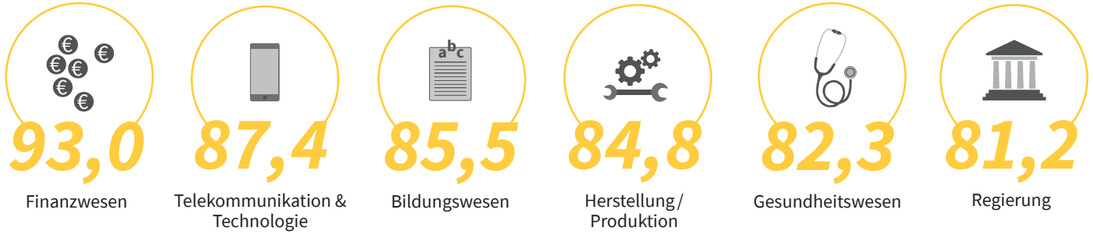
USA
34,4 %
359 236
482 985

Quelle: (ISC)²

Glossar der Cyberbegriffe auf Seite 100 – 103

Zu wenig Expertise

Fehlende Fachkräfte nach Branchen; qualifizierte Entscheidungsträgerinnen und Entscheidungsträger in der IT-Sicherheit (n=1 200); weltweit; 2023; in Prozent



Quelle: CyberEdge

Zu wenig Engagement

Maßnahmen, um dem Personalmangel entgegenzuwirken; globale Fachleute für Cybersicherheit (n=10 521); weltweit; 2023; in Prozent *

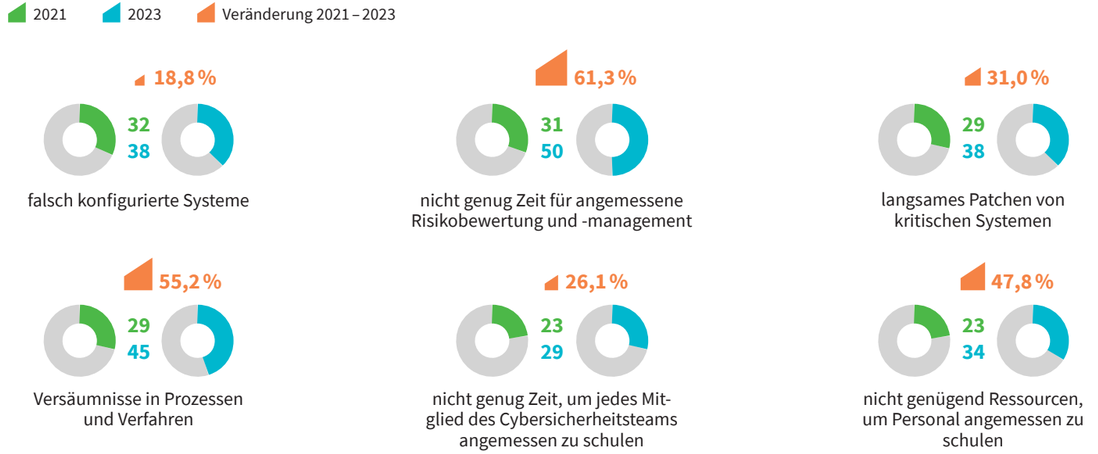
Welche der folgenden Maßnahmen ergreift Ihre Organisation oder plant sie zu ergreifen, um den Personalmangel im Bereich der Cybersicherheit in Ihrer Organisation zu verhindern oder abzumildern?

* Mehrfachnennungen möglich. Quelle: (ISC)²

Zu wenig Ressourcen

Konsequenzen von Personalmangel im Bereich Cybersicherheit; globale Cybersicherheits-Expertinnen und Experten, in deren Teams Personalmangel herrscht (2023: n=5 000+); weltweit; in Prozent *

Welche der folgenden Probleme haben Sie erlebt, die Ihrer Meinung nach durch eine ausreichende Zahl von Cybersecurity-Mitarbeiterinnen und -Mitarbeitern hätten gemildert werden können?



* Mehrfachnennungen möglich. Quelle: (ISC)²

Zu wenig Mittel

Ursachen für den Fachkräftemangel; Cybersicherheits-Expertinnen und -Experten (n=5 526); weltweit; 2023; in Prozent *

Sie haben angegeben, dass Ihrer Organisation Cybersicherheits-Fachkräfte fehlen. Was denken Sie, ist die größte Ursache für diesen Mangel?

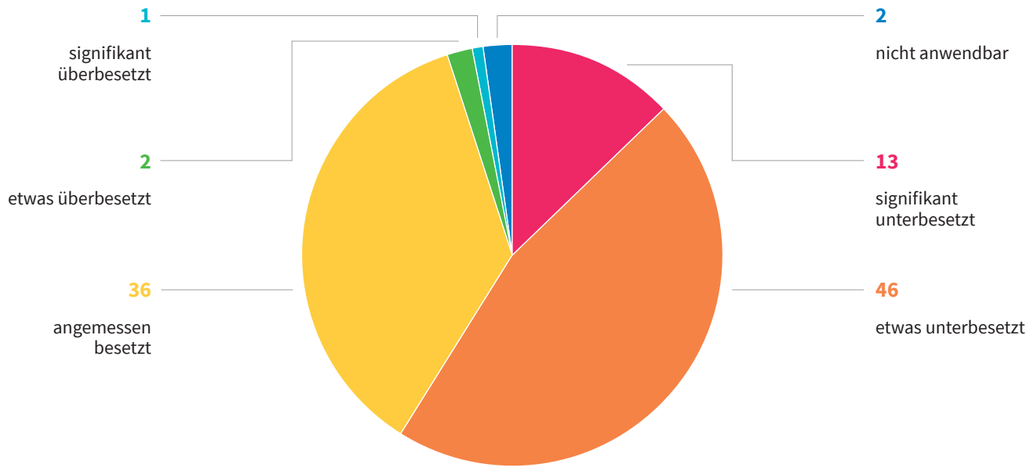
Meine Organisation findet nicht genug qualifizierte Talente.	41
Meiner Organisation fehlen die finanziellen Mittel.	34
Meine Organisation zahlt keinen wettbewerbsfähigen Lohn.	30
Meine Organisation hat Schwierigkeiten, mit der Fluktuation / dem Personalabbau Schritt zu halten.	27
Die Führungsebene setzt Personalressourcen falsch ein.	24
Meine Organisation ist nicht in der Lage, dem Sicherheitspersonal Weiterbildungs- oder Beförderungsmöglichkeiten zu bieten.	24
Meine Organisation verwendet nicht ausreichend Ressourcen, um IT-Personal zu Sicherheitspersonal fortzubilden.	23
Meine Organisation räumt dem Thema Sicherheit keine Priorität ein.	20
Meine Organisation hat keine Pläne, um frei werdende Stellen nachzubesetzen.	17
Meine Organisation trainiert das Personal nicht ausreichend.	15

* Mehrfachnennungen möglich. Quelle: (ISC)²

Reduziert

Einschätzung zum Fachkräftemangel; Fachleute für Cybersicherheit (n=2 178); weltweit; 2023; in Prozent

Wie würden Sie die derzeitige Personalausstattung des Cybersicherheits-Teams Ihrer Organisation beschreiben?



Quelle: ISACA

Positioniert

Kommunikationsketten der Cybersicherheitsteams in Unternehmen; Fachleute für Cybersicherheit (n=2 178); weltweit; 2023; in Prozent

Wem ist das Cybersicherheitsteam in Ihrer Organisation unterstellt?

CISO: Chief Information Security Officer	49
CIO: Chief Information Officer	17
CEO: Chief Executive Officer	8
CTO: Chief Technology Officer	7
Vorstand	5
CSO: Chief Security Officer	5
Sonstige	5
CRO: Chief Revenue Officer	2
CFO: Chief Financial Officer	2
CAE: Chief Audit Executive	<1

Quelle: ISACA

Definiert

Kommunikationsketten der CISOs in Unternehmen; Fachleute für Cybersicherheit (n=2 178); weltweit; 2023; in Prozent

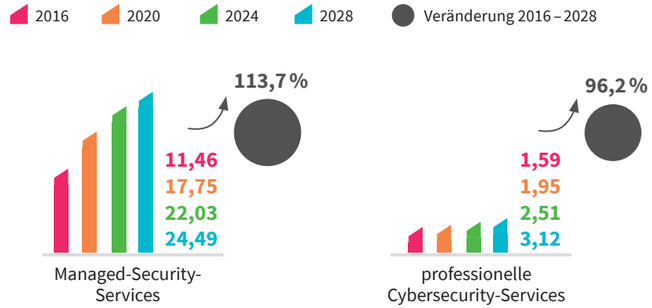
Wem ist der CISO in Ihrer Organisation unterstellt?

CIO	25
CEO	24
kein CISO vorhanden	11
Vorstand	9
CTO	9
COO	5
CSO	4
Sonstige	4
CRO	4
CFO	4
CAE	<1

Quelle: ISACA

Prognostiziert

Umsatz mit Security-Services; weltweit; in Milliarden Euro



Quelle: Statista Market Insights

Managed Security Services (MSS) bieten kontinuierliche, rund um die Uhr laufende Überwachungs- und Verwaltungsdienste, die darauf abzielen, die allgemeine Sicherheitslage eines Unternehmens proaktiv zu verbessern und zu verwalten. Beispiele: 24/7-Sicherheitsüberwachung und -management oder Managed Firewall Services.

Professional Security Services (PSS) hingegen sind spezialisierte, zeitlich begrenzte Dienstleistungen, die auf spezifische Sicherheitsprojekte oder -initiativen fokussiert sind und oft tiefgehende Beratung und Expertise bieten. Beispiele: Durchführung eines Penetrationstests oder Entwicklung und Implementierung einer neuen Sicherheitsstrategie.

Investiert

Ausgaben für öffentliche Cloud-Dienste für Endnutzer; Prognose; 2024; weltweit; in Milliarden Euro

Business Process as a Service (BPaaS) ist die bedarfsorientierte Bereitstellung einer nutzerspezifischen Zusammenstellung von IT-Ressourcen und nicht IT-unterstützten Funktionalitäten nach dem Everything as a Service (EaaS) Konzept. Diese Zusammenstellung unterstützt einen kompletten Geschäftsprozess eines Kunden.

Platform-as-a-Service (PaaS) ist eine vollständige Entwicklungs- und Bereitstellungsumgebung in der Cloud, die Ressourcen für die Umsetzung einfacher cloudbasierter Apps sowie anspruchsvoller, cloudfähiger Unternehmensanwendungen bietet. Sie erwerben die nötigen Ressourcen über ein nutzungsbasiertes Zahlungsmodell von einem Cloud-Dienstanbieter und greifen über eine sichere Internetverbindung darauf zu.

Mit Software-as-a-Service (SaaS) können sich Benutzer über das Internet mit cloudbasierten Apps verbinden und diese nutzen. Gängige Beispiele sind E-Mail-, Kalender- und Office-Tools (z. B. Microsoft Office 365).

Infrastructure-as-a-Service (IaaS) ist ein Cloud-Computing-Dienst, der bedarfsbasiert grundlegende Computer-, Speicher- und Netzwerkressourcen mit nutzungsbasierter Bezahlung bietet. IaaS ist einer von vier Cloud-Diensttypen, zu denen auch Software-as-a-Service, Platform-as-a-Service und serverloses Computing gehören.

Desktop as a Service (DaaS) ist ein Cloud-Computing-Angebot, bei dem eine Drittpartei das Backend einer virtuellen Desktop-Infrastruktur (VDI) hostet. Bei DaaS werden Desktop-Betriebssysteme in virtuellen Maschinen (VM) auf Servern im Rechenzentrum eines Cloud-Anbieters ausgeführt.

225,6
Cloud Application Services (SaaS)

168,5
Cloud System Infrastructure Services (IaaS)

163,2
Cloud Application Infrastructure Services (PaaS)

67,4
Cloud Business Process Services (BPaaS)

2,9
Desktop as a Service (DaaS)

627,5
Gesamtmarkt

Quellen: Gartner, Gabler Wirtschaftslexikon, Microsoft, ComputerWeekly

Addiert

Geschätzte Menge an neu kreierten Daten im Internet pro Minute; weltweit; 2023; diverse Einheiten

241 Millionen
gesendete E-Mails

41,6 Millionen
versendete Nachrichten über WhatsApp

6,3 Millionen
Google-Suchen

6 060
hochgeladene Lebensläufe auf LinkedIn

6 944
Eingaben bei ChatGPT

30
DDoS-Angriffe durch Cyberkriminelle

3 720
heruntergeladene Threads über Instagram

48 000
Stunden von gestreamten Inhalten auf Twitch

4 Millionen
auf Facebook gelikte Inhalte

694 000
gesendete Reels via Privatnachricht über Instagram

durchschnittlich produzierte Daten pro Person
102 MB

747
Buchungen über Airbnb

69 400
gestreamte Taylor-Swift-Songs

Dauer von gestreamten Inhalten
43 Jahre

auf Amazon getätigte Käufe im Wert von
420 000 Euro

Quelle: Domo

Registriert

Zahl kompromittierter Accounts zum Stichtag 13.03.2024; weltweit

13 405 191 392
identifizierte kompromittierte Accounts

1 472 564
geleakte Accounts pro Tag

1 846
Zahl der Leaks

Quelle: HPI

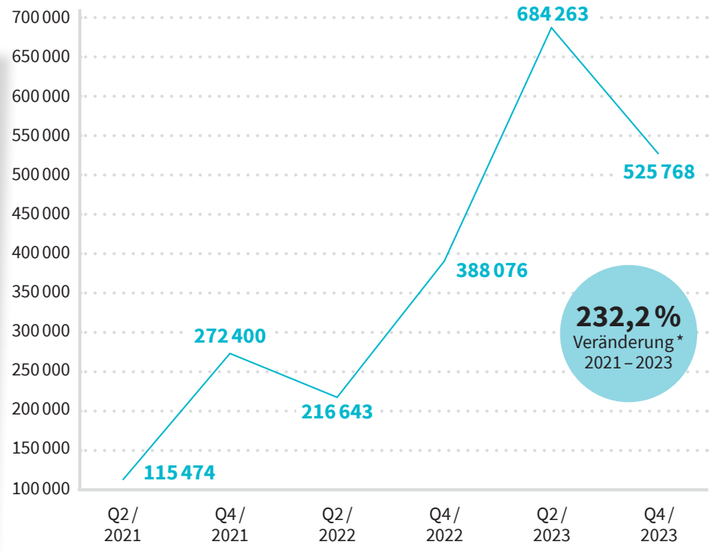
Zum Hintergrund:
Das Hasso-Plattner-Institut für Digital Engineering (HPI) überprüft, ob eine Mailadresse kompromittiert ist bzw. ob Identitätsdaten ausspioniert wurden. Täglich werden persönliche Identitätsdaten durch kriminelle Cyberattacken erbeutet. Ein Großteil der gestohlenen Angaben wird in Internet-Datenbanken veröffentlicht und dient als Grundlage für weitere illegale Handlungen. Der HPI Identity Leak Checker überprüft mithilfe der E-Mailadresse, ob die persönlichen Identitätsdaten bereits im Internet veröffentlicht wurden. Per Datenabgleich wird kontrolliert, ob die E-Mailadresse in Verbindung mit anderen persönlichen Daten (z. B. Telefonnummer, Geburtsdatum oder Adresse) im Internet offengelegt wurde und missbraucht werden könnte.

Abkassiert

Durchschnittliche Ransomware-Zahlungen; qualifizierte Entscheidungsträgerinnen und -träger in der IT-Sicherheit (n=1 200); weltweit; in Euro

Zur Einordnung:
Die Zahlen zeigen über das Jahr verteilt einen schwankenden Verlauf. Auffällig ist, dass das dritte und vierte Quartal der jeweiligen Jahre oft hohe Zahlungen und die restlichen Quartale vergleichsweise geringere Zahlungen aufweisen.

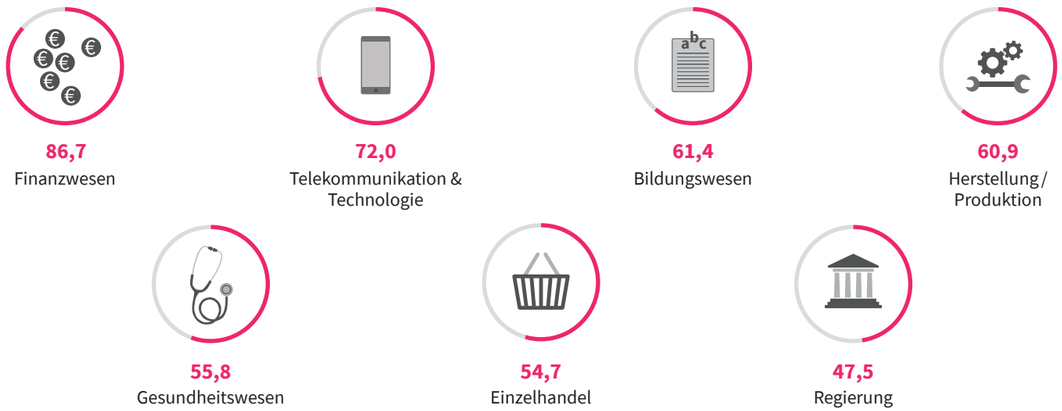
Zu erklären ist das mit saisonalen Feiertagen bzw. Aktionen wie Weihnachten und Black Friday. Aus diesen Anlässen bestellen Nutzer vermehrt Geschenke oder reduzierte Artikel im Internet. Die Angreifer nutzen diese Gelegenheiten aus und greifen mehr und häufiger an.



* Vergleich der Summen der vier Quartale des jeweiligen Jahres. Quelle: CyberEdge

Verletzbar

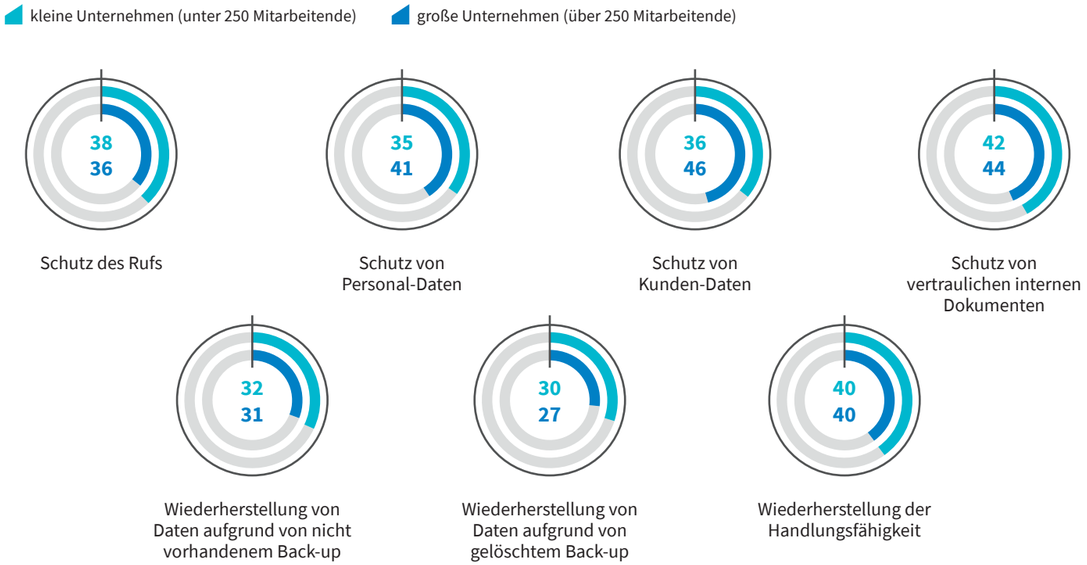
Von Ransomware betroffene Organisationen nach Branchen; qualifizierte Entscheidungsträgerinnen und -träger in der IT-Sicherheit (n=1 200); weltweit; 2023; in Prozent



Quelle: CyberEdge

Erpressbar

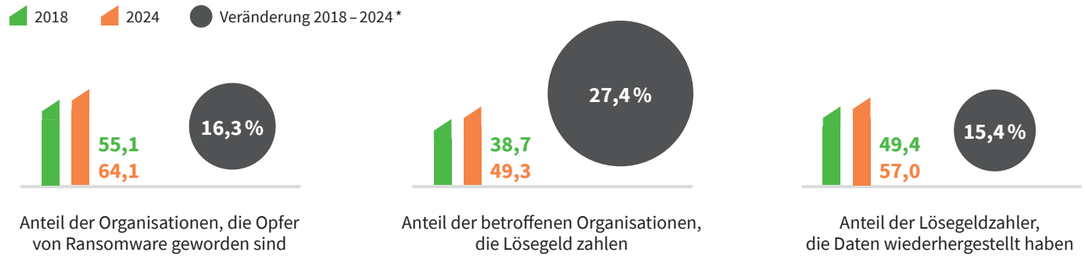
Hauptgründe für die Zahlung bei einem Ransomware-Angriff; weltweit; 2023; in Prozent *



* Mehrfachnennungen möglich. Quelle: Hiscox

Vernachlässigbar

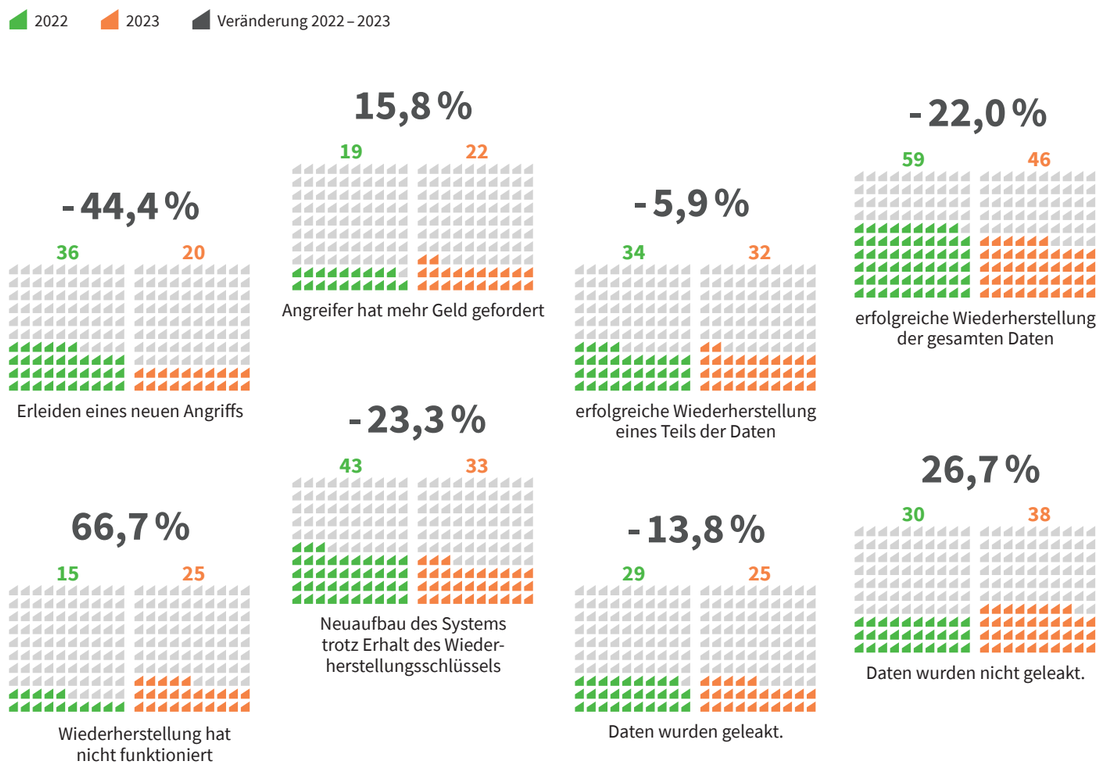
Ransomware: Angriffe, Bezahlung, Datenrettung; qualifizierte Entscheidungsträgerinnen und -träger in der IT-Sicherheit (n=1 200); weltweit; in Prozent



* Die Datenerhebung zu den angegebenen Jahren erfolgte jeweils im November des vorherigen Jahres. Die Daten für 2024 entsprechen damit denen aus der Umfrage im November 2023. Quelle: CyberEdge

Unrettbar

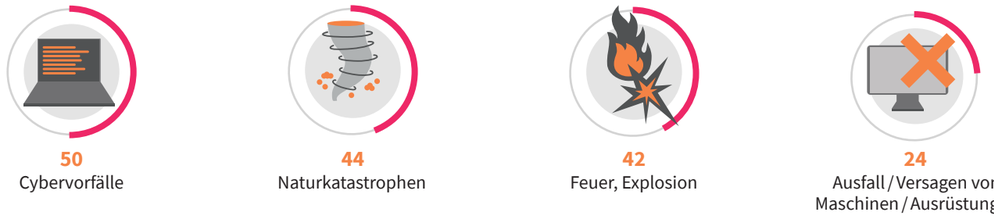
Folgen nach Zahlung bei einem Ransomware-Angriff; weltweit; 2023; in Prozent *



* Mehrfachnennungen möglich. Quelle: Hiscox

Gefürchtet

Von Unternehmen meistgefürchtete Ereignisse für Betriebsunterbrechnungen; Umfrageteilnehmerinnen und -teilnehmer (n=955); weltweit; 2024; in Prozent *



50 Cybervorfälle

44 Naturkatastrophen

42 Feuer, Explosion

24 Ausfall / Versagen von Maschinen / Ausrüstungen

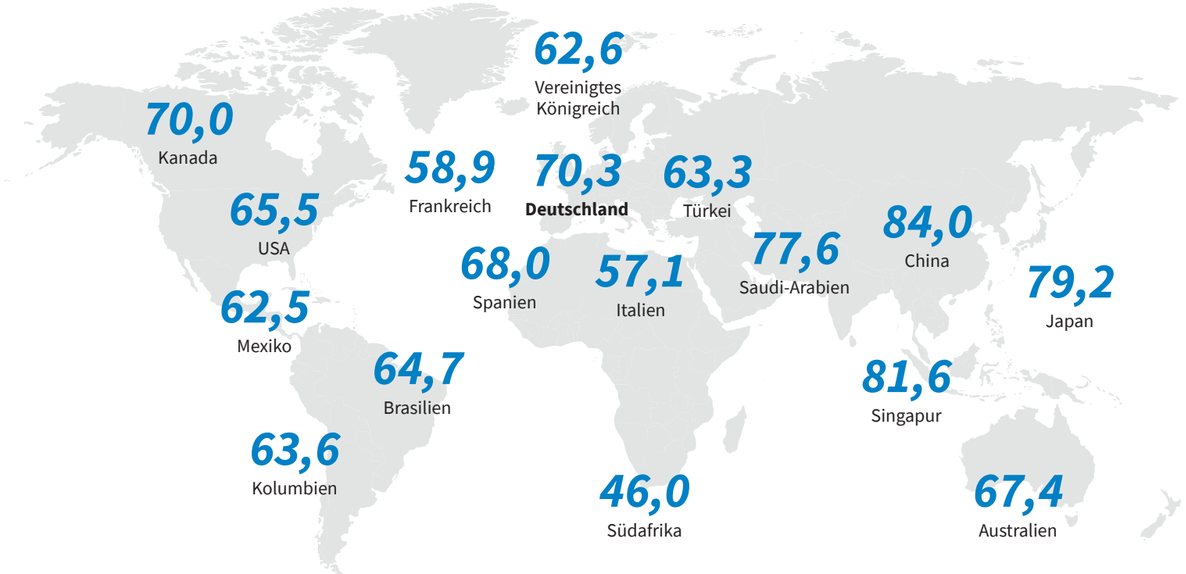
Anteil der Unternehmen, die Cybervorfälle fürchten nach Unternehmensgröße

kleine Unternehmen (< 100 Mio. USD Umsatz) 32
mittlere Unternehmen (100 – < 500 Mio. USD Umsatz) 34
große Unternehmen (> 500 Mio. USD Umsatz) 41

* Mehrfachnennungen möglich. Quelle: Allianz

Gefährdet

Anteil der Unternehmen, die eine Gefährdung durch einen erfolgreichen Cyberangriff im Jahr 2024 für eher oder sehr wahrscheinlich halten; IT-Entscheidungsträgerinnen und -träger (n=1 200); weltweit; 2023; in Prozent *



Quelle: CyberEdge

Gezahlt

Top-10-Bußgelder für Datenschutzverstöße 2019 – 2024 *; weltweit; in Euro

1
4 536 999 350
USA
Facebook Inc.
24.7.2019
*Verstoß gegen frühere FTC **-Datenschutz-anordnungen und das Gesetz der Federal Trade Commission*

2
1 200 000 000
Irland
Meta Platforms Ireland Ltd.
22.5.2023
rechtswidrige Übermittlung personenbezogener Facebook-Daten an die USA

3
1 165 011 903
China
DiDi
21.7.2022
Verstöße gegen Gesetze zur Netzwerksicherheit, Datensicherheit und zum Schutz persönlicher Informationen

4
746 000 000
Luxemburg
Amazon Europe Core S.à r.l
30.7.2021
Verstöße im Zusammenhang mit der Anzeige von Werbung und der Weitergabe von Daten an Dritte

5
508 130 081
USA
Equifax Inc.
22.7.2019
Unzureichende Schutzmaßnahmen ermöglichten Diebstahl von Bonitätsdaten von 147 Mio. Betroffenen.

6
405 000 000
Irland
Instagram
5.9.2022
Rekord-Bußgeld für Instagram nach Bruch von Datenschutzrechten Minderjähriger

7
390 000 000
Irland
Meta Platforms Ireland Ltd.
4.1.2023
Vertragserfüllung, keine Rechtsgrundlage für personalisierte Werbung

8
379 397 228
USA
Google
15.11.2022
Rekord-Vergleich nach irreführenden Informationen zum Standort-Tracking

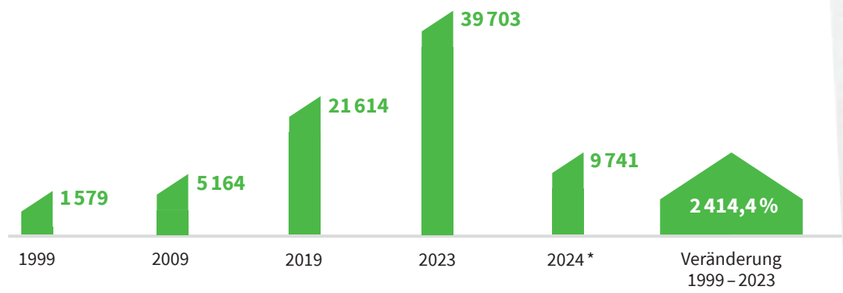
9
345 000 000
Irland
TikTok Technology Limited
15.9.2023
Missachtung beim Umgang mit den Daten Minderjähriger

10
265 000 000
Irland
Meta Platforms Ireland Ltd.
28.11.2022
Entscheidung im Data-Scraping-Verfahren gegen Meta

* Datenabruf am 23.4.2024. ** FTC: Federal Trade Commission (Bundesbehörde der USA). Quelle: DSGVO-Portal

Geteilt

Zahl der von CVE dokumentierten Schwachstellen in der IT-Sicherheit; weltweit

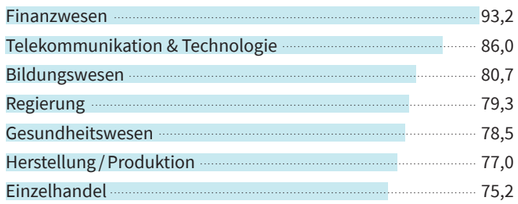


* Stand 21.3.2024. Quelle: CVE unterstützt durch U.S. Department of Homeland Security und Cybersecurity and Infrastructure Security Agency

Zum Verständnis:
Die Aufgabe des CVE® -Programms ist es, öffentlich bekannt gemachte Sicherheitslücken in der Cybersicherheit zu identifizieren, zu definieren und zu katalogisieren. Für jede Schwachstelle im Katalog gibt es einen CVE-Eintrag. Die Schwachstellen werden von Organisationen aus der ganzen Welt, die eine Partnerschaft mit dem CVE-Programm eingegangen sind, entdeckt, zugewiesen und veröffentlicht. Die Partner veröffentlichen CVE-Datensätze, um konsistente Beschreibungen von Sicherheitslücken zu kommunizieren.

Ziele

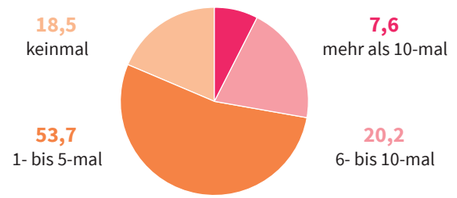
Anteil erfolgreicher Cyberattacken je Branche; IT-Entscheidungsträgerinnen und -träger (n=1 200); weltweit; 2023; in Prozent



Quelle: CyberEdge

Treffer

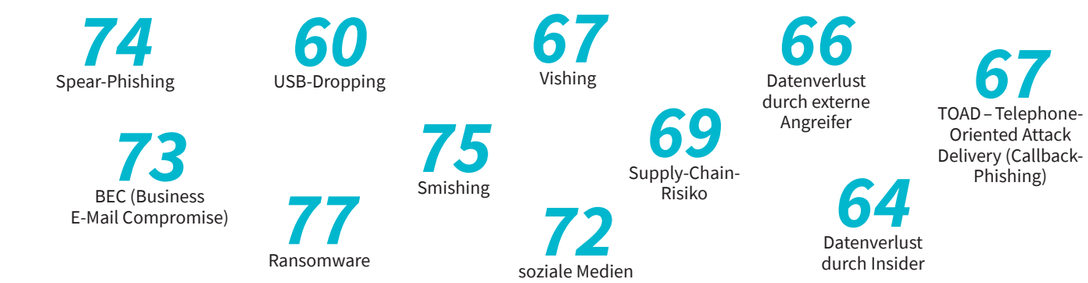
Zahl erfolgreicher Cyberattacken innerhalb der vergangenen zwölf Monate; IT-Entscheidungsträgerinnen und -träger (n=1 200); weltweit; 2023; in Prozent



Quelle: CyberEdge

Angriffsarten

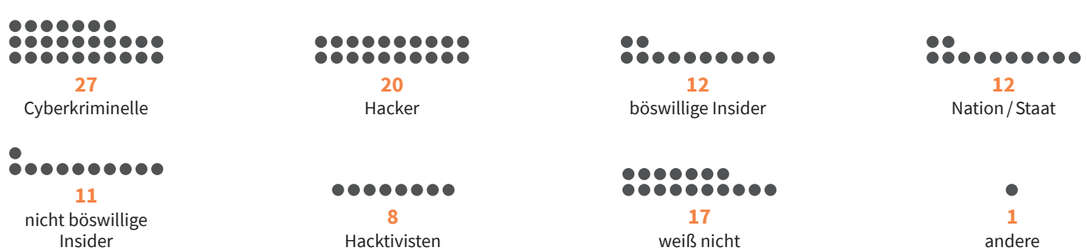
Häufigkeit von Cyberangriffen nach Art; Endnutzerinnen und -nutzer (n=7 500) und Sicherheitsexpertinnen und -experten (n=1 050) aus 15 Ländern weltweit; 2023; in Prozent *



* Mehrfachnennungen möglich. Quelle: Proofpoint

Angreifer

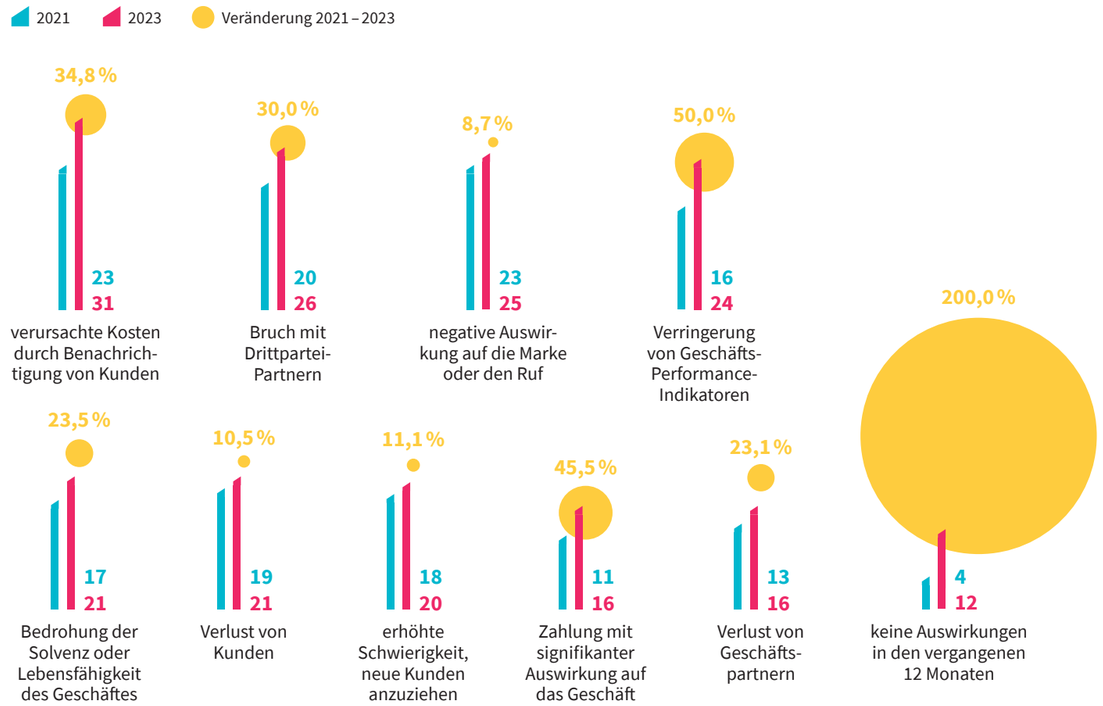
Bedrohungsakteure erfolgreicher Angriffe; Fachleute für Cybersicherheit (n=2 178); weltweit; 2023; in Prozent *



* Mehrfachnennungen möglich. Quelle: ISACA

Empfindlich

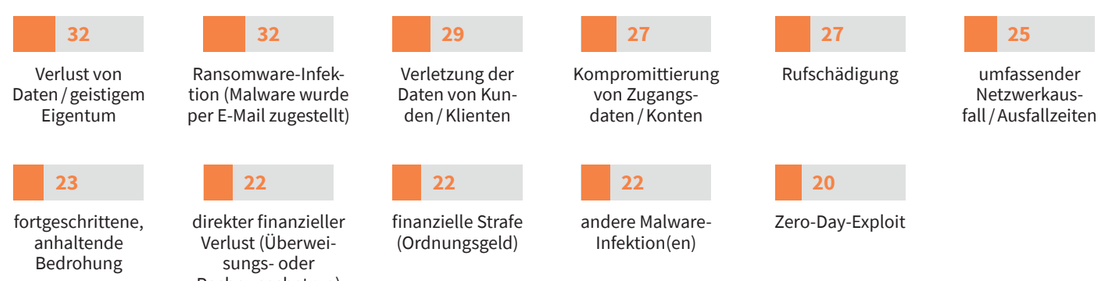
Effekte und Auswirkungen einer Cyberattacke; Sicherheitsprofis (n=5 005); weltweit; in Prozent *



* Mehrfachnennungen möglich. Quelle: Hiscox

Persönlich

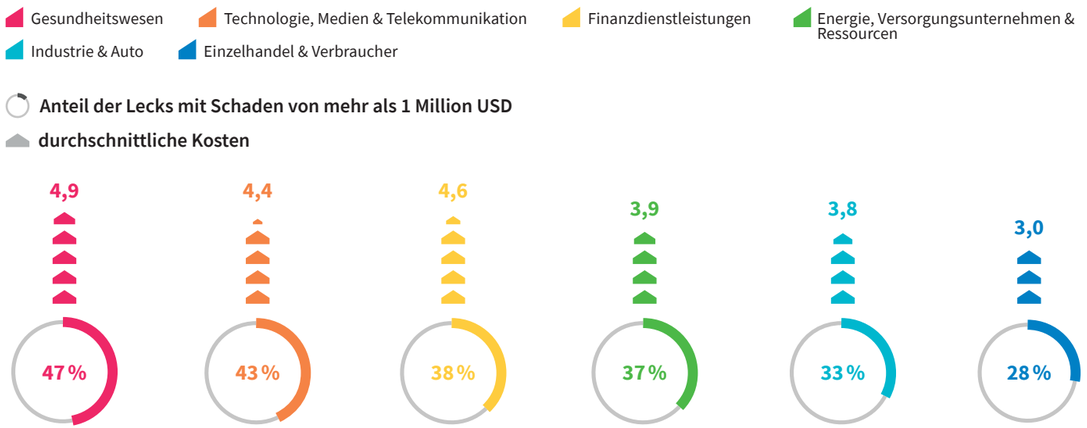
Auswirkungen erfolgreicher Phishing-Angriffe; Endnutzerinnen und -nutzer (n=7 500) und Sicherheitsexpertinnen und -experten (n=1 050) aus 15 Ländern weltweit; 2023; in Prozent *



* Mehrfachnennungen möglich. Quelle: Proofpoint

Schutzlos

Durchschnittlicher Schaden durch ein Datenleck; weltweit; 2023; in Millionen Euro / in Prozent



Quelle: PwC

Ahnungslos

Vergangene Zeit, bis ein Datenleck entdeckt wird nach Angriffsart; Personen aus Unternehmen, die von einem Datenleck betroffen waren (n=553); weltweit; in Tagen

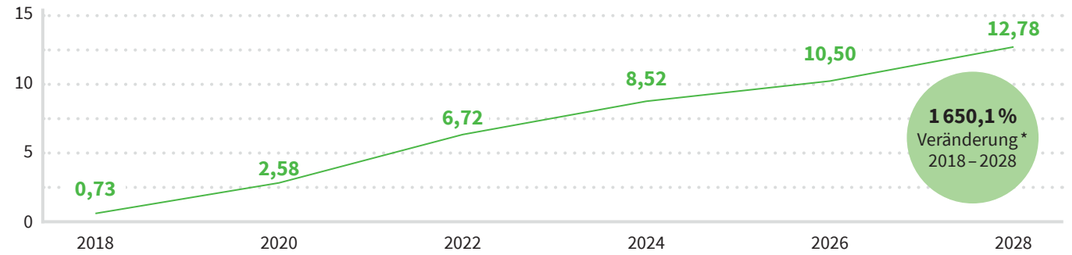
	mittlere Zeit bis zur Identifikation	mittlere Zeit bis zur Eindämmung	gesamte Zeit
gestohlene oder kompromittierte Berechtigungsnachweise	240	88	328
böswilliger Insider	228	80	308
Social Engineering	218	80	298
Phishing	217	76	293
versehentlicher Datenverlust oder verlorenes Gerät	205	78	283
unbekannte Sicherheitslücken (Zero-Day)	195	77	272
physische Sicherheitsgefährdung	198	69	267
Gefährdung von geschäftlichen E-Mails	194	72	266
Fehlkonfiguration der Cloud	190	68	258
ungepatchte Sicherheitslücken	183	70	253
andere technische Fehlkonfiguration	180	56	236

Anteil der Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die denken, dass ein Hackerangriff …

Quellen: IBM, Statista

Grenzenlos

Zukünftige Entwicklung der Kosten durch Cybercrime; weltweit; in Milliarden Euro *



* Die Daten basieren auf den durchschnittlichen Wechselkursen der jeweiligen Jahre. Die Prognosen (ab 2024) wurden auf Grundlage des Wechselkurses aus 2023 berechnet.
Quelle: Statista

Ausweglos

Veränderung des Cyberbudgets im Vergleich zum Vorjahr; Führungskräfte aus unterschiedlichen Branchen; weltweit; 2024; in Prozent

84 Erhöhung

4 Verringerung

12 Sonstiges

Quelle: PwC

Endlos

Anteil der Unternehmen mit steigendem Budget für Cybersicherheit; IT-Entscheidungsträgerinnen und -träger (n=1 200); weltweit; in Prozent

48,3 2014

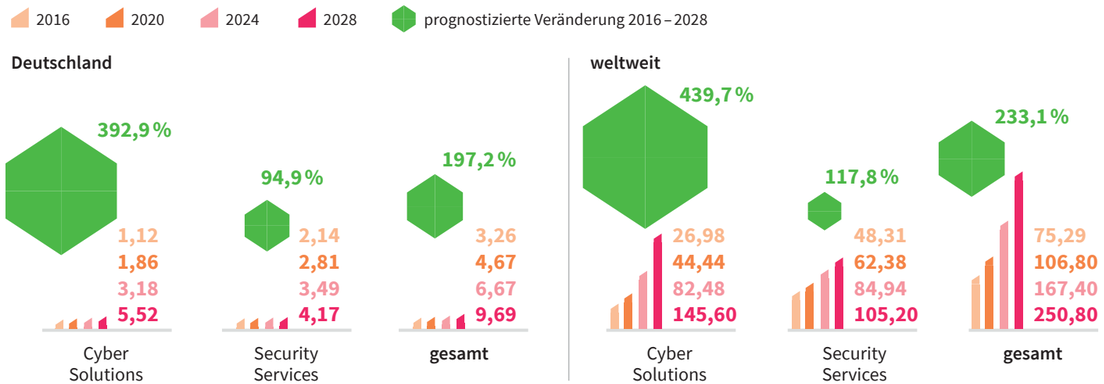
88,7 2024

83,6 % Veränderung 2014 – 2024

Quelle: CyberEdge

Alternativlos

Umsatz des Cybersicherheitsmarktes; weltweit; in Milliarden Euro

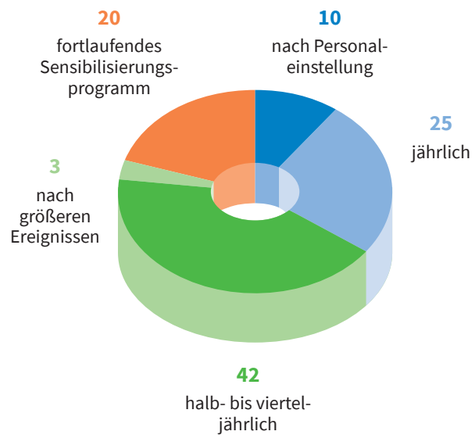


Quelle: Statista Market Insights

Zu wenig

Häufigkeit von Cybersicherheit-Trainings; IT-Profis (n=750); weltweit; 2023; in Prozent

Wie oft investiert Ihr Unternehmen in Cybersicherheit-Trainings?

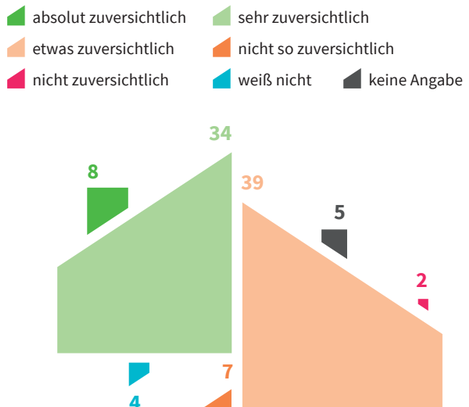


Quelle: HLB

Zu naiv

Vertrauen in Cybersicherheits-Teams in Unternehmen; Cybersecurity-Fachleute (n=2 178); weltweit; 2023; in Prozent

Wie zuversichtlich sind Sie, dass Ihr Sicherheits-Team in der Lage ist, Cyberbedrohungen zu erkennen und auf sie zu reagieren?



Quelle: ISACA

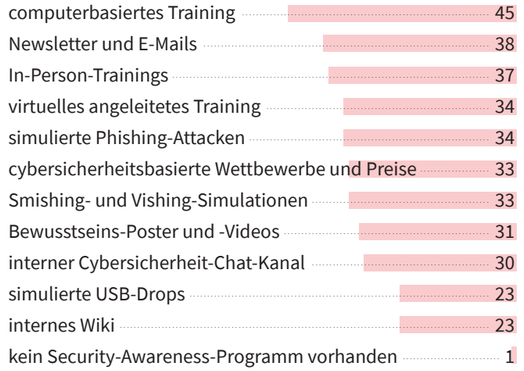
Zu leichtfertig

Hürden bei der Bewertung des Cyberrisikos; Cybersecurity-Fachleute (n=2 178); weltweit; 2023; in Prozent *

* Mehrfachnennungen möglich. Quelle: ISACA

Effektvoll

Durchgeführte Trainingsmaßnahmen für Security Awareness; Endnutzerinnen und -nutzer (n=7 500) und Sicherheitsexpertinnen und -experten (n=1 050) aus 15 Ländern weltweit; 2023; in Prozent*

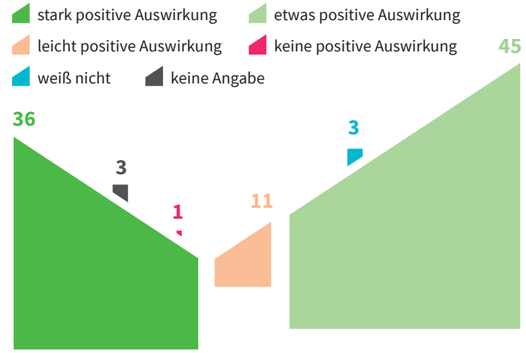


* Mehrfachnennungen möglich. Quelle: Proofpoint

Wirkungsvoll

Auswirkungen von Cybersecurity-Awareness-Programmen; Cybersecurity-Fachleute (n=2 178); weltweit; 2023; in Prozent

Welchen Einfluss hatten die Cybersicherheits- und Sensibilisierungsprogramme auf das allgemeine Cybersicherheits-Bewusstsein der Mitarbeitenden in Ihrem Unternehmen?

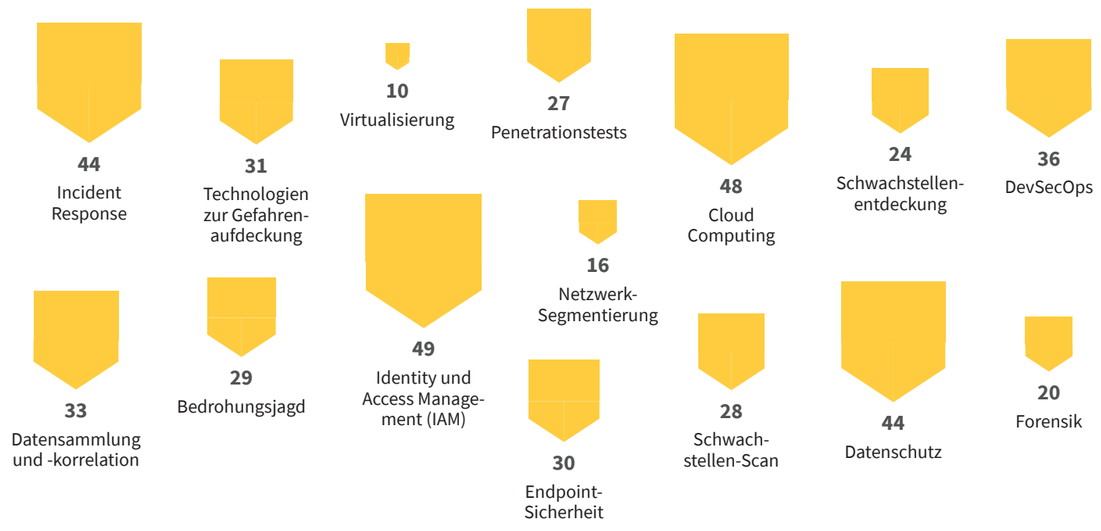


Quelle: ISACA

Leidvoll

Die wichtigsten Sicherheitskompetenzen; Cybersecurity-Fachleute (n=2 178); weltweit; 2023; in Prozent *

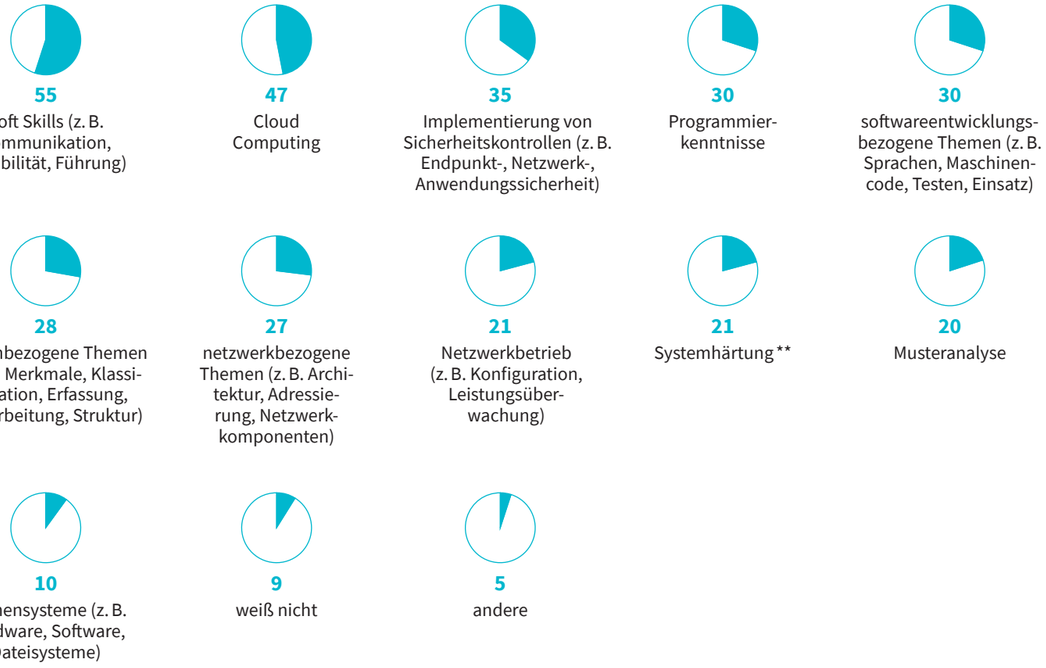
Welche sind die fünf wichtigsten Sicherheitskompetenzen, die in Ihrem Unternehmen heute benötigt werden?



* Mehrfachnennungen möglich. Quelle: ISACA

Was fehlt

Die größten Qualifikationsdefizite bei Cybersecurity Professionals; Cybersecurity-Fachleute (n=2 178); weltweit; 2023; in Prozent *



* Mehrfachnennungen möglich. ** Systemhärtung: Prozess der Reduzierung von Sicherheitsrisiken durch das Eliminieren von überflüssigen Systemfunktionen, das Konfigurieren von Sicherheitseinstellungen und das Anwenden von Sicherheitspatches, um das System widerstandsfähiger gegenüber Angriffen zu machen. Quelle: ISACA

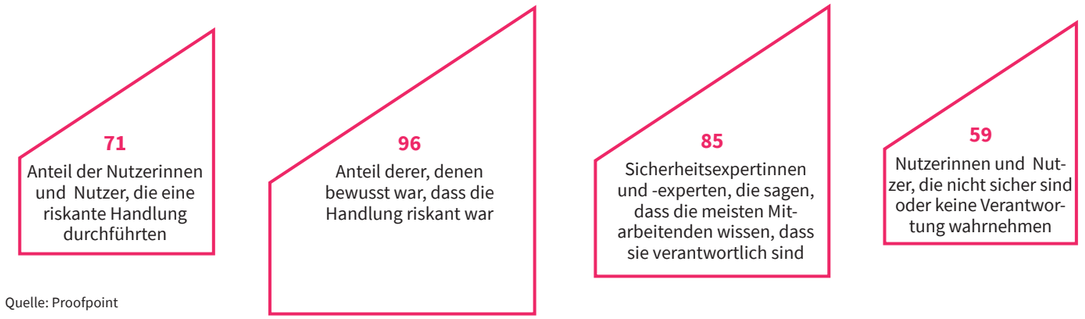
Was hilft

Motivierende Maßnahmen zur Priorisierung von Cybersicherheit; Endnutzerinnen und -nutzer (n=7 500) und Sicherheitsexpertinnen und -experten (n=1 050) aus 15 Ländern weltweit; 2023; in Prozent

Quelle: Proofpoint

Was irritiert

Risikobereitschaft von Arbeitnehmerinnen und Arbeitnehmern; Endnutzerinnen und -nutzer (n=7 500) und Sicherheitsexpertinnen und -experten (n=1 050) aus 15 Ländern weltweit; 2023; in Prozent



Quelle: Proofpoint

Was passiert

Riskante Handlungen in Unternehmen, die schon einmal durchgeführt wurden; Endnutzerinnen und -nutzer (n=7 500) und Sicherheitsexpertinnen und -experten (n=1 050) aus 15 Ländern weltweit; 2023; in Prozent *

Nutzung von Arbeitsgeräten für persönliche Aktivitäten	29
Wiederverwendung oder Teilung des Passworts	26
Verbindungsherstellung in der Öffentlichkeit ohne VPN	26
Antwort auf eine Nachricht einer unbekannten Person (E-Mail, SMS oder Text)	24
Zugriff auf unangemessene Website	20
Klicken auf Links oder Herunterladen von Anhängen einer unbekannten Person	19
Teilen von Arbeitsgeräten mit Freunden oder der Familie	16
Anrufen einer unbekannten Nummer aus einer dringenden E-Mail	13
Tailgating: Einlassgewährung einer anderen Person ohne Eintragung	11
Hochladen sensitiver Daten auf ungeprüfte Drittanbieter-Cloud	10
Weitergabe von Zugangsdaten an nicht vertrauenswürdige Quelle	9
noch keine riskante Handlung durchgeführt	29

* Mehrfachnennungen möglich. Quelle: Proofpoint

Was verführt

Gründe für riskante Handlungen in Unternehmen; Endnutzerinnen und -nutzer (n=7 500) und Sicherheitsexpertinnen und -experten (n=1 050) aus 15 Ländern weltweit; 2023; in Prozent *

* Mehrfachnennungen möglich. Quelle: Proofpoint

Die Mobilfunkforensik arbeitet im Großraum, manchmal mit robusten Methoden: Hier werden Chips aus Handys geschraubt und – wenn es sein muss – mittels Bohrer oder Hitze von der Platine gelöst.

Die Trickbot-Gruppe arbeitet organisiert, hierarchisch gegliedert.

Fotos: iStock

Nicht allein gegen die Cybermafia

Von einem Dresdner Altbau aus wird ein so stiller wie effektiver Kampf geführt: Die Polizisten im Cybercrime Competence Center Sachsen gehen gegen international verflochtene Banden von Online-Kriminellen vor. Ihre stärksten Waffen heißen Zusammenarbeit und Vertrauen.

Text und Foto: Daniel Erk

Allein schon das Wort ruft Bilder im kollektiven Gedächtnis hervor: „Cyberkriminalität“ scheint auf ewig mit abgedunkelten Räumen in kühlen Glasbauten verbunden zu sein. Über riesige Monitorwände laufen dort endlose Datenreihen aus Nullen und Einsen durch, selbstverständlich in Grün auf Schwarz. Nur: Mit dem Alltag im Cybercrime Competence Center (SN4C) des Landeskriminalamts Sachsen am Stadtrand von Dresden haben diese so eindrücklichen wie schlichten Vorstellungen rein gar nichts zu tun. Zwar türmt sich auch in den Räumen des SN4C modernste IT-Technik, doch ansonsten ist die Welt der Cyberkriminalität und deren Bekämpfung deutlich komplexer.

Mit federnden Schritten läuft Henrik Hohenlohe über den weiten Flur eines Dresdner Altbaus. Seit 2016 ist der 46-jährige Kriminaloberrat Leiter des SN4C, der größten Organisationseinheit in der Abteilung 3 des sächsischen Landeskriminalamtes (LKA). Hohenlohe hat beste Laune: Seine Leute waren gerade wichtiger Bestandteil eines internationalen Coups. Europol nennt den Erfolg in einer Pressemeldung „die größte jemals durchgeführte Operation gegen Bot-Netze“ und einen „Schlag gegen das Ökosystem von Dropper-Malware“. Dropper wie IcedID, SystemBC, Pikabot, Smokeloader und Bumblebee wären lahmgelegt, mehr als 2 000 Domains unter Kontrolle gebracht und weltweit mehr als hundert Server abgeschaltet oder gestört worden, unter anderem in Großbritannien, Kanada, Bulgarien, den USA und der Ukraine. Nach 16 Durchsuchungen in mehreren Ländern konnten vier Personen festgenommen werden, drei in der Ukraine, eine in Armenien. Klangvoller Name der gelungenen Operation: „Endgame“.

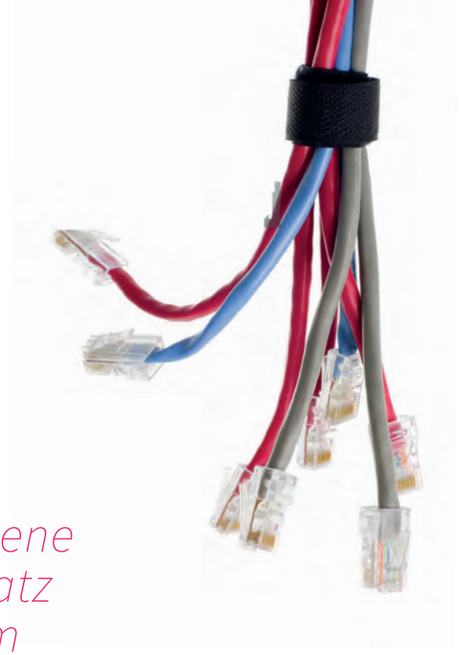
Sieben auf einen Streich

Später veröffentlicht das Bundeskriminalamt (BKA) in Wiesbaden die Namen und Gesichter von acht weiteren Beschuldigten, die nun auf der „Europe’s Most Wanted“-Liste von Europol stehen. Sieben Tatverdächtige, heißt es auf der Seite des BKA, stehen „im Verdacht, Mitglied der Trickbot-Gruppierung (…) gewesen zu sein. Diese Gruppierung ist seit mindestens 2016 aktiv und verwendete verschiedene Schadsoftware-Varianten (…), um Computersysteme zu infizieren, sensible Daten zu stehlen und in vielen Fällen sogenannte Ransomware nachzuladen, mit welcher die Systeme verschlüsselt und ein Lösegeld, zahlbar in Kryptowährungen, zur Entschlüsselung verlangt werden konnte.“

Nach den Ermittlungen des Bundeskriminalamtes hatte die mindestens seit 2016 aktive „Trickbot-Gruppe“, wie sie sich selbst nannte, mehr als hundert Mitglieder und „arbeitet organisiert, hierarchisch gegliedert“ sowie „projekt- und gewinnorientiert“. Die Gruppierung sei verantwortlich für die Infektion von „mehreren Hunderttausend Systemen in Deutschland und weltweit“, darunter Behörden, Krankenhäuser, Unternehmen und auch Privatpersonen.

Dropper sind unerkannte Einfallstore zu Computern oder ganzen Systemen, weshalb sie oft auch als Trojanische Pferde bezeichnet werden. Die Dropper selbst richten meist keinen ›

Kriminaloberrat Henrik Hohenlohe ist seit acht Jahren Cyberkrieger von Staats wegen – und so sieht er aus, wenn seinem Team gerade ein großer Fisch ins digitale Netz gegangen ist.



„Der täterbezogene Ermittlungsansatz gleicht oft einem Hase-und-Igel-Spiel.“

–Henrik Hohenlohe

Schaden an. Sie werden oft durch Mails ungewollt installiert und von der Virensoftware nicht als Problem erkannt, ganz einfach, weil es keine Viren sind. Jedoch kann über sie Schadsoftware „nachgeladen“ werden. Schaltet man also die Dropper aus, indem man die dazugehörigen Botnetze angreift, nimmt man Cyberkriminellen eines ihrer wichtigsten Werkzeuge.

Lieber die Infrastruktur lahmlegen

Genau darin sind Henrik Hohenlohe und sein Team ziemlich gut. „Wir verfolgen mittlerweile auch den sogenannten Infrastrukturansatz, weil er aus unserer Sicht effektiver ist“, erklärt Hohenlohe. „Neben dem täterbezogenen Ermittlungsansatz, der oft ein Stück weit einem Hase-und-Igel-Spiel zwischen den Strafverfolgungsbehörden und den Tätern gleicht, verfolgen wir damit das Ziel, die zugrunde liegende Infrastruktur der Täter lahmzulegen.“

Allein kann das sächsische Cybercrime Competence Center mit seinen rund 90 Mitarbeitenden gegen das digital organisierte Verbrechen jedoch nicht viel ausrichten. Erst im Verbund mit Ermittlungsbehörden anderer Bundesländer, dem BKA und internationalen Partnern wie etwa dem FBI kann eine Operation wie „Endgame“ gelingen.

Hohenlohe eilt weiter über die Flure bis zu jenem Großraum, in dem die Mobilfunkforensik arbeitet. Hier werden Chips aus Handys geschraubt und – wenn es sein muss – mittels Bohrer oder Hitze von der Platine gelöst. Fast egal, wie sehr ein Handy zerstört oder verschlüsselt wurde, am Ende kommt das LKA fast immer an die Daten, erzählt Hohenlohe – mit ein wenig Stolz in der Stimme.

Zurück in seinem schmucklosen Büro nimmt er an einem Resopaltisch Platz, darauf ein MacBook, ein paar Ordner mit Ermittlungsakten, Unterlagen zu „Business Intelligence“. An der Wand hängt eine Kinderzeichnung von einem Roboter in Rot und Blau, darunter steht „Viel Spaß im LKA“. Doch mit Spaß hat Hohenlohes Arbeit selten zu tun, viel zu massiv ist mittlerweile der Schaden, den Cyberkriminalität anrichtet. Sie ist eine mächtige Sparte des Organisierten Verbrechens.

„Straftaten im Bereich Cybercrime liegen in Deutschland weiter auf einem hohen Niveau“ heißt es im letztjährigen „Bundeslagebild Cybercrime“ des BKA. Während die Zahl der ausschließlich in Deutschland verübten Verbrechen mit knapp 135 000 in den vergangenen Jahren in etwa konstant geblieben ist, steigt die Zahl der vom Ausland aus in Deutschland verübten Cyberverbrechen seit ihrer Erfassung im Jahr 2020 Jahr für Jahr. 2023 waren es laut „Bundeslagebild Cybercrime“ 28 Prozent mehr Cyberverbrechen „im engeren Sinne“ aus dem Ausland. Den Gesamtschaden in 2023 schätzt der IT-Branchenverband Bitkom auf rund 148 Milliarden Euro. „So wie alles andere in unserer Gesellschaft digitalisiert sich auch die

Fotos: iStock

Kriminalität“, sagt Hohenlohe schulterzuckend. „Mittlerweile findet in den meisten Ermittlungsverfahren eine Auswertung digitaler Spuren statt.“

Die Grenzen zwischen analoger, sozusagen klassischer, und digitaler Kriminalität verwischen zunehmend. Wann eine Straftat ein ausgewiesenes Cyberverbrechen ist, lässt sich nicht mehr klar beantworten. Vielleicht schon, wenn für die Vorbereitung ein Smartphone benutzt wurde? Oder doch erst, wenn Datenbanken entwendet oder ganze IT-Systeme blockiert wurden? Für Hohenlohe ist das nur „eine akademische Frage“. Seine Abteilung kümmert sich sowieso um alle diese Fälle, ausnahmslos.

Die Module des Verbrechens

Deutsche Ermittlungsbehörden unterscheiden offiziell dennoch zwischen Cyberkriminalität „im weiteren und im engeren Sinne“. Der Unterschied: Erstere fasst alle Straftaten zusammen, bei denen in irgendeiner Form Computer, das Internet oder Mobiltelefone für „herkömmliche Verbrechen“ wie Betrugsdelikte oder Kinderpornografie genutzt wurden, quasi Verbrechen mit IT. Hier leistet Hohenlohes Abteilung schlicht Ermittlungsunterstützung: Daten sichern, Handys oder Rechner aufschrauben, Mikrochips lösen und auslesen.

Das andere, also die Cyberkriminalität im engeren Sinn, erklärt Hohenlohe, meint sämtliche Angriffe auf IT-Systeme und Datenbanken: Phishing, Hacking, Ransomware.

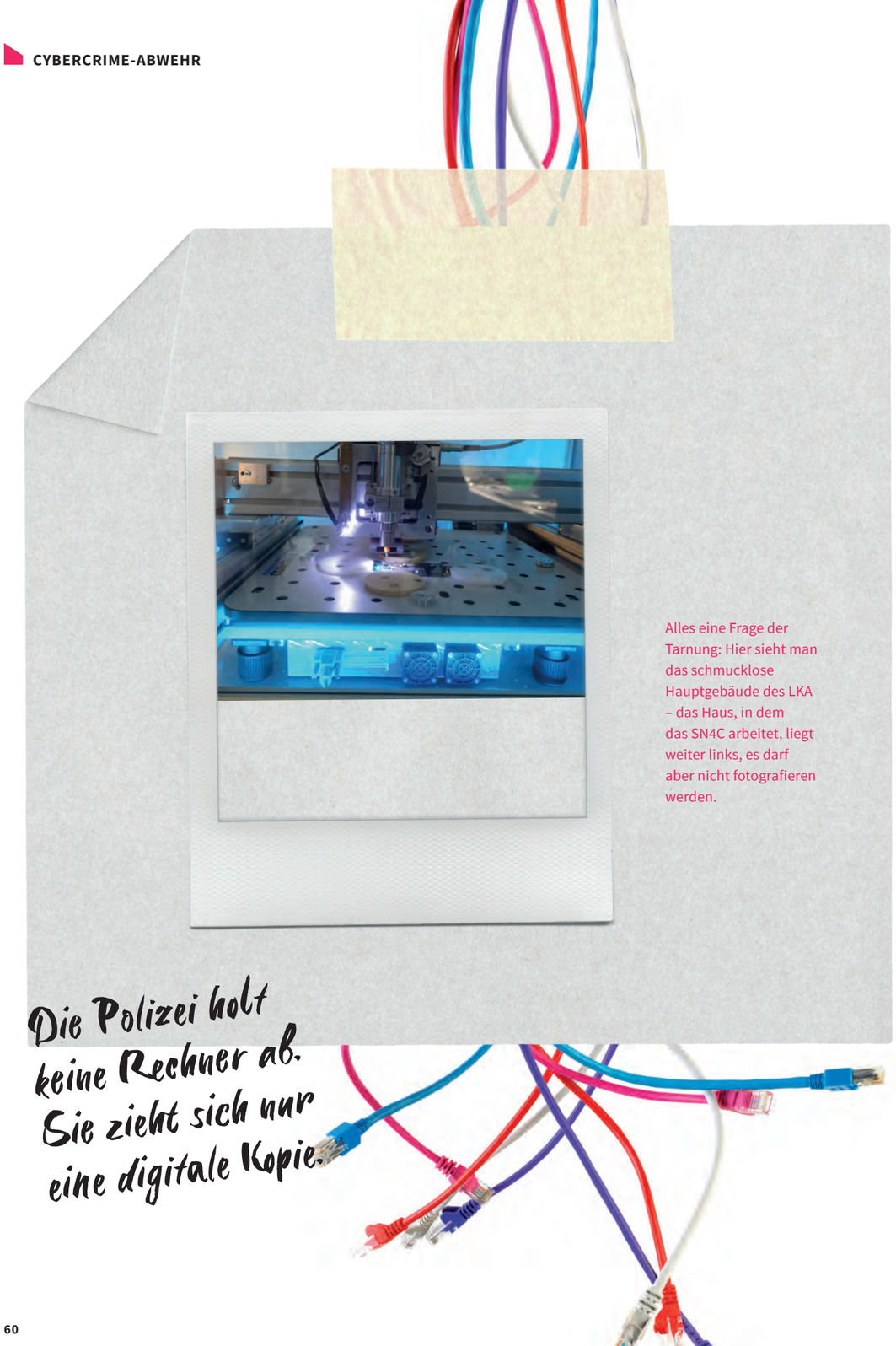
Selbstverständlich habe man in Dresden die wichtigen Basiskompetenzen alle im Haus, sagt Hohenlohe. Mit der Zahl von rund 90 Mitarbeitenden sei es jedoch unmöglich, alle Bereiche und Fähigkeiten zu hundert Prozent abzudecken. Das sei mittlerweile aber auch gar nicht mehr notwendig. Die bundes- und europaweite Zusammenarbeit unter den Ermittlungsbehörden funktioniere heute so gut, dass man sich eng austausche und gegenseitig unterstütze.

Letztlich verfolgen Ermittlungsbehörden überall auf der Welt immer dieselben Täter, die immer dieselben Straftaten begehen – oft erfolglos, weil die Verbrechen unübersichtlich und komplex sind. Die internationale Zusammenarbeit helfe, ein klareres Bild der Täter und ihrer Taten zu bekommen, erklärt Hohenlohe. Mit aufwendig konzertierten Operationen wie „Endgame“ ließen sich Strukturen von Cyberkriminellen zerstören und Täter vor Gericht bringen. Dafür steuert jede Cybercrime-Behörde ihre individuellen Kompetenzen bei. In Dresden zum Beispiel, sagt Hohenlohe, haben sie einen ausgewiesenen Experten für Kryptowährungen. Dessen Fähigkeiten frage auch schon mal das US-amerikanische FBI an.

Insofern machten es die Ermittler nicht anders als die Verbrecher, sagt Hohenlohe: Man nutzt den Sachverstand anderer Experten zu eigenen Zwecken. „Heutzutage braucht man als Täter eigentlich keine tiefgreifenden Programmierkenntnisse mehr, schließlich gibt es das, was wir ‚Cybercrime as a Service‘ nennen.“ Kriminelle können längst alle Module eines Verbrechens, wie Hohenlohe sie nennt, zusammenstellen und in jedem Bereich – von den Phishing Mails über das Eindringen in die Datenbanken bis hin zum Wissen um Kryptowährungen zur Auszahlung des Lösegeldes – auf eine enorme Spezialisierung und Professionalisierung zurückgreifen. „Diese Infrastruktur ist international und anonym“, sagt Hohenlohe. Die verschiedenen Täter würden sich untereinander oft gar nicht mehr kennen. Um solche Netzwerke aufzutun und zu zerstören, bräuchten Strafverfolgungsbehörden ähnliche Strukturen. „Wir stellen diesen internationalen Systemen der Täter ein internationales System der Strafverfolgung gegenüber“, fasst Hohenlohe zusammen.

Kriminaloberkommissarin Sabine Schütz arbeitet im LKA Sachsen für die sogenannte ZAC, die Zentrale Ansprechstelle Cybercrime. Auch wenn Schütz Informatik studierte, eine Zeit lang als Frontend-Entwicklerin und in der Suchmaschinenoptimierung gearbeitet hat – ihr Kindheitstraum war immer die Arbeit bei der Polizei, erzählt die 38-Jährige. Schütz hat acht Jahre im Ermittlungsdienst des sächsischen Cybercrime-Zentrums gearbeitet und ist heute die Frau, die sächsische Unternehmen im Idealfall anrufen, wenn sie ein Problem mit Hackern und/oder Erpressern haben. ›

Sabine Schütz ist auf ZAC, also Ansprechpartnerin bei der Zentralen Ansprechstelle Cybercrime: Wenn sächsische Unternehmen einen Angriff auf ihre Systeme vermuten, rufen sie im Idealfall die Polizistin an.



Alles eine Frage der Tarnung: Hier sieht man das schmucklose Hauptgebäude des LKA – das Haus, in dem das SN4C arbeitet, liegt weiter links, es darf aber nicht fotografieren werden.

Die Polizei holt keine Rechner ab. Sie zieht sich nur eine digitale Kopie.

Fotos: iStock

Wie so ein Angriff aussehen kann, erläutert sie in der Praxis regelmäßig. In ihrer Standardpräsentation mit dem Titel „Cybercrime – Phänomene und polizeiliche Handlungsfelder“ skizziert sie das Schreckensszenario einer typischen Cybererpressung. In der betroffenen Firma gehen Mails ein, in denen es zum Beispiel heißt: „Alle Ihre Dateien wurden verschlüsselt. Dies umfasst (ist aber nicht darauf beschränkt) Fotos, Dokumente und Tabellenkalkulationen.“ Es folgen eine Bitcoin-Adresse sowie die Erklärung, wie die Daten im Falle einer Zahlung wieder zu entschlüsseln seien.

Mit mehr als zehn Prozent aller Anzeigen stehen solche Ransomware-Erpressungen in Sachsen auf Platz 3 der Cyberangriffe 2023. Dabei schätzen Experten das Dunkelfeld – also die Zahl der nicht angezeigten Straftaten – auf bis zu 91,5 Prozent. Anders gesagt: Nicht einmal zehn Prozent der Opfer von Phishing, Hacking und digitaler Erpressung zeigen die verübten Verbrechen an. Der Rest zahlt. Und schweigt.

Wenn Irrglaube teuer wird

Durchschnittlich 621 858 US-Dollar – also insgesamt mehr als 1,1 Milliarden Euro – zahlten nach Angaben des BKA im vergangenen Jahr Unternehmen an solche Erpresser, um möglichst schnell wieder an ihre Daten oder in ihre Systeme zu kommen. Und auch, um nicht öffentlich bekennen zu müssen, wie schlecht sie ihre IT gesichert haben.

Nach der unzureichenden Sicherung der Systeme machen Unternehmen hier gleich den zweiten Fehler, weiß Sabine Schütz. Doch sie weiß auch, dass es dafür nachvollziehbare Gründe gibt. In ihrer Präsentation vor Unternehmen listet sie die größten Vorurteile gegenüber ihrer Cybercrime-Abteilung auf. „Lösegeld zahlen vs. nicht zahlen?“ – das steht ganz oben auf ihrer Liste. „Die Entscheidung bleibt in Ihrer Hand! Die Polizei rät zum ‚nicht bezahlen‘“. Direkt darunter heißt es: „Die finden den Täter doch sowieso nicht!“ Und: „Die Polizei nimmt unsere Technik mit!“ Es sei genau dieser Irrglaube, der von Cybercrime betroffene Unternehmen davon abhalte, sich an die Polizei zu wenden, sagt Schütz.

Auch Henrik Hohenlohe ordnet ein: „Es hält sich ja immer noch die Vorstellung, wir kommen mit einer Hundertschaft auf den Hof, nehmen die gesamte Rechentechnik mit, und das Unternehmen kann deshalb nicht mehr weiterarbeiten.“ Tatsächlich aber reiche für die Ermittlungen eine forensische Kopie, also ein Duplikat, bei dem Bit für Bit alle Dateien, Ordner, aber auch der nicht genutzte oder freigegebene Speicherplatz kopiert werden. Nur die Rechner von Tatverdächtigen würden beschlagnahmt.

Dann beginnen die digitalen Ermittlungen. Logfile für Logfile, Datei für Datei suchen Hohenlohes Leute nach Spuren, die die Kriminellen hinterlassen haben könnten – ähnliche Strukturen und Codes in der Programmierung, Formulierungen in den Mails, ein bestimmtes Vorgehen im Digitalen und Finanziellen. So, erzählt Schütz, lasse sich trotz aller Abstraktheit des Digitalen doch ein recht konkretes Muster des jeweiligen Verbrechens herausarbeiten.

Die Cyberermittlungen werden von den klassischen Instrumenten der Polizeiarbeit ergänzt: Befragungen, Verhöre, Fingerabdrücke. Bestimmte interne Informationen seien in Unternehmen nur beschränkten Personenkreisen zugänglich, sagt Schütz. Deshalb stellen sich die Fragen: Wer wusste was? Wer hat welche Informationen weitergegeben? Und wie und wo könnte schädliche Software ins System gelangt sein? Aus den Antworten füge sich dann ein Bild des Verbrechens. Im besten Fall könne man im Anschluss konkrete Verdächtige ausmachen.

Was heißt hier eigentlich Erfolg?

„Der Fokus der polizeilichen Ermittlung richtet sich zunächst auf den oder die Täter. Das ist sozusagen der erste Strang“, sagt Henrik Hohenlohe. „Der zweite Strang ist deren Infrastruktur, die es zu bekämpfen gilt. Als dritten Bekämpfungsstrang kann man aber auch den Vertrauensverlust bezeichnen, den Täter oder Tätergruppierungen in der Szene bei Erfolgen der Strafverfolgung erleiden. Im Optimalfall bringt man diese drei Komponenten zusammen, um das Phänomen in den Griff zu bekommen.“

Erfolge wie die Operation „Endgame“ seien vor allem auch so wichtig, weil sie Opfern von Cyberkriminalität signalisieren: Die Polizei ist nicht machtlos! Das Internet ist auch faktisch kein rechtsfreier Raum. Der Erfolg schafft im besten Fall Vertrauen. Und das Vertrauen sorgt, im besten Fall, für mehr Anzeigen und mehr Informationen – und damit wiederum für mehr Erfolge.

Wobei sich die Frage aufdrängt: Was heißt eigentlich Erfolg? Wie bei allen Arten von Polizeiarbeit wird es auch im Bereich Cyberkriminalität nie möglich sein, ein Verbrechen für immer und vollkommen zu verhindern, räumt Experte Hohenlohe ein. Ja, manche Formen von Phishing hätten in den vergangenen Jahren deutlich abgenommen. Gleichzeitig aber seien andere Formen des massenhaften digitalen Betrugs in die Höhe geschossen.

Die zukünftige Entwicklung der Cyberkriminalität zeichnet sich bereits deutlich ab. „Das große Thema ist sicherlich künstliche Intelligenz. Ganz einfach weil viele Scams damit automatisiert werden können und die Mails und ihre Gestaltung viel glaubhafter generiert werden können“, sagt Hohenlohe. Es ist bald kaum mehr damit zu rechnen, dass sich technisch weniger versierte Cyberkriminelle durch fragwürdige Formulierungen oder nachlässige Gestaltung in und von Spam-Mails verraten. Umso entscheidender ist und bleibt der Faktor Mensch. Aufmerksame Mitarbeiterinnen und Mitarbeiter bieten den wirksamsten Schutz vor Cyberkriminalität.

WIRTSCHAFT

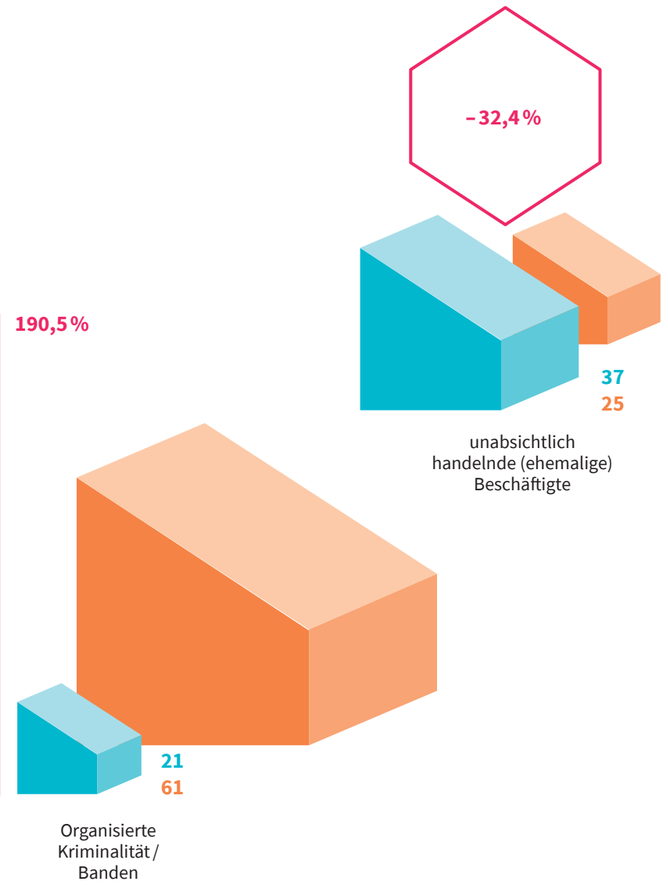
Die Zahl der Cyberangriffe steigt kontinuierlich, die Kriminellen rüsten auf – und treffen auf weit geöffnete Einfallstore. In Unternehmen und Organisationen fehlt es an Fachkräften und Kompetenzen, an Sicherheitskonzepten und -technologien, an Strukturen und Prozessen – und nicht selten an der Einsicht in die Notwendigkeit all dessen.

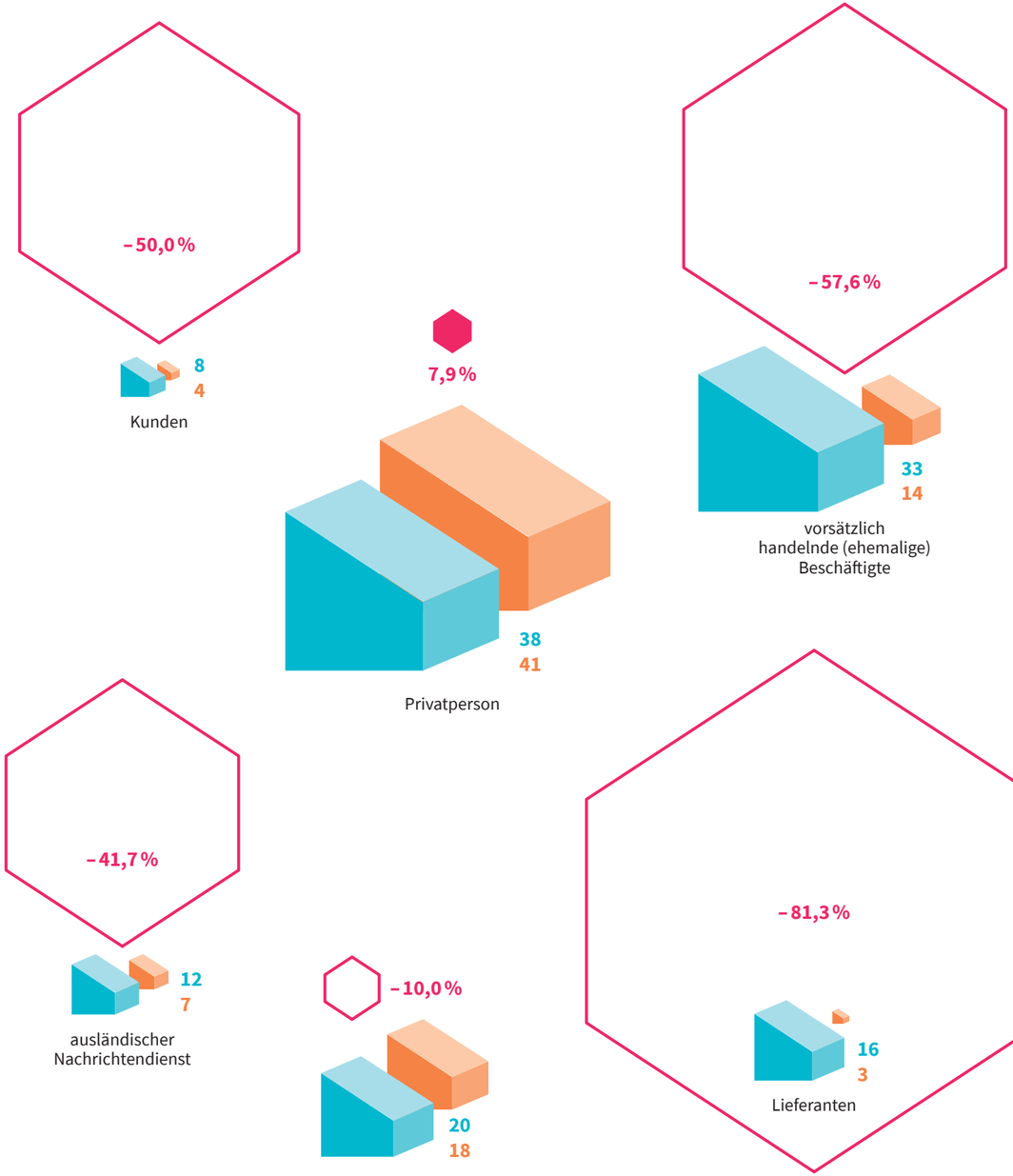
Kriminelle Banden

IT-Angriffe auf Unternehmen nach Täterkreis; Unternehmen, die in den vergangenen zwölf Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (2023: n=1 002; 2019: n=801); Deutschland; in Prozent *

Von welchem Täterkreis gingen die Handlungen in den vergangenen 12 Monaten aus?

2019 2023 Veränderung 2019 – 2023



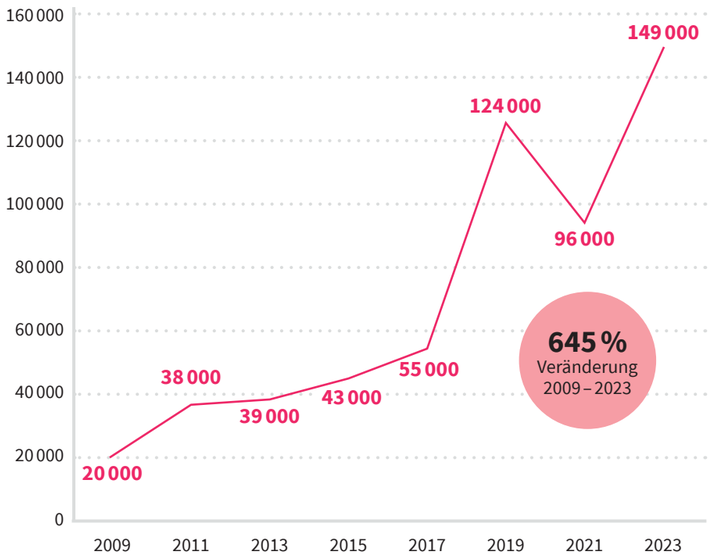


* Mehrfachnennungen möglich. Quelle: Bitkom

Glossar der Cyberbegriffe auf Seite 100 – 103

Unbesetzt

Zahl zu besetzender IT-Stellen in der Gesamtwirtschaft; Unternehmen ab drei Beschäftigten (n=853); Deutschland



Quelle: Bitkom

Unentschieden

Auswirkungen des IT-Fachkräftemangels; Unternehmen in Deutschland (n=501); 2023; in Prozent

„Aufgrund des IT-Fachkräftemangels sind wir zunehmend auf externe Dienstleister angewiesen."

49
stimme voll zu / eher zu

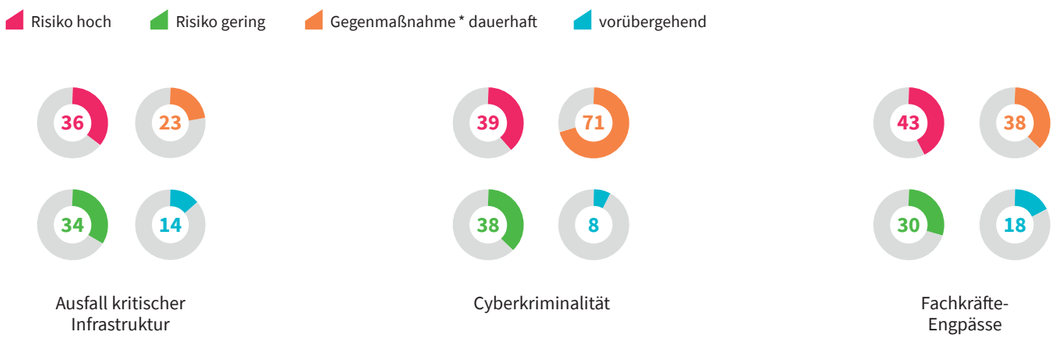
48
stimme eher nicht / gar nicht zu

3
weiß nicht / keine Angabe

Quelle: TÜV-Verband

Ungeschützt

Risikobewertung von Unsicherheitsfaktoren und Gegenmaßnahmen; bayerische Unternehmen aus dem Industrie-Dienstleistungsverbund (n=300); Deutschland; 2023; in Prozent

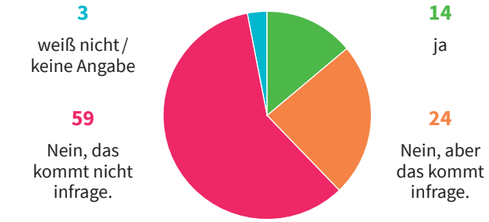


* Falls bereits Gegenmaßnahmen gegen das genannte Risiko ergriffen wurden, erfolgte die weitere Frage, ob diese Maßnahmen dauerhaft oder vorübergehend sind. Quelle: vbw

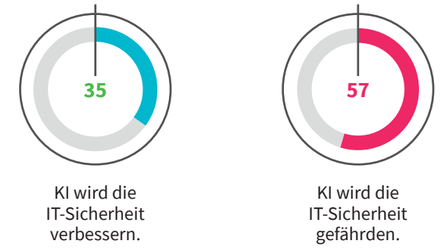
Unheimlich

Anteil der Unternehmen, die KI zur Verbesserung der IT-Sicherheit einsetzen; Unternehmen mit mindestens zehn Beschäftigten und einem Jahresumsatz von einer Million Euro oder mehr (n=1 002); Deutschland; 2023; in Prozent

Haben Sie sich in Ihrem Unternehmen bereits mit dem Einsatz von KI zur Verbesserung der IT-Sicherheit beschäftigt?



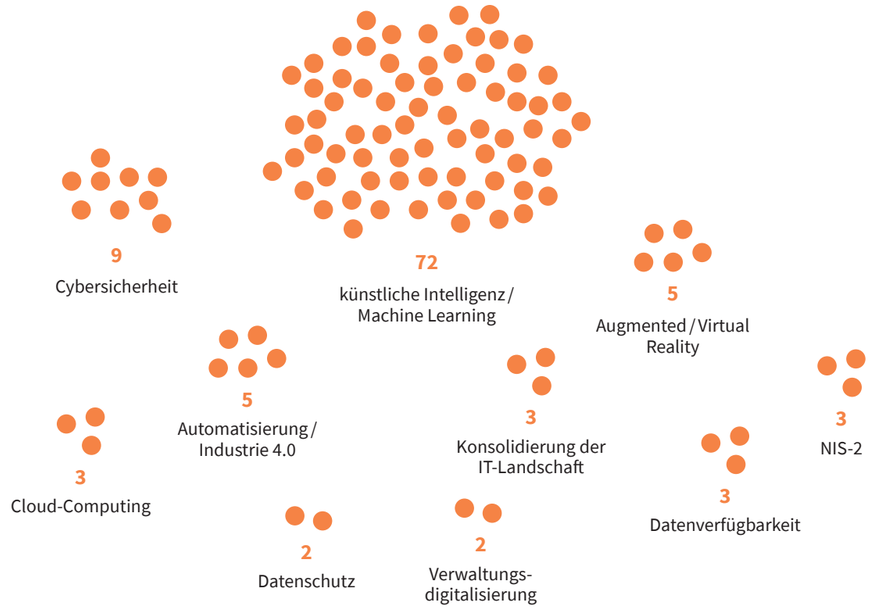
Welcher Aussage stimmen Sie am ehesten zu?



Quelle: Bitkom

Unangefochten

Digital-Trends im Jahr 2024; Umfrage in mittelständischen Unternehmen (n=105); Deutschland; 2023; in Prozent



Quelle: Bundesverband IT-Mittelstand e. V. (bitmi)

Unverzichtbar

Relevanz von Technologien für die Kunden von IT-Service-Unternehmen; IT-Service-Unternehmen in Deutschland; 2023 / 2024; Werte für die Optionen „sehr relevant“ und „eher relevant“ in Prozent *

Data & Analytics	DevOps	Cloud-native	künstliche Intelligenz	Costumer Experience	Low Code / No Code	RPA / Robotics
92	92	91	83	83	65	63

Industry-Cloud-Plattformen	souveräne Cloud	Composable Enterprise	Campusnetze, 5G & Edge Computing	Virtual Reality / Augmented Reality	Web 3.0 / Metaverse
51	47	46	34	30	27

* Mehrfachnennungen möglich. Quelle: Lünendonk

Unrettbar

Bewertung von Aussagen im Bereich Wirtschaftsschutz; Unternehmen, die in den vergangenen zwölf Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (2023: n=1 002; 2015: n=550); Deutschland; in Milliarden Euro

Wodurch sind Ihrem Unternehmen innerhalb der vergangenen zwölf Monate Schäden im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

2015 2023 Veränderung 2015 – 2023

Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	Erpressung mit gestohlenen oder verschlüsselten Daten	datenschutzrechtliche Maßnahmen (z. B. Information von Kunden)	Patentrechtsverletzungen (auch schon vor der Anmeldung)	Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	Umsatzeinbußen durch nachgemachte Produkte (Plagiate)
386 %	973 %	520 %	11 %	236 %	33 %
7,2	1,5	2,0	9,4	6,4	11,5
35,0	16,1	12,4	10,4	21,5	15,3

Imageschaden bei Kunden oder Lieferanten / negative Medienberichterstattung	Kosten für Ermittlungen und Ersatzmaßnahmen	Kosten für Rechtsstreitigkeiten	höhere Fluktuation / Abwerben von Mitarbeitenden	sonstige Schäden	**Gesamtschaden pro Jahr**
498 %	k. A.	359 %	k. A.	1 000 %	302 %
5,9	k. A.	6,5	0,9	0,1	51,2
35,3	25,2	29,8	k. A.	1,1	205,9

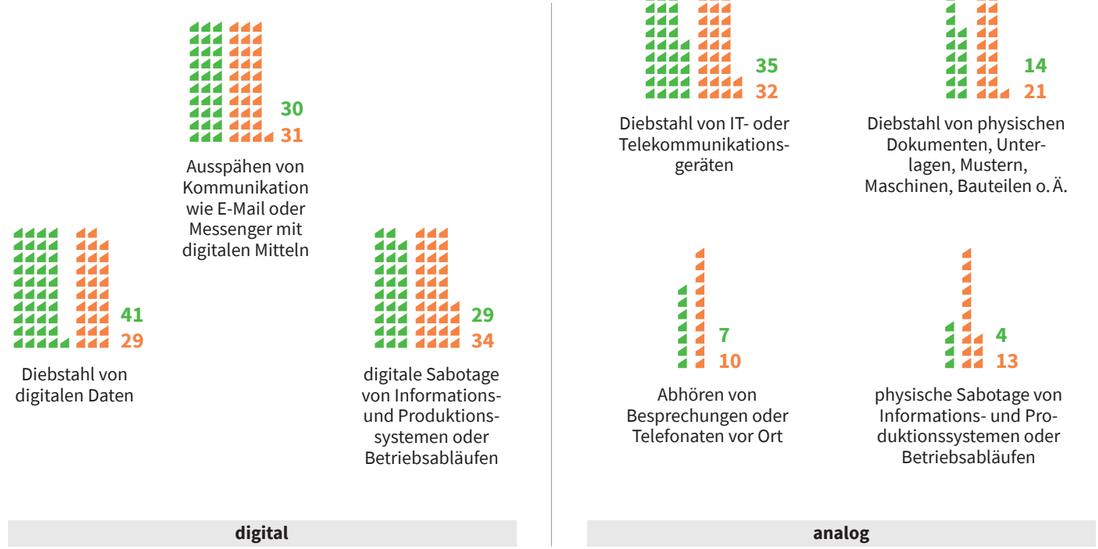
Quelle: Bitkom

Unkalkulierbar

IT-Angriffe auf Unternehmen nach Art des Angriffs; Unternehmen mit mindestens zehn Beschäftigten und einem Jahresumsatz von einer Million Euro oder mehr (n=1 002); Deutschland; 2023; in Prozent *

Von welchen der folgenden Handlungen war Ihr Unternehmen innerhalb der vergangenen 12 Monate (vermutlich) betroffen?

betroffen vermutlich betroffen



* Mehrfachnennungen möglich. Quelle: Bitkom

Unübersehbar

Angriffsparameter von DDoS-Attacken; Deutschland; 2023

1 875
durchschnittliche Angriffe pro Monat

658 Mbit / s
durchschnittliche Bandbreite

45 Minuten
durchschnittliche Dauer eines Angriffs

Quellen: BKA, Deutsche Telekom

Unersetzbar

Häufigste Ransomware-Angriffsziele; Deutschland; 2022 – 2023

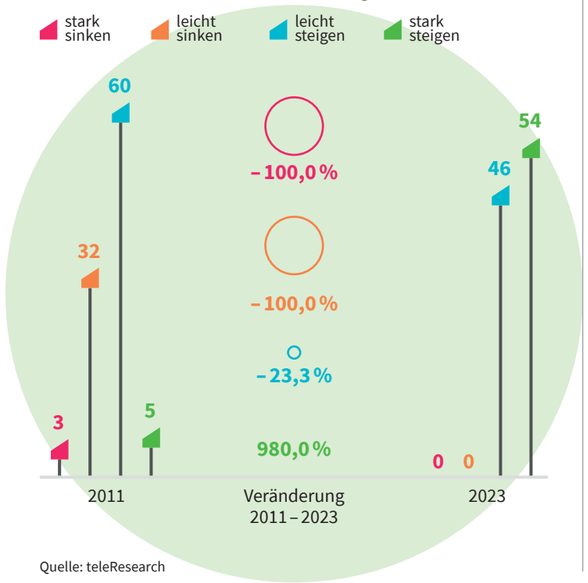
Forschungs- und Bildungseinrichtungen	30
Kommunen und kommunale Betriebe	27
Krankenhäuser	4
Sonstige	3
andere	68
davon kleine Unternehmen *	3
davon mittlere Unternehmen *	59
davon große Unternehmen *	6

* kleine Unternehmen: weniger als 50 Mitarbeitende; mittlere Unternehmen: 50 bis 249 Mitarbeitende; große Unternehmen: 250 Mitarbeitende und mehr. Quelle: BSI

Befürchtungen

Zukünftige Bedeutung von Cyberangriffen / Datenklau für Unternehmen; Führungskräfte deutscher Unternehmen (n=509); in Prozent

Wie wird sich die Bedeutung des Problems Cyberangriffe / Datenklau für Ihr Unternehmen künftig entwickeln?

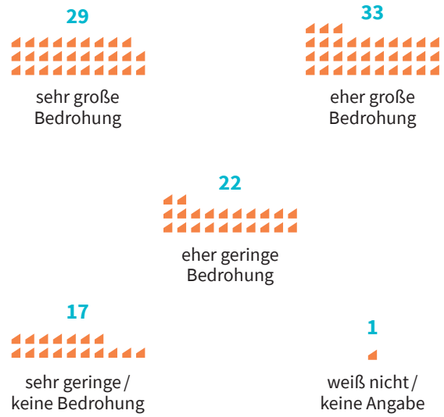


Quelle: teleResearch

Bedrohungen

Bedrohungsgefühl durch analoge und digitale Angriffe; deutsche Unternehmen (n=1 002); 2023; in Prozent

Inwieweit sehen Sie analoge und digitale Angriffe als Bedrohung für Ihr Unternehmen?



Quelle: Bitkom

Sorgen

Sorgen der Unternehmen in Hinblick auf die Folgen eines möglichen Cyberangriffs; Führungskräfte aus den Bereichen Business, Technologie und Sicherheit (n=274); Deutschland; 2023; in Prozent *

49 Einnahmensverluste

47 Verlust von Kunden-, Mitarbeiter- oder Transaktionsdaten

46 Schaden an der Unternehmensmarke

37 Schaden an der Produkt- oder Servicequalität

35 Verlust von geistigem Eigentum

32 Betriebsunterbrechungen

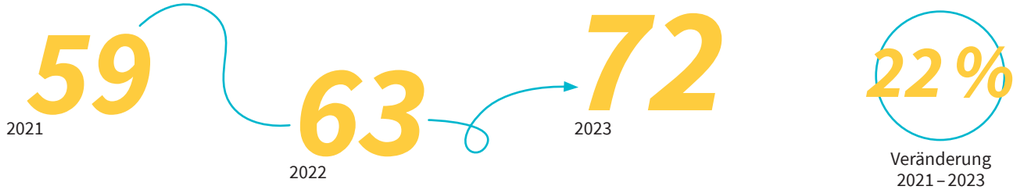
22 straf- oder zivilrechtliche Haftung

19 Verletzung oder Tod

* Mehrfachnennungen möglich. Quelle: PwC

Schäden

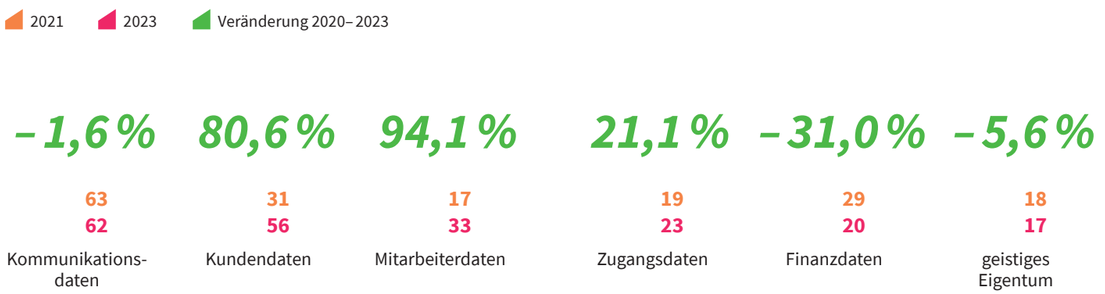
Anteil am entstandenen Gesamtschaden, der auf Cyberattacken zurückgeführt werden kann; Unternehmen mit mindestens zehn Beschäftigten und einem Jahresumsatz von einer Million Euro oder mehr (n=726); Deutschland; in Prozent



Quelle: Bitkom

Daten

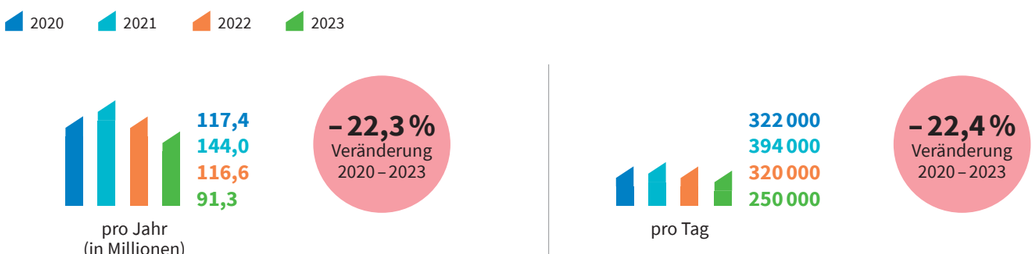
Art der gestohlenen Daten; Unternehmen mit mindestens zehn Beschäftigten und einem Jahresumsatz von einer Million Euro oder mehr (n=411); Deutschland; in Prozent *



* Mehrfachnennungen möglich. Quelle: Bitkom

Perspektiven

Zahl neuer Schadprogramm-Varianten; Deutschland; 2023

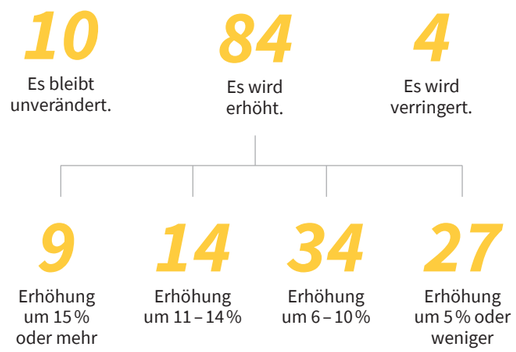


Quelle: BSI

Erwartet

Entwicklung des Cyberbudgets; Führungskräfte aus den Bereichen Business, Technologie und Sicherheit (n=274); Deutschland; 2024; in Prozent

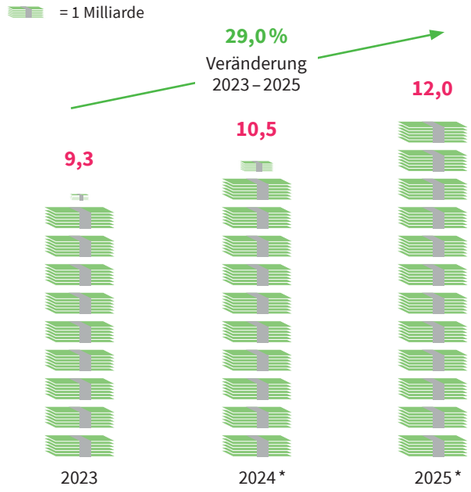
Wie wird sich das Cyberbudget Ihrer Organisation im Jahr 2024 verändern?



Quelle: PwC

Geplant

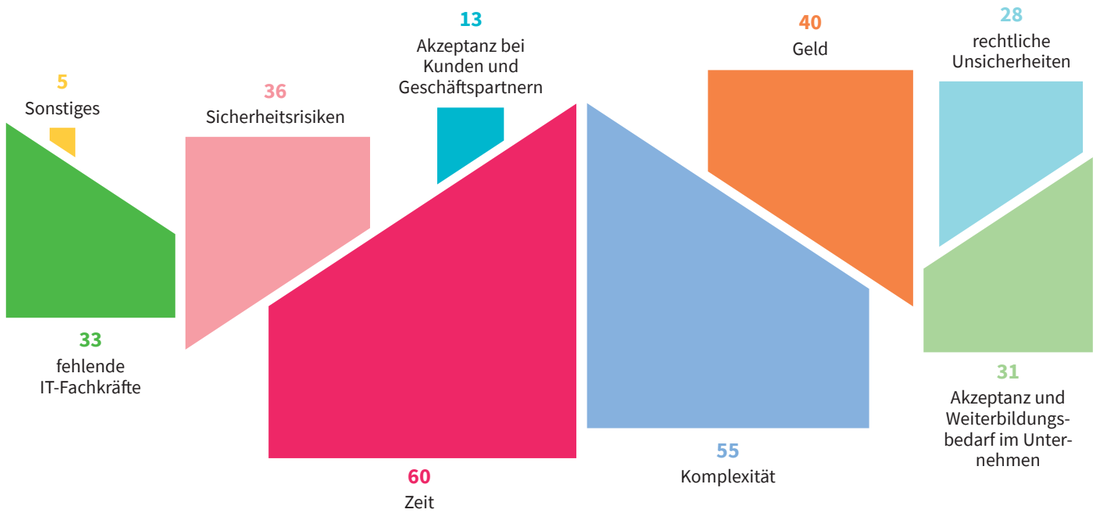
Entwicklung der Ausgaben für IT-Sicherheit; Deutschland; in Milliarden Euro



* Prognose. Quelle: Bitkom

Geahnt

Herausforderungen der Digitalisierung; Digitalisierungsumfrage der IHKs zum Thema Daten- und Informationssicherheit in Unternehmen (n=4 000+); Deutschland; 2023; in Prozent



Quelle: DIHK

Definiert

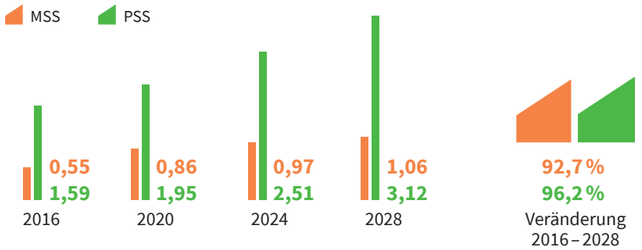
Zuständigkeit für die Berichterstattung über Cyber- und Datenschutzrisiken an die Geschäftsleitung; Führungskräfte aus den Bereichen Business, Technologie und Sicherheit (n=242); Deutschland; 2022; in Prozent

Wer ist in Ihrer Organisation in erster Linie für die Berichterstattung über Cyber- und Datenschutzrisiken an die Geschäftsleitung verantwortlich?

Quelle: PwC

Umgesetzt

Umsatz mit Managed Security Services und Professional Security Services; Deutschland; in Milliarden Euro



Quelle: Statista Market Insights

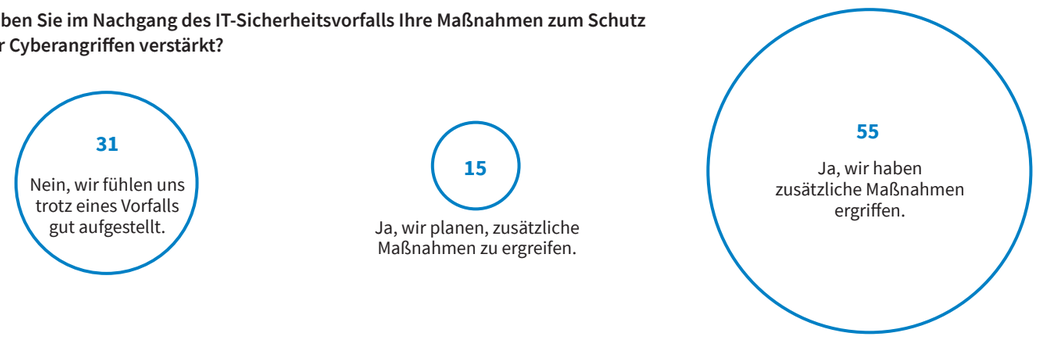
Managed Security Services (MSS) bieten kontinuierliche, rund um die Uhr laufende Überwachungs- und Verwaltungsdienste, die darauf abzielen, die allgemeine Sicherheitslage eines Unternehmens proaktiv zu verbessern und zu verwalten. Beispiele: 24/7-Sicherheitsüberwachung und -management oder Managed Firewall Services.

Professional Security Services (PSS) hingegen sind spezialisierte, zeitlich begrenzte Dienstleistungen, die auf spezifische Sicherheitsprojekte oder -initiativen fokussiert sind und oft tiefgehende Beratung und Expertise bieten. Beispiele: Durchführung eines Penetrationstests oder Entwicklung und Implementierung einer neuen Sicherheitsstrategie.

Ergänzt

Zusätzliche Schutzmaßnahmen nach einem IT-Sicherheitsvorfall; Unternehmen, die in den vergangenen zwölf Monaten mindestens einen IT-Sicherheitsvorfall hatten; Deutschland; 2023; in Prozent

Haben Sie im Nachgang des IT-Sicherheitsvorfalls Ihre Maßnahmen zum Schutz vor Cyberangriffen verstärkt?



Quelle: TÜV-Verband

Mehr Sicherheit

Strategische, organisatorische und technische Maßnahmen für mehr Cybersicherheit; Unternehmen in Deutschland (n=4 114); 2023; in Prozent *

* Mehrfachnennungen möglich. Quelle: DIHK

Mehr Maßnahmen

Kompetenzen für die Verbesserung der IT-Sicherheit; Unternehmen in Deutschland (n=501); 2023; in Prozent *

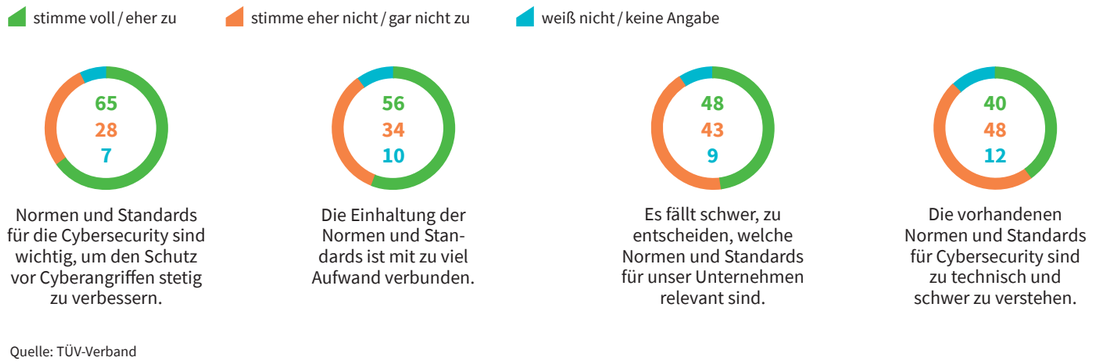
Haben Sie eine oder mehrere der folgenden Maßnahmen für die Verbesserung der IT-Sicherheit ergriffen?

Sicherheitsprüfung aus Angreiferperspektive (Penetrationstest)	32
Einführung IT-sicherheitsrelevanter Zertifizierungen	26
Durchführung von Notfallübungen	24
Beratung durch externe Fachexpertinnen und -experten	72
Schulungen für die Mitarbeitenden außerhalb der IT	50
verstärkter Informationsaustausch, z. B. Networking mit Partnern, Verbänden	48
spezielle Fortbildungen für IT-Mitarbeitende	40
strategische Allianzen und Partnernetzwerke, z. B. für Unterstützung im Bedarfsfall	29
Einstellung zusätzlicher IT-Expertinnen und -Experten	18

* Mehrfachnennungen möglich. Quelle: TÜV-Verband

Mehr Standards

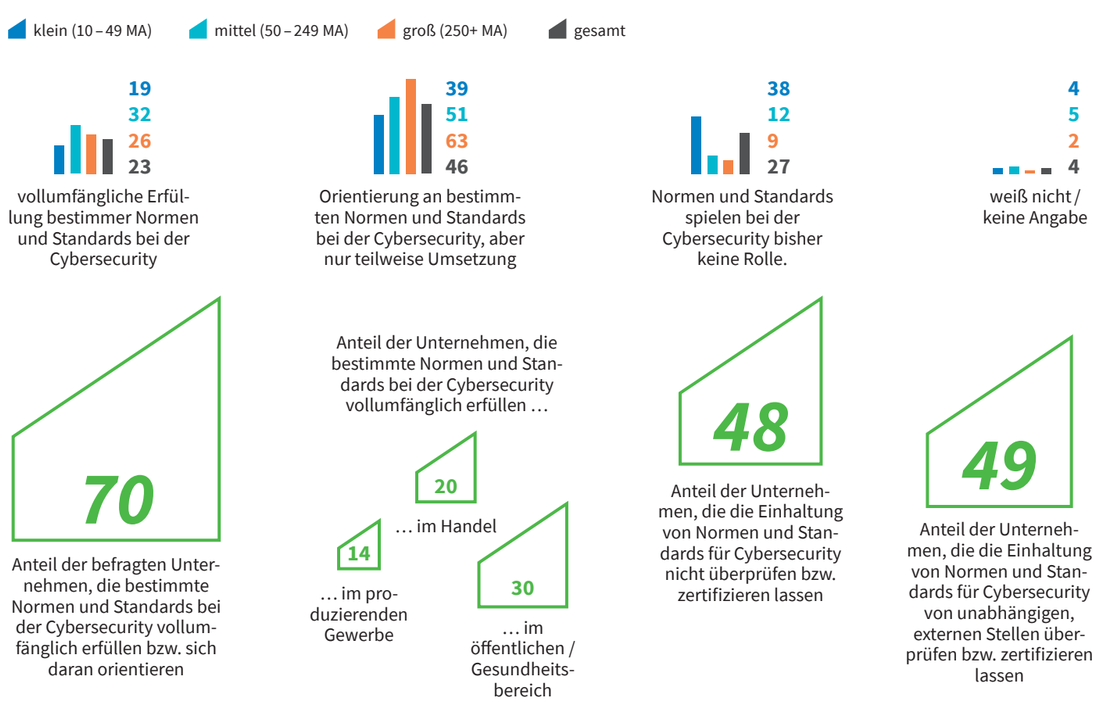
Vor- und Nachteile von Normen und Standards für Cybersicherheit; Unternehmen in Deutschland (n=501); 2023; in Prozent



Quelle: TÜV-Verband

Mehr Schutz

Rolle von Normen und Standards für Cybersicherheit nach Unternehmensgröße; Unternehmen in Deutschland (n=501); 2023; in Prozent



Quelle: TÜV-Verband

Einerseits, andererseits

Einstellung zu gesetzlichen Maßnahmen für IT-Sicherheit; Unternehmen in Deutschland (n=501); 2023; Zustimmung zu den Aussagen in Prozent *

IT-Sicherheitsvorfälle helfen dabei, das Thema Cybersicherheit bei der Unternehmensleitung zu priorisieren.	84
Gesetzliche Vorgaben erhöhen den bürokratischen Aufwand im Bereich Cybersecurity.	84
Jedes Unternehmen sollte gesetzlich verpflichtet sein, angemessene Maßnahmen für seine Cybersecurity zu ergreifen.	64
Strengere gesetzliche Vorgaben für die Cybersecurity von Unternehmen machen das ganze Internet sicherer.	56
Strengere gesetzliche Vorgaben helfen uns dabei, zusätzliche Maßnahmen für Cybersecurity im Unternehmen umzusetzen.	49

* Mehrfachnennungen möglich. Quelle: TÜV-Verband

Zum einen, zum anderen

Priorisierung bei der Zuteilung des Cybersicherheits-Budgets; Führungskräfte aus den Bereichen Business, Technologie und Sicherheit (n=104); Deutschland; 2023; in Prozent *

Welche der folgenden Investitionen priorisieren Sie bei der Zuteilung des Cybersicherheits-Budgets Ihrer Organisation in den nächsten 12 Monaten (Top 3)?

- 62 – Modernisierung von Technologie inkl. Infrastruktur
- 52 – Optimierung momentaner Technologie und Investitionen
- 47 – laufende Verbesserung der Risiko-Haltung basierend auf Cyber-Roadmap
- 35 – Abhilfe nach jüngsten Cybersicherheitsverstößen oder Eingriffen in die Organisation oder Industrie
- 29 – Einhaltung von Regeln und Anordnungen
- 29 – laufendes Sicherheitstraining
- 17 – neue Geschäftsinitiativen
- 15 – Verschiebung von Geschäftsprioritäten
- 1 – unsicher

* Mehrfachnennungen möglich. Quelle: PwC

Sowohl als auch

Einstellung der Mitarbeitenden zu Cybersecurity-Maßnahmen; Unternehmen in Deutschland (n=501); 2023; Zustimmung zu den Aussagen in Prozent *

- 79 – Die Mitarbeitenden haben die Bedeutung von Cybersecurity erkannt.
- 73 – Die Mitarbeitenden wirken aktiv an der Einhaltung der Vorgaben für die Cybersicherheit des Unternehmens mit.
- 51 – Die Mitarbeitenden sind häufig genervt, weil sie bestimmte IT-Sicherheitsanforderungen erfüllen müssen (z. B. bei Authentifizierung, Passwortwechsel).
- 11 – Es kommt häufig vor, dass Mitarbeitende bewusst die IT-Sicherheitsvorgaben umgehe.

* Mehrfachnennungen möglich. Quelle: TÜV-Verband

Wir können

Erhebung und Berichterstattung von Cybersecurity-Risiken; Sicherheits- und IT-Beauftragte (n=110); Deutschland; 2023; in Prozent *

Welche Methoden verwendet Ihre Organisation, um ihre Cybersicherheitsfähigkeiten zu bewerten und darüber zu berichten?

- 47 – ISO 27001
- 46 – Kontrollmatrix der Cloud Security Alliance
- 34 – Überprüfung der Cyber-Resilienz
- 38 – NIST Cybersicherheits-Framework
- 33 – CIS-Kontrollen
- 32 – Cybersicherheitsprofil des Koordinierungsrats des Finanzdienstleistungssektors (FSSCC)
- 31 – SANS kritische Kontrollen
- 31 – ISA/EAC 62443
- 29 – ISF-Standard guter Praxis

* Mehrfachnennungen möglich. Quelle: PwC

27001: eine internationale Norm, die Anforderungen für ein Informationssicherheits-Managementsystem (ISMS) festlegt. Sie hilft Organisationen, ihre Informationen sicher zu verwalten.
NIST Cybersicherheits-Framework: ein Rahmenwerk, entwickelt vom US National Institute of Standards and Technology, das Standards und Richtlinien zur Verbesserung der Cybersicherheit für kritische Infrastrukturen bietet.
Kontrollmatrix der Cloud Security Alliance: ein Rahmenwerk, das spezifische Sicherheitskontrollen und Richtlinien für Cloud-Anbieter und Nutzer zur Sicherstellung der Sicherheit in der Cloud bietet.
Überprüfung der Cyber-Resilienz: eine Bewertungsmethode, die entwickelt wurde, um die Fähigkeit von Organisationen zu messen, sich von Cyberangriffen zu erholen und ihre kritischen Dienste aufrechtzuerhalten.
FSSCC: ein spezifisches Sicherheitsprofil, das von dem Koordinierungsrat des Finanzdienstleistungssektors entwickelt wurde, um branchenspezifische Risiken und Bedrohungen zu adressieren.
CIS-Kontrollen: eine Reihe von Aktionen zur Cyberverteidigung, die von der Center for Internet Security entwickelt wurden, um Organisationen zu helfen, die wichtigsten Angriffsvektoren gegen Cyberattacken zu schützen.
ISF-Standard guter Praxis: ein Standard, der vom Information Security Forum entwickelt wurde und umfassende Sicherheitsrichtlinien und -praktiken für Unternehmen anbietet.
SANS kritische Kontrollen: eine Liste von Prioritäten und effektiven Sicherheitskontrollen, die von SANS Institute bereitgestellt wird, um Cyberangriffen vorzubeugen und zu begegnen.
ISA/EAC 62443: ein internationaler Standard für die Sicherheit industrieller Automatisierungs- und Steuerungssysteme, der Leitlinien für die sichere Integration und Wartung von industriellen Netzwerksystemen bietet.

Wir planen

Ansatzpunkte für Investitionen in Cybersicherheit; Unternehmen in Deutschland (n=501); 2023; in Prozent *

Werden die Investitionen bzw. Maßnahmen erhöht, verringert oder bleiben sie gleich in den vier Phasen der Abwehr und im Umgang mit Cyberangriffen?

Erhöhung von Investitionen / Maßnahmen | gleichgebliebene Investitionen / Maßnahmen | Verringerung von Investitionen / Maßnahmen

	Erhöhung	gleichgeblieben	Verringerung
Schutz (Protect)	45	51	0
Erkennung (Detect)	38	56	<1
Reaktion (Response)	28	66	<1
Wiederherstellung (Recover)	37	57	<1

* Fehlende Angaben zu 100 Prozent weiß nicht / keine Angabe. Quelle: TÜV-Verband

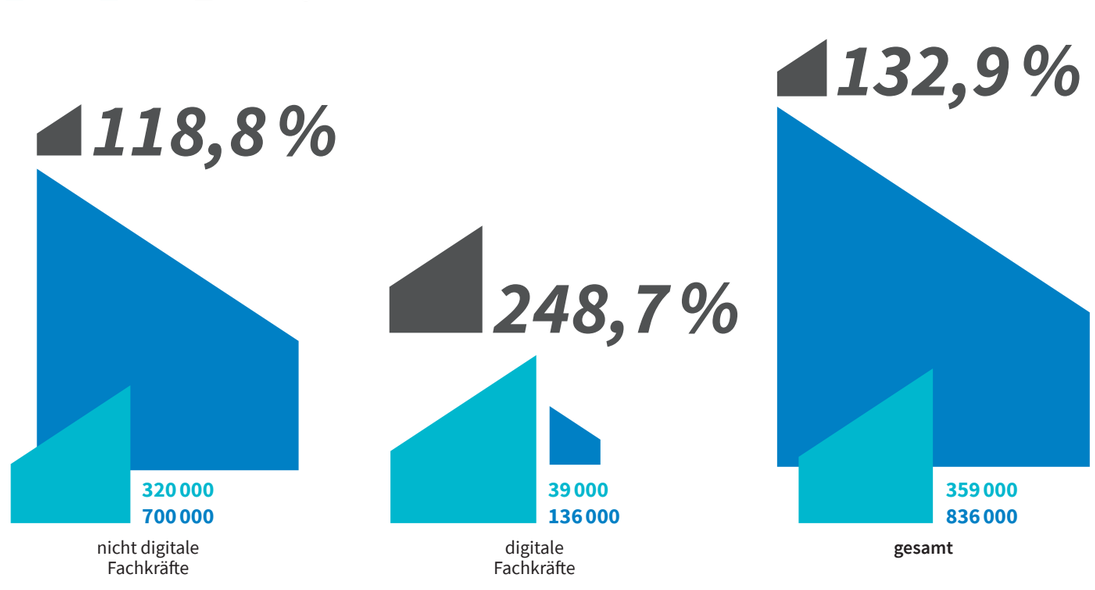
Was geschieht

Wichtigkeit von Cybersicherheit in kleinen und mittleren Unternehmen; Entscheider und IT-Verantwortliche von kleinen und mittleren Unternehmen (n=300); Deutschland; 2023; in Prozent

Quelle: GDV

Was kommt

Prognose zur Entwicklung der Fachkräfte-Lücke bis 2030 im öffentlichen Sektor *; Deutschland



* Das McKinsey-Modell zur Berechnung der Fachkräfte-Lücke geht zunächst aus von der Zahl der aktuell (Ende 2022) offenen Stellen sowie der Zahl der Personen in den voraussichtlich in Rente / Pension gehenden Jahrgängen und den nachrückenden Jahrgängen bis 2030. Anschließend ist die Lücke an digitalen Fachkräften approximiert worden anhand des Anteils der Informatik- und IKT-Berufe am Gesamtbedarf 2022 (11 %) und 2030 (16 %). Quelle: McKinsey

Was hilft

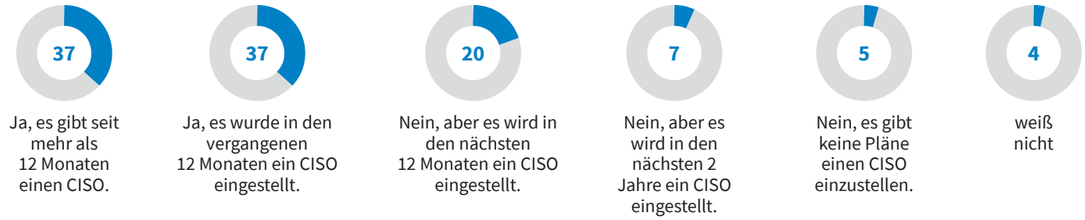
Maßnahmen mit dem größten Potenzial zur kurzfristigen Behebung des IT-Fachkräftemangels; IT- / Personal-Entscheiderinnen und -Entscheider (n=1 001); Deutschland; 2023; in Prozent *

* Mehrfachnennungen möglich. Quelle: Civey, neue fische

Was wird

CISO in Unternehmen; IT-Entscheiderinnen und -Entscheider (n=204); Deutschland, Österreich, Schweiz; 2022; in Prozent *

Gibt es in Ihrer Organisation einen Chief Information Security Officer (CISO)?

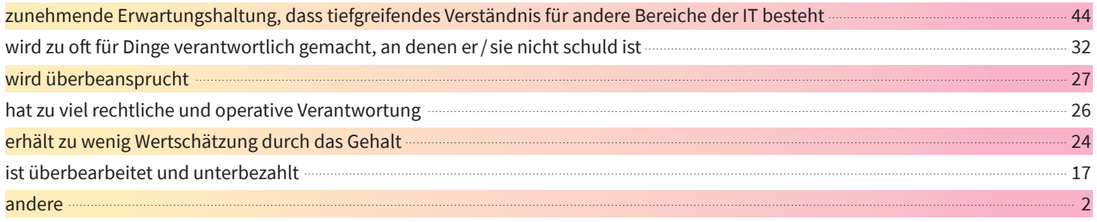


* Mehrfachnennungen möglich. Quelle: Fastly, Sapio Research

Was ist

Außenwahrnehmung der Rolle des CISO; IT-Entscheiderinnen und -Entscheider (n=204); Deutschland, Österreich, Schweiz; 2022; in Prozent *

Wie wird die Rolle des CISO Ihrer Meinung nach gesehen?



* Mehrfachnennungen möglich. Quelle: Fastly, Sapio Research

Tabea Rößner
begann ihre politische Karriere in der Mainzer Lokalpolitik und sitzt seit 2009 für Bündnis 90/Die Grünen im Bundestag. Dort leitet die frühere Rundfunk- und Fernsehjournalistin aus Rheinland-Pfalz seit 2021 den Ausschuss für Digitales. Geboren als viertes von sechs Kindern einer Pfarrersfamilie, engagiert sich die heute 57-Jährige seit ihrer Jugend für Menschenrechte, gegen Fluglärm und soziale Benachteiligung. So sammelte sie in der Corona-Zeit gebrauchte Laptops, damit Homeschooling auch für Kinder aus benachteiligten Familien möglich wurde. Zur Bundestagswahl 2025 kandidiert sie nicht erneut.

„Es ist viel kriminelle Energie unterwegs.“

Die Kulturwissenschaftlerin und ehemalige Journalistin Tabea Rößner leitet den Ausschuss für Digitales im Deutschen Bundestag. Ob es um den Datenschutz, die Grenzen von KI oder Hackerangriffe auf kritische Infrastrukturen geht: Die Grünen-Politikerin versteht sich als Kämpferin für Meinungsfreiheit, Demokratie und Bürgerrechte.

Interview: Stefan Scheytt

Frau Rößner, was wissen Sie, was wir nicht wissen? Als Vorsitzende des Ausschusses für Digitales des Deutschen Bundestags sind Sie doch sicher Geheimnisträgerin, oder?

Tabea Rößner: Teilweise. Auf Antrag können wir in bestimmte geheime Vorgänge Einblick nehmen und tun das auch hin und wieder. Es gibt auch als geheim eingestufte, nicht öffentliche Ausschusssitzungen, in denen vertrauliche Themen besprochen werden. Aber ich bin keine Geheimnisträgerin in dem Sinn, dass es zum Beispiel regelmäßige Briefings durch die Geheimdienste gäbe. Wir sind die Legislative, und Ermittlungen sind Sache der Exekutive, also etwa des Bundeskriminalamtes (BKA) oder der Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT).

Was ist Ihre Aufgabe als Ausschussvorsitzende, und welchen Einfluss auf die Digitalpolitik haben Sie?

Als Ausschussvorsitzende koordiniere ich die Sitzungen, leite die Diskussionen und sorge zusammen mit den Obleuten der Fraktionen dafür, dass alle relevanten Themen besprochen werden – und das so oft öffentlich wie möglich. Gemeinsam haben wir direkten Einfluss auf die Gestaltung der Digitalpolitik, indem wir Gesetzesvorschläge erarbeiten, bewerten und Empfehlungen aussprechen.

Geben Sie bitte ein Beispiel.

Etwa das im März im Bundestag beschlossene Digitale-Dienste-Gesetz – es setzt den Digital Services Act der EU auf nationaler Ebene um und regelt unter anderem die Digitalaufsicht über die Online-Plattformen. Hier haben wir als Koalitionsfraktionen noch Verbesserungen am Gesetzentwurf vorgenommen. Zum Beispiel dadurch, dass die Bundesnetzagentur als Regulierer bei der Besetzung bestimmter Leitungsstellen unabhängiger von Ministerien und vom Bundestag agieren kann; auch der zugehörige Beirat wurde eigenständiger gestellt etwa durch Informationsansprüche und Aufwandsentschädigungen für die Mitglieder.

Außerdem haben wir dafür gesorgt, dass der Zugang für Nutzerinnen und Nutzer leichter ausgestaltet werden muss und dass das BKA für mehr Transparenz jährlich einen Tätigkeitsbericht vorlegt. So spiegelt sich die parlamentarische Arbeit des Digitalausschusses in konkreten Gesetzen und Stellungnahmen wider.

Andere Ausschüsse haben andere Interessen. Wie gehen Sie damit um?

In der Tat. Obwohl dem Ausschuss Mitglieder aller Parteien angehören, stehen wir als Digital-Politiker manchmal auch ›

zusammen gegen andere Fachpolitiker. Etwa bei der elektronischen Patientenakte, zu der die Gesundheitspolitiker mehrheitlich eine andere Linie vertreten haben als wir.

Oder beim Thema Chat-Kontrolle: Traditionell haben die Mitglieder des Innenausschusses da eher die Sicherheit im Blick und sind offener für die Forderung nach mehr Befugnissen für die Ermittlungsbehörden, während wir Digital-Politiker die Bürger- und Freiheitsrechte stärker im Fokus haben. Solche Konflikte müssen dann fraktionsintern in Arbeitsgruppen sowie in den Koalitionsfraktionen und Ausschüssen ausverhandelt werden.

Welche Rolle spielt die Cybersicherheit im Ausschuss?

Eine wichtige, aber nicht die alleinige Rolle, weil Digitalisierung ein Querschnittsthema ist. Der Digitalausschuss ist formal dem Digital- und Verkehrsministerium zugeordnet. Cybersicherheit liegt allerdings hauptsächlich in der Zuständigkeit des Innenministeriums, weshalb vieles dazu über den Innenausschuss läuft, manches auch über den Wirtschaftsausschuss, etwa wenn vor allem Unternehmen betroffen sind. Aber auch wir als Digitalausschuss beschäftigen uns damit, beispielsweise in Anhörungen mit Sachverständigen zur Cybersicherheit.

Dabei ging es zum Beispiel darum, wie die Zuständigkeit der Behörden straffer organisiert, die Strafverfolgung verbessert oder Sicherheitslücken geschlossen werden können. Gerade nach konkreten Vorfällen lassen wir uns – neben dem federführenden Ausschuss – von Experten berichten.

Was sind das für konkrete Vorfälle?

Das jüngste Beispiel ist sicherlich die Diskussion über große Sicherheitslücken beim Videokonferenzsystem WebEx, das etliche Bundesministerien und -behörden, aber auch Unternehmen einsetzen. Man erinnert sich an die sogenannten Taurus-Leaks, als ein vertrauliches Gespräch deutscher Offiziere via WebEx über Voraussetzungen für einen Einsatz des Waffensystems „Taurus“ in der Ukraine abgehört und veröffentlicht wurde. Es stand die Frage im Raum, ob es sich um ein Fehlverhalten einzelner Generäle handelte oder ob es sich auch um Sicherheitslücken beim Anbieter handeln könnte. Letzteres wäre gravierend – mit Blick auf die Integrität unserer Kommunikation. Die Verantwortlichen sind dieser Frage viel zu lange ausgewichen. Erst nachdem wir Parlamentarier mehrfach öffentlich dazu aufforderten, ist man den Dingen auf den Grund gegangen. Hierzu wurden die Verantwortlichen zuletzt im Ausschuss befragt.

Das zeigt: Wir leisten als Parlament unseren Beitrag zur Sachaufklärung und können dann auch entsprechende politische Schlüsse ziehen. In dem Fall hat die Bundesregierung im Ausschuss versichert, zu große Abhängigkeiten von einzelnen Unternehmen – nicht nur solchen aus autoritären Staaten – zu reduzieren und an Eigenentwicklungen zu arbeiten. Auch den Hersteller hatten wir in die Sitzung eingeladen, dessen Vertreter sich dann den kritischen Fragen der Abgeordneten stellen musste. Bei ähnlichen Vorfällen wie dem Angriff auf den Deutschen Bundestag haben wir ebenfalls entsprechend gehandelt und so unseren Teil als Parlament geleistet, Aufklärung voranzutreiben und Nachjustierungen durchzusetzen.

Mini-Parlament fürs Digitale

Der Digitalausschuss, der 2014 seine Arbeit aufnahm, ist einer von 25 ständigen Ausschüssen im Deutschen Bundestag. Als „vorbereitende Beschlussorgane“ haben diese Gremien in ihrem jeweiligen Fachgebiet große Bedeutung für die Arbeit des Bundestags. Denn wie ein Mini-Parlament beratschlagen sie über Gesetzentwürfe, können aber auch selbst die Initiative ergreifen und Themen aus ihrem Geschäftsbereich bearbeiten, sich von Ministerien informieren lassen, öffentliche Anhörungen mit Experten einberufen und Unterausschüsse bilden.

Der Digitalausschuss hat derzeit 33 Mitglieder, sie kommen aus allen Fraktionen und spiegeln die Sitzverteilung im Bundestag wider. Neben der Ausschussvorsitzenden sind die Obleute der Fraktionen einflussreiche Akteure im parlamentarischen Aushandlungsprozess. In seiner Selbstbeschreibung benennt der Ausschuss als sein Aufgabengebiet „aktuelle netzpolitische Themen einschließlich des Ausbaus der digitalen Infrastruktur“. Wie breit das Spektrum ist, zeigt ein Blick in die Tagesordnungen des Ausschusses, der sich seit seiner Konstituierung nach der Bundestagswahl im Herbst 2021 69-mal getroffen hat (Stand Juli 2024): Der Ausschuss befragt Vertreter der Plattform X zu willkürlichen Sperrungen und zur Einhaltung der Regeln des europäischen „Digital Services Act“. Er spricht mit Google-Vertretern über die Sicherheit von Cloud-Infrastrukturen. Die Mitglieder diskutieren Empfehlungen der Bundesnetzagentur zum „Recht auf schnelles Internet“ sowie über die Frage, wer die nationale Aufsicht über künstliche Intelligenz führen soll, wie sie durch den „AI Act“ der EU vorgesehen ist. Die Abgeordneten befragen den für Digitales zuständigen Bundesminister Volker Wissing (FDP) zur Verlängerung von Mobilfunkfrequenzen und zur befristeten Ausnahmeregelung für Verkehrsunternehmen, die das Deutschlandticket noch immer nicht als Digitalticket anbieten. Der Ausschuss hört Expertinnen und Experten zum Thema Cybersicherheit an und veranstaltete eine eigene Sitzung nur dazu, warum der vor vielen Jahren eingeführte Personalausweis mit elektronischem Identitätsnachweis von den Bürgerinnen und Bürgern so wenig angenommen wird.

Der Ausschuss galt nach seiner Gründung lange Zeit als Feigenblatt deutscher Innovationspolitik. Denn wirklich wichtige Entscheidungen wurden in anderen Ausschüssen vorbereitet, dem Innen- oder Rechtsausschuss etwa. Erst seit es das Bundesministerium für Digitales und Verkehr gibt, derzeit geführt von Volker Wissing, steht das Digitale nicht nur vorn im Namen: Der Digitalausschuss berät seitdem auch federführend und erarbeitet Beschlussempfehlungen fürs Plenum.

Und trotzdem passieren ständig neue Angriffe.

Ja, und das Problem betrifft bei Weitem nicht nur die Politik. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) nennt in seinem Lagebericht eine Schadenshöhe durch IT-Angriffe laut Bitkom-Studie in Höhe von 148 Milliarden Euro. Unsere Reaktion auf all diese Vorkommnisse muss entschlossener sein. Wir brauchen nicht weniger als eine Kehrtwende im Bereich der IT-Sicherheitspolitik, die bisher weitgehend gescheitert ist. Es braucht neue Rechtsgrundlagen, zum Beispiel für den Schutz unserer kritischen Infrastrukturen.

Bei all diesen komplexen Fragen sind Fachwissen und technisches Verständnis sehr wichtig. Sie haben Musikwissenschaft, Kunstgeschichte, Theater-, Film- und Fernsehwissenschaft studiert. Was qualifiziert Sie für Digitalpolitik?

Ich habe eine hohe Affinität zu dem Thema. Vor meiner Wahl in den Bundestag 2009 habe ich fast zwanzig Jahre als Journalistin fürs Fernsehen und fürs Radio gearbeitet, schon dadurch habe ich viel Technikwissen, ich war immer digital unterwegs. Aber selbst wenn ich Informatik studiert hätte, wäre ich heute nicht mehr auf dem neuesten Stand des Wissens. Es geht vielmehr darum, sich über neue Entwicklungen auf dem Laufenden zu halten. Das betrifft aber nicht nur technische Entwicklungen, sondern auch gesellschaftliche und politische. Das tun wir Politiker die ganze Zeit. Man braucht also kein Fachstudium, um Digitalpolitik machen zu können.

Viele Menschen sehen das anders.

Ich weiß. Aber zum einen zeichnet gute Politikerinnen und Politiker aus, dass sie sich schnell in Themen einarbeiten können, Zusammenhänge verstehen und die richtigen Fragen stellen – das fällt mir als frühere Journalistin leicht. Zum anderen soll der Bundestag ja das Volk abbilden und keine Versammlung von Freaks oder Nerds sein. Natürlich müssen wir fachlich fundiert entscheiden, aber gleichzeitig auch das große Ganze im Blick haben, Interessen gegeneinander abwägen und Entscheidungen dann verständlich kommunizieren.

Außerdem habe ich einen Mitarbeiterstab, der viele fachliche Qualifikationen mitbringt. Und ich lese viel Fachliteratur und Newsletter aus dem Digitalbereich, treffe Wissenschaftlerinnen, Berater, Vertreterinnen und Vertreter von Unternehmen, Thinktanks und NGOs und natürlich auch Mitarbeiterinnen und Mitarbeiter von Behörden wie dem Bundesamt für Sicherheit in der Informationstechnik oder die Datenschutzbeauftragten.

Und wenn das alles nicht hilft?

Wir Politikerinnen und Politiker können nicht alles bis ins Detail wissen, das gilt natürlich auch für das Digitale, bei dem es ja nicht nur um technische Fragen geht, sondern zum Beispiel auch um verfassungsrechtliche oder verwaltungsspezifische. Wie gesagt: Unsere Aufgabe ist es, das große Ganze im Blick zu haben und unterschiedliche Interessen zusammenzuführen. Wenn es aber doch mal ein Detail gibt, für das ich Erklärungsbedarf habe, kenne ich nach so langer Zeit inzwischen viele Menschen mit höchster Expertise, die ich anrufen kann.

Welche Lobbys wollen Einfluss auf Ihre Entscheidungen nehmen?

Alle, die man sich denken kann, und das gehört zum politischen Prozess. Lobbyismus an sich ist erst mal nichts Negatives. Wir sprechen mit Wirtschaftsverbänden und – weil manche oft eigene Termine wollen – auch mit Vertretern von Unternehmen. Wichtig ist für mich, dass wir uns alle anhören, auch die Verbände der Zivilgesellschaft, die eher das Gemeinwohl im Sinn haben. Das sind Organisationen wie der Verbraucherzentrale Bundesverband, die Gesellschaft für Freiheitsrechte, AlgorithmWatch und das Bündnis F5, Digitalcourage und natürlich der Chaos Computer Club, der gerade im Bereich Cybersicherheit eine der ersten Adressen ist.

Welches Problem in der Digitalpolitik wollen Sie in dieser Legislaturperiode unbedingt noch lösen?

Ein zentrales Anliegen sind Projekte mit großer Hebelwirkung, dazu gehört der beschleunigte Ausbau des Breitbandnetzes. Ebenso brauchen wir auch den konsequenten Roll-out von Zukunftstechnologien wie Glasfaser und den neuesten Mobilfunkstandard, denn nur eine flächendeckende Infrastruktur ermöglicht gesellschaftliche Teilhabe. Darüber hinaus arbeiten wir mit Nachdruck an einer einheitlichen Umsetzung der Digital-Aufsicht in Deutschland. Wir machen uns auch für ein Gesetz stark, das ein Recht auf die Ende-zu-Ende-Verschlüsselung festschreibt, aber die Sicherheits- und Geheimdienste sind da anderer Meinung. Das ist ein typischer Zielkonflikt, vor dem wir Politikerinnen und Politiker stehen.

Wie hat sich Ihr eigenes Verhalten im Cyberraum verändert?

Ziemlich stark: Ich nutze verschlüsselte Kommunikationsmittel, sichere meine Geräte regelmäßig und bin sehr vorsichtig mit der Weitergabe sensibler Informationen. Vor vielen Jahren, als ich noch Journalistin beim ZDF war, bekam ich von einer Kollegin eine E-Mail mit Anhang, die ich samt Schadsoftware an andere Kollegen weiterleitete. Das hat mir damals so einen Schock versetzt, dass ich noch vorsichtiger wurde und seither Antivirusprogramme und bestimmte Firewalls nutze.

Was können wir alle tun?

Insgesamt brauchen wir eine viel höhere Sensibilität für diese Themen. Das fängt bei jedem Einzelnen an. Die Menschen sind immer mehr im Netz unterwegs, privat und am Arbeitsplatz, und das führt fast zwangsläufig dazu, dass jeder Einzelne, aber auch Unternehmen, Behörden oder Krankenhäuser angreifbarer sind als früher. Und gleichzeitig ist viel kriminelle Energie unterwegs, die Angriffe und Tricks zum Verwischen der Spuren werden immer ausgefeilter. Es ist ein Wettrennen im Gang zwischen den Kriminellen und denjenigen, die versuchen, ihre Angriffe abzuwehren. Das Bewusstsein dafür muss bei allen noch viel stärker werden.

WIR

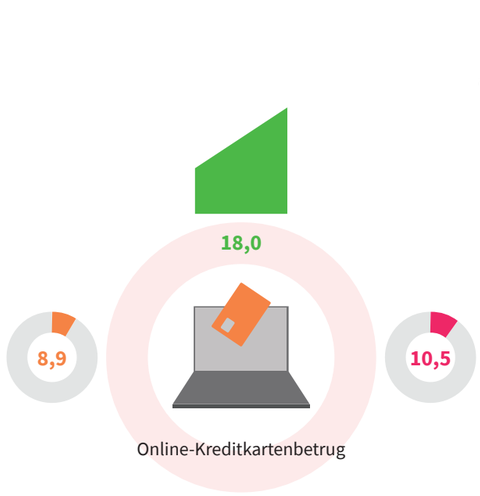
Unser Leben ist digital. Wir arbeiten, spielen, lernen, kaufen, bezahlen, kommunizieren, wählen, feiern, lesen, entspannen, heiraten und trauern in der digitalen Welt. Warum sorgen wir dort nicht auch für Unversehrtheit? Weshalb kümmern wir uns nicht um unseren Schutz? Wieso machen wir es Kriminellen immer wieder leicht?

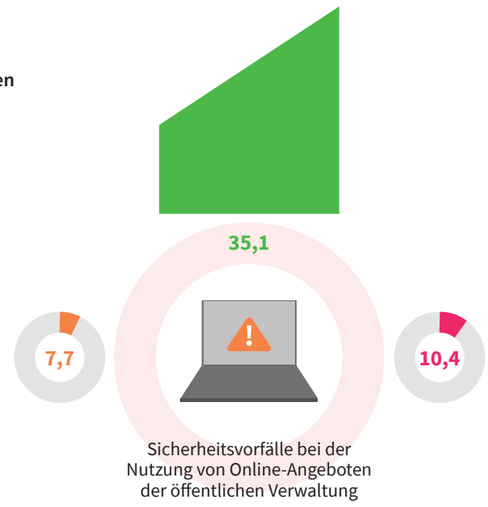
Was uns passiert

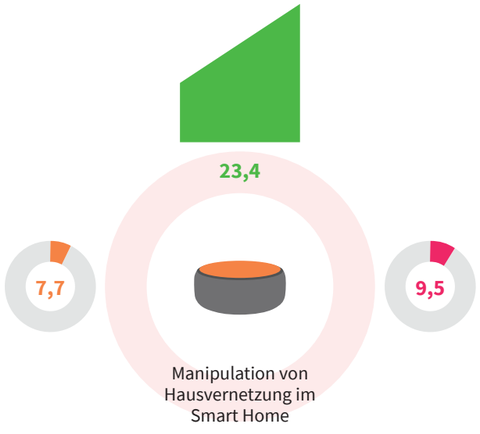
Die seltensten und häufigsten IT-Sicherheitsvorfälle; Verbraucherinnen und Verbraucher über 16 Jahre (n=2 000+); Deutschland; in Prozent

2022 2023 Veränderung 2022 – 2023

am seltensten

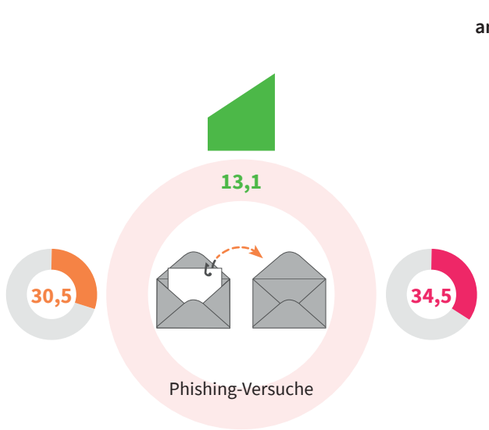


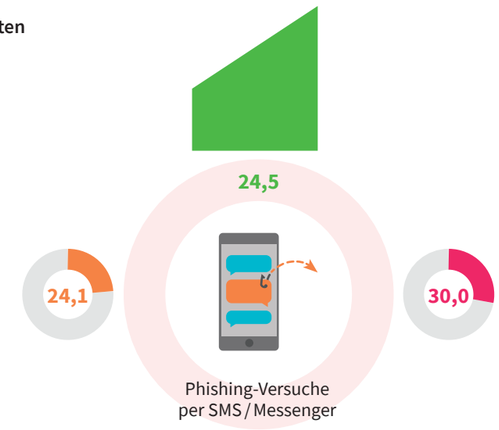


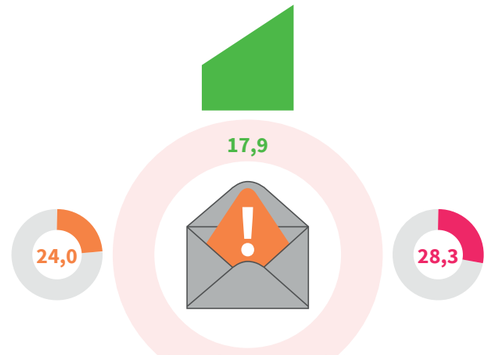


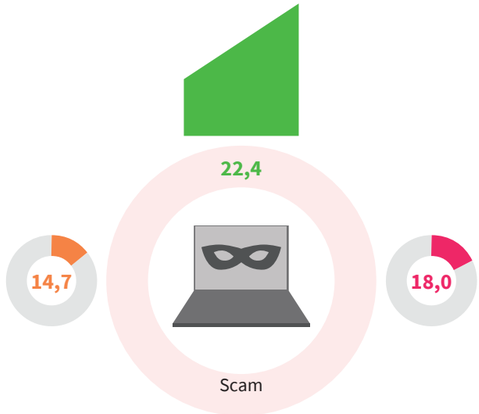
Quelle: DsiN

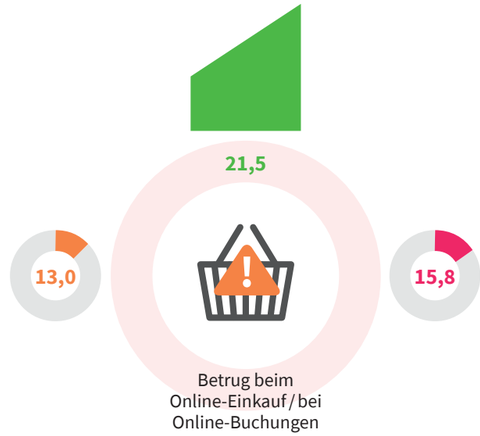
am häufigsten







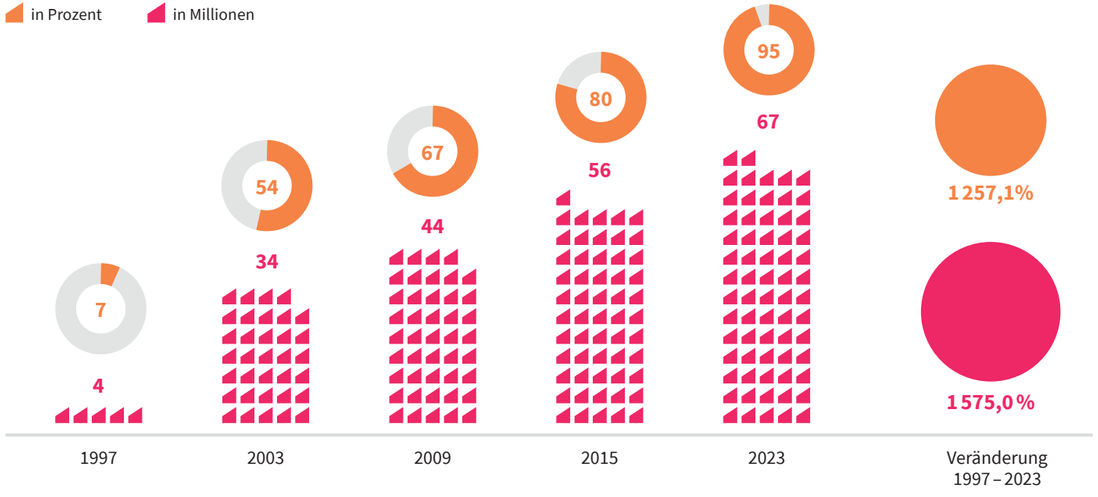




Glossar der Cyberbegriffe auf Seite 100 – 103

Was uns treibt

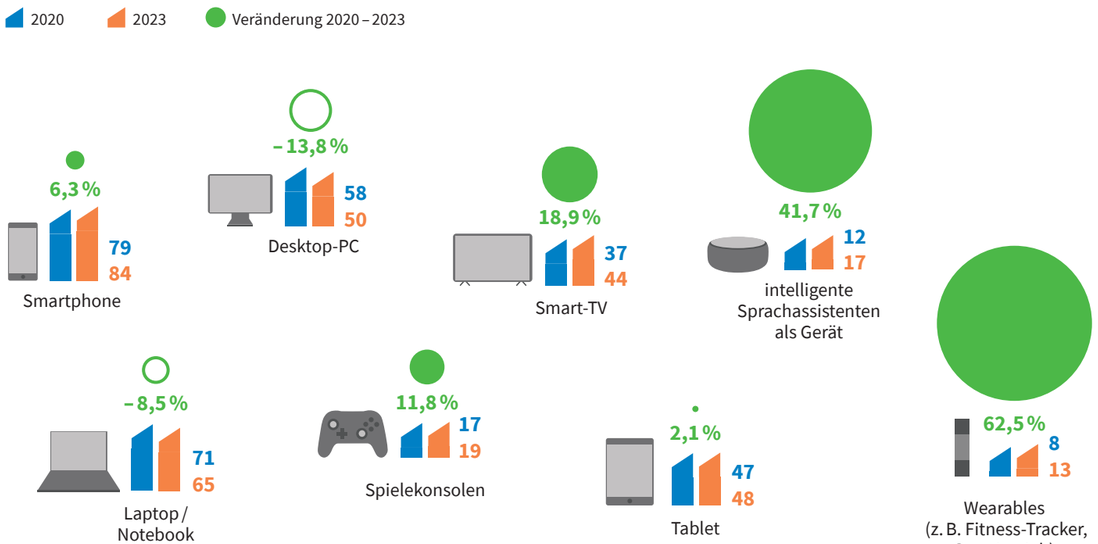
Entwicklung der Online-Nutzung; deutschspr. Bevölkerung ab 14 Jahren; Deutschland; in Prozent / in Millionen



Quelle: ARD / ZDF

Was wir nutzen

Verwendung von Geräten zur Internetnutzung; Bürgerinnen und Bürger (n=3 000+); Deutschland; in Prozent

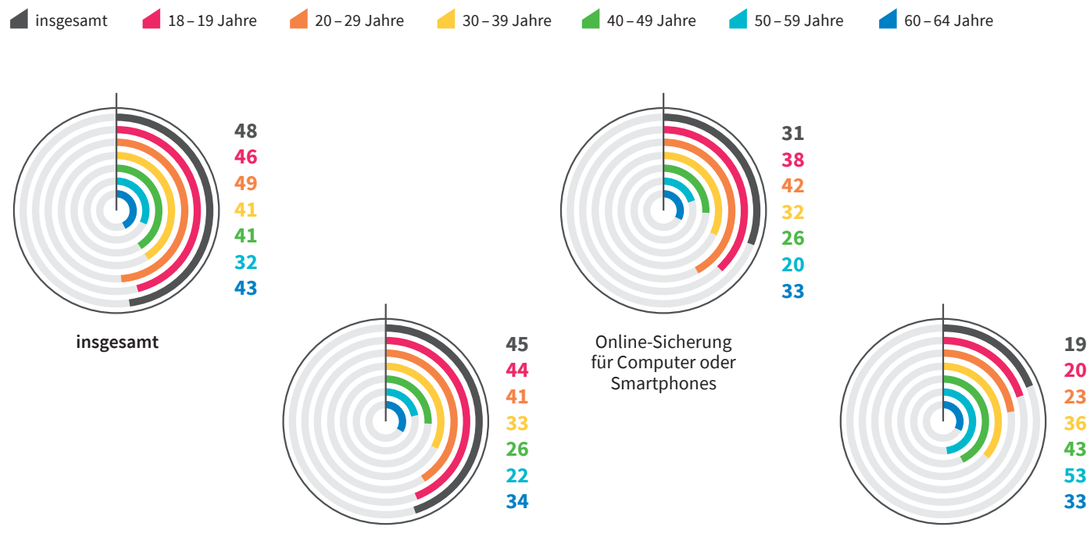


Quelle: Postbank

Wie wir uns unterscheiden

Cloud-Nutzung nach Altersgruppen; Bürgerinnen und Bürger (n=35 938); Deutschland; 2023; in Prozent

Welchen dieser Online-Services haben Sie in den vergangenen 12 Monaten verwendet?



Quelle: Statista Global Consumer Survey

Wie wir kommunizieren

Nutzung von Online-Kommunikationsdiensten; Bürgerinnen und Bürger (n=35 938); Deutschland; 2023; in Prozent

Whatsapp	86
Facebook Messenger	34
FaceTime	20
Telegram	16
Skype	14
Discord	12
Microsoft Teams	11
Zoom	11
iMessage	9
andere	16

Quelle: Statista Global Consumer Survey

Wie wir uns verhalten

Nutzung sozialer Medien; Verbraucherinnen und Verbraucher über 16 Jahre (n=2 000+); Deutschland; 2023; in Prozent

Soziale Netzwerke nutzen	57,9
Genau auf vertrauensvolle Quellen achten	63,7
Mit Freunden und Familie kommunizieren	61,3
Über das Tagesgeschehen informieren sich	36,6
Wenig Gedanken über den Schutz ihres Online-Profils machen sich	27,1
Bereits negative Erfahrungen in sozialen Medien gemacht haben	26,1

* Mehrfachnennungen möglich. Quelle: DsiN

Windows-Versionen

Marktanteile der verschiedenen Windows-Versionen; Deutschland; 2023 ; in Prozent

75,41	19,98	2,62	1,22	0,38	0,24	0,16
Windows 10	Windows 11	Windows 7	Windows 8.1	Windows 8	Windows XP	andere

Support-Ende für …

8. April 2014	10. April 2012	14. Januar 2020	12. Januar 2016	10. Januar 2023
Windows XP	Windows Vista *	Windows 7	Windows 8	Windows 8.1

4,6 %

Anteil der Windows-Rechner, für die es demzufolge keinen Support und somit auch keine Sicherheits-Updates mehr gibt

* Gelistet unter „andere“. Quelle: Statcounter

macOS-Versionen

Marktanteile verschiedener macOS-Versionen; Deutschland; 2023; in Prozent

macOS Catalina	84,99
macOS Mojave	10,02
macOS High Sierra	1,93
macOS Sierra	0,73
OS X El Capitan	0,58
OS X Mavericks	0,85
andere	0,90

Quelle: Statcounter

IOS-Versionen

Marktanteile verschiedener iOS-Versionen; Deutschland; 2024; in Prozent

iOS 17.2	34,76
iOS 17.1	29,00
iOS 16.6	7,81
iOS 16.7	4,15
iOS 16.1	3,42
iOS 16.3	2,77
iOS 17.3	2,68
andere	15,40

Quelle: Statcounter

Android-Versionen

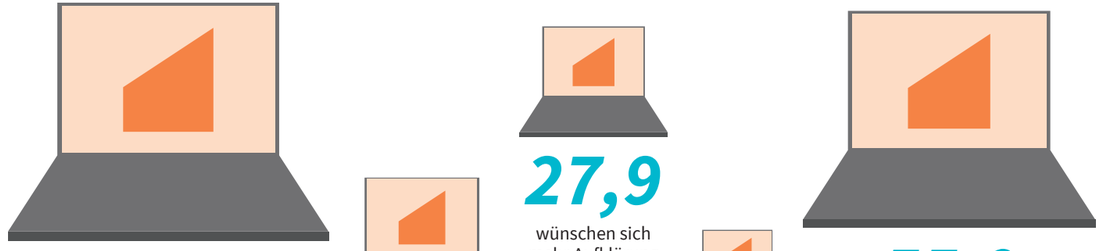
Marktanteile verschiedener Android-Versionen; Deutschland; 2024; in Prozent *

13.0	33,01
14.0	19,60
12.0	14,11
11.0	11,63
10.0	9,00
9.0 Pie	4,66
8.0 Oreo	2,67
6.0 Marshmallow	2,16
7.0 Nougat	1,23

* Aktuelle Android-Versionen erhalten regelmäßige Updates. Die Versionen 10.0 und älter werden nicht mehr unterstützt. Quelle: Statcounter

Künstlich und persönlich

Künstliche Intelligenz aus Verbrauchersicht; Verbraucherinnen und Verbraucher ab 16 Jahren (n=2 000+); Deutschland; in Prozent *



60,3
geben an zu wissen, was man unter KI versteht.

31,2
hätten mehr Vertrauen, wenn die Haftung für getroffene Entscheidung klar wäre.

27,9
wünschen sich mehr Aufklärung über Chancen und Risiken von KI.

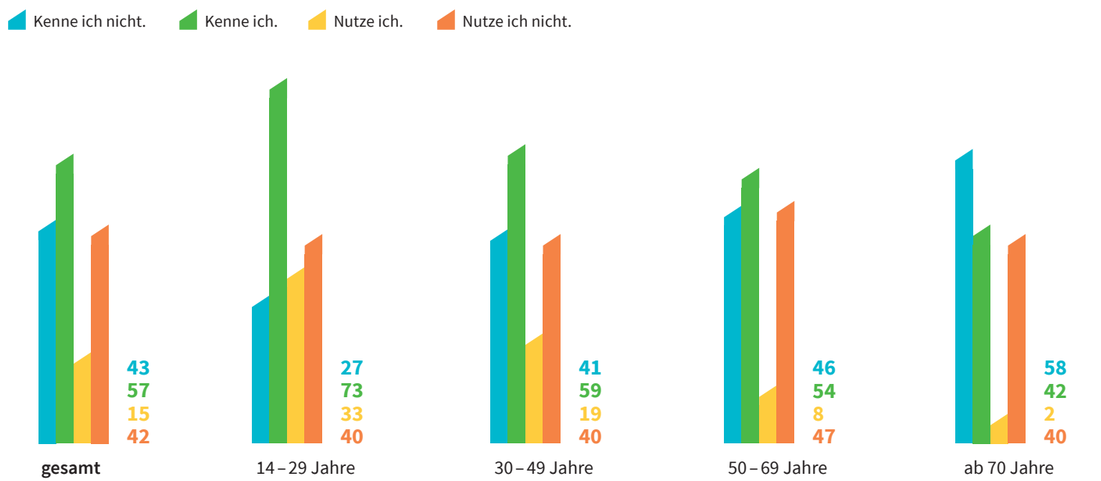
19,1
haben hohes Vertrauen in Anwendungen, die mit KI arbeiten.

55,0
haben die Absicht, KI-gestützte IT-Sicherheitsprogramme zu nutzen oder das bereits getan.

* Mehrfachnennungen möglich. Quelle: DsiN

Künstlich und praktisch

Bekanntheit und Nutzung von KI-Chatbots; deutschspr. Bevölkerung ab 14 Jahren; Deutschland; 2023; in Prozent



Quelle: ARD / ZDF

Täter

Kriminalitätsstatistik zu Cybercrime *; Deutschland

2021	2022	2023		
146 363	176,0	14 780	29 855	29,3 %
136 865	162,4	13 780	28 875	29,2 %
134 407	158,7	12 696	30 860	32,2 %
erfasste Fälle	Fälle pro 100 000 Einwohner	Versuche **	Tatverdächtige insgesamt	Aufklärungsquote

* Cybercrime ist ein sogenannter Summenschlüssel („897 000 Cybercrime“). Folgende Schlüssel sind hier enthalten:
543 000 Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung §§ 269, 270 StGB
674 200 Datenveränderung, Computersabotage §§ 303a, 303b StGB
678 000 Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei gemäß §§ 202a, 202b, 202c, 202d StGB
897 100 Computerbetrug § 263a StGB
Der Summenschlüssel weist Überschneidungen mit dem Summenschlüssel „Computerbetrug“ auf.
** Unter „Versuche“ werden alle erfassten Versuche aus den relevanten Straftaten aufgeführt. Bei manchen Straftaten ist laut dem Strafgesetzbuch (StGB) auch schon der Versuch einer Straftat strafbar.
Quelle: Bundeskriminalamt

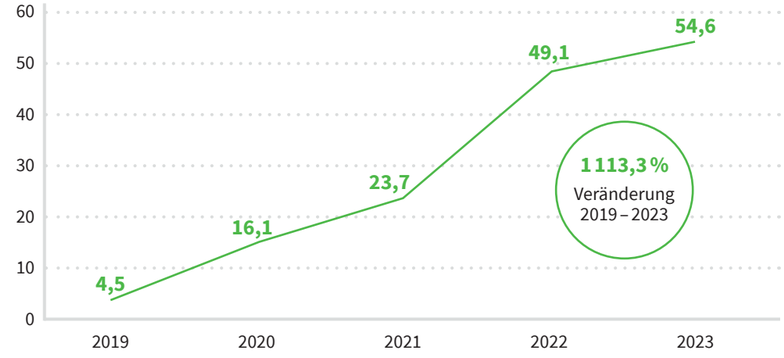
Opfer

Opfer von Internetkriminalität nach Art der Straftaten; Befragte, die innerhalb der vergangenen zwölf Monate Opfer von Cybercrime geworden sind (n=358); Deutschland; 2023; in Prozent

* Mehrfachnennungen möglich. Quelle: BSI / ProPK

Entdeckt

Zahl der entdeckten Cybercrime-Bedrohungen; Deutschland, Österreich, Schweiz; in Millionen



Zahl der 2023 durch G DATA entdeckten Cyberattacken

54 579 192
gesamt

149 532
pro Tag

104
pro Minute

Quelle: G DATA CyberDefense AG

Entsendet

Zahl neuer Schadprogramm-Varianten und -Infektionen; Deutschland; 1. Juni 2022 bis 30. Juni 2023

insgesamt | pro Tag

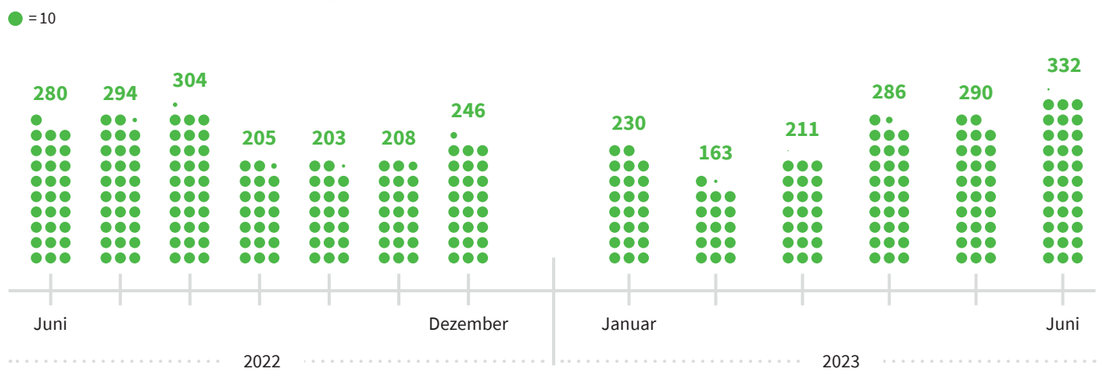
Schadprogramm-Varianten

ca. 91,3 Millionen
ca. 250 000

Schadprogramm-Infektionen

ca. 21 000
ca. 7,7 Millionen

Entwicklung der Zahl neuer Schadprogramm-Varianten; in Tausend



Quelle: BSI

Verbrecherisch

Von Schadprogrammen und Spam betroffene Websites, Mails und Software; Deutschland; 1. Juni 2022 bis 30. Juni 2023

370
Zahl der Websites, die täglich wegen enthaltener Schadprogramme für den Zugriff aus den Regierungsnetzen gesperrt wurden

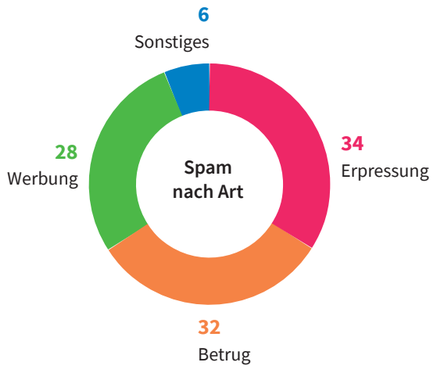
775
Zahl der Mails mit Schadprogrammen, die täglich in deutschen Regierungsnetzen abgefangen wurden

66 %
Anteil aller Spam-Mails, die Cyberangriffe waren

32 %
davon Betrugs-Mails

34 %
davon Erpressungs-Mails

84 %
Finance-Phishing-Anteil am gesamten Mail-Betrug



durchschnittlich pro Monat gefundene Schwachstellen in Softwareprodukten

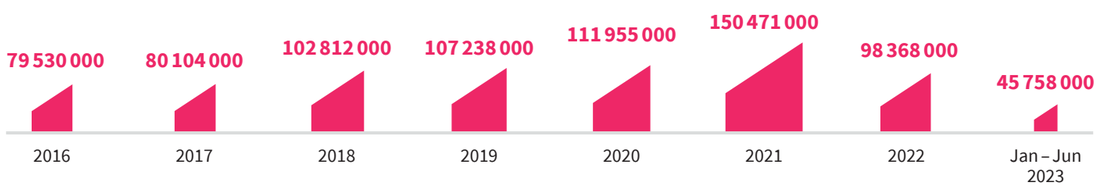
+2 000
gefundene Schwachstellen

+300
davon kritisch

Quelle: BSI

Vergeblich

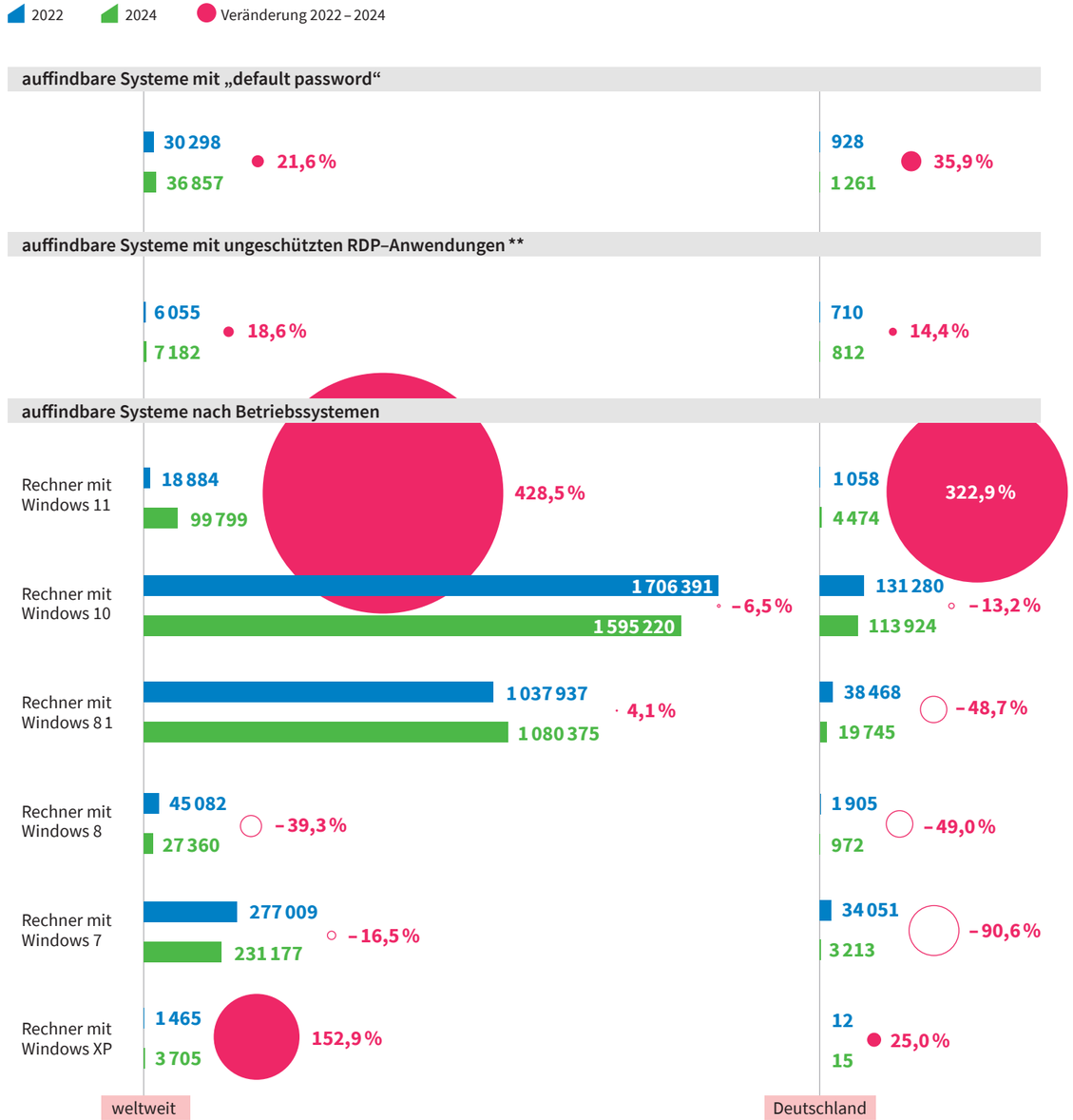
Zahl bekannt gewordener neuer Malware-Varianten; Deutschland



Quelle: BSI

Verletzlich

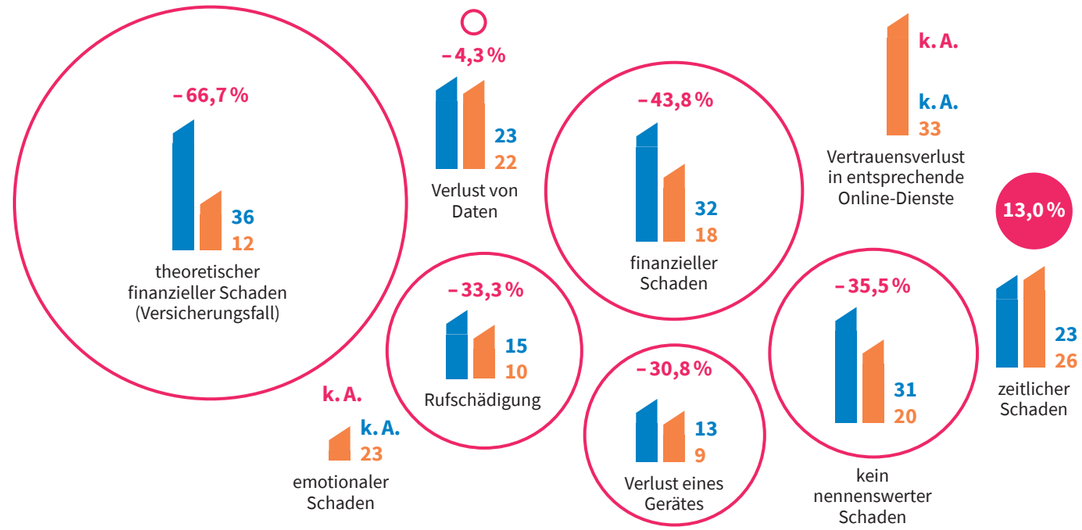
Zahl der über Shodan * via Internet auffindbaren „verletzlichen“ Systeme; Deutschland & weltweit



* Shodan.io ist eine Suchmaschine, die ungeschützte Anwendungen oder Systeme mit nur geringen Sicherheitsvorkehrungen im Internet findet. Geräte / Anwendungen / Systeme, die gefunden werden, bieten leichte Ziele für missbräuchliche Angriffe aus dem Bereich Cybercrime. ** Remote Desktop Protocol (RDP) ist eine Software, mit der sich über ein Netzwerk aus der Ferne auf einen Rechner mit Windows-Betriebssystem zugreifen lässt.
Quelle: Shodan.io

Beschädigt

Schäden bei Opfern von Cyberkriminalität; Befragte, die bereits Opfer von Internetkriminalität geworden sind; Deutschland; in Prozent *



* Mehrfachnennungen möglich. Quelle: BSI

Befürchtet

Befürchtete Schäden im Internet; Personen ab 16 Jahren, die das Internet nutzen und nicht von Cyberattacken betroffen waren (n=2 184); Deutschland; 2023; in Prozent *

Welche Schäden durch Internetkriminalität fürchten Sie am meisten?

	Rang 1	Rang 2	Rang 3
finanzieller Schaden	50	21	11
Verlust von Daten	22	35	16
Rufschädigung	7	12	17
Vertrauensverluste in Online-Dienste	5	9	17
emotionaler Schaden	6	9	15
Verlust eines Geräts	7	9	13
zeitlicher Schaden	2	6	11

* Mehrfachnennungen möglich. Quelle: BSI

Besorgt

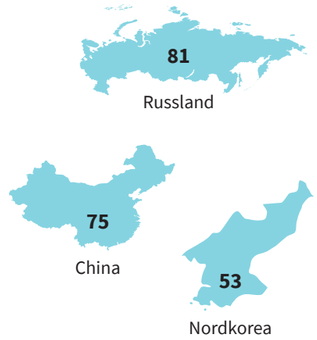
Konkrete Ängste vor Vorfällen im Internet; Internetnutzerinnen und -nutzer ab 16 Jahren (n=1 018); Deutschland; 2023; in Prozent *

Viren oder Ransomware	90
Identitätsdiebstahl	62
Diebstahl von Passwörtern	55
Betrug beim Online-Banking	42
Beleidigung oder Mobbing	41
Betrug beim Online-Einkauf	39
Hassrede	29
sexuelle Belästigung	18

* Mehrfachnennungen möglich. Quelle: Bitkom

Beschuldigt

Länder, die die größte Gefahr im Bereich Cybersicherheit darstellen; Internetnutzerinnen und -nutzer ab 16 Jahren (n=1 018); Deutschland; 2023; in Prozent *

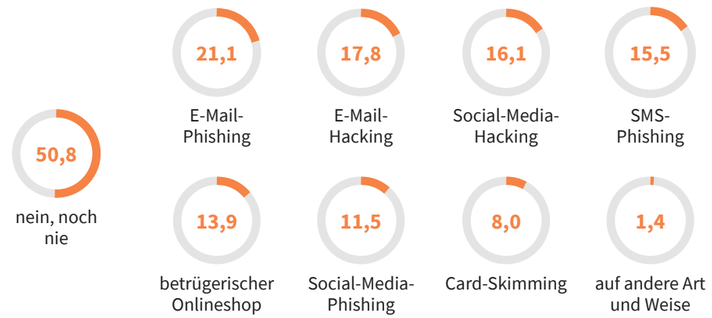


* Mehrfachnennungen möglich. Quelle: Bitkom

Betroffen

Betroffenheit von Hackerangriffen nach Art des Angriffs; Nutzerinnen und Nutzer von VPN-Diensten (n=578); Deutschland; 2023; in Prozent *

Sind Sie schon einmal Opfer eines Hackerangriffs geworden? Und wenn ja, welcher Bereich war betroffen?

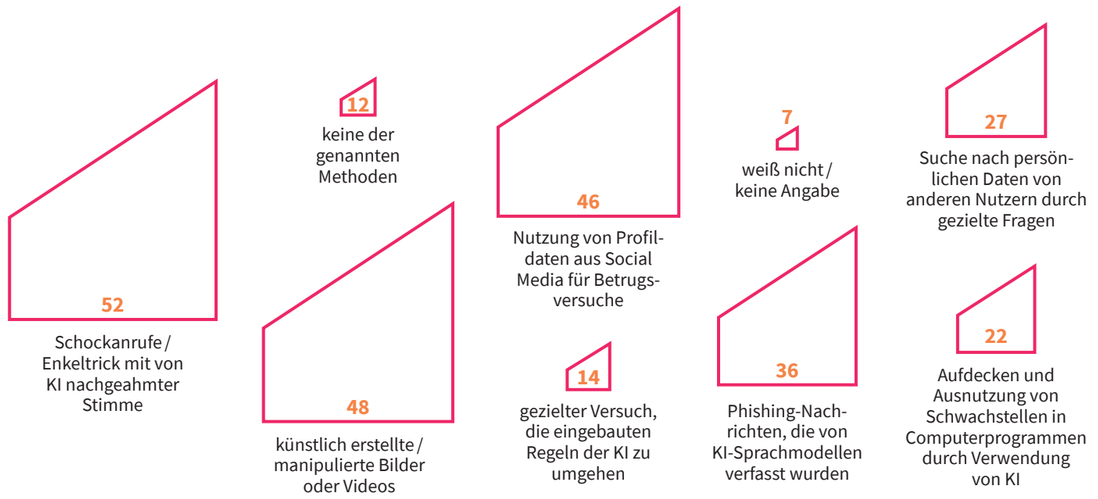


* Mehrfachnennungen möglich. Quelle: Forbes Advisor

Bekannt

Bekanntheit von krimineller Nutzung von KI; Personen ab 16 Jahren, die das Internet nutzen (n=3 012); Deutschland; 2023; in Prozent

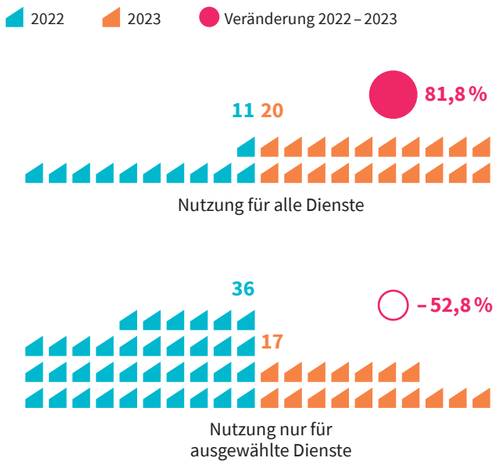
Haben Sie von folgenden Methoden Krimineller bereits gehört?



* Mehrfachnennungen möglich. Quelle: BSI

Nützlich

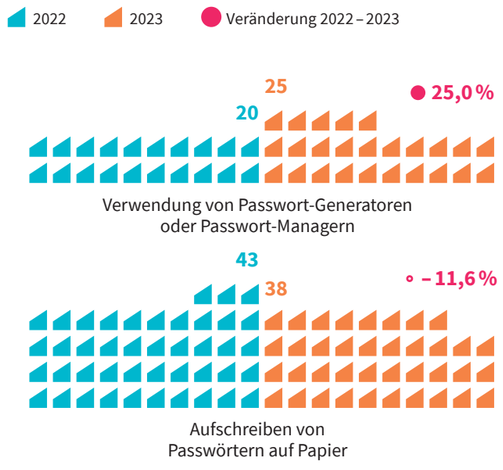
Nutzung von Zwei-Faktor-Authentifizierung; Internetnutzerinnen und -nutzer ab 16 Jahren (n=1 018); Deutschland; 2023; in Prozent



Quelle: Bitkom

Betulich

Umgang mit Passwörtern; Internetnutzerinnen und -nutzer ab 16 Jahren (n=1 018); Deutschland; 2023; in Prozent



Quelle: Bitkom

Zögerlich

Bekannteste / unbekannteste Sicherheitsmaßnahmen; Verbraucherinnen und Verbraucher ab 16 Jahren (n=2 000+); Deutschland; 2023; in Prozent

am bekanntesten

98,4 Verwendung starker Passwörter

98,1 Nutzung unterschiedlicher Passwörter für unterschiedliche Zwecke

98,0 Updates von Apps

97,7 Schutz des Geräts mit einer PIN

97,6 regelmäßige Aktualisierung des Betriebssystems des Computers

am unbekanntesten

87,4 Einsatz eigener elektronischer Signaturen

86,2 Auslesen der E-Mail-Header

85,5 Einsatz von VPN oder Proxy-Clients

Quelle: DsiN

Sträflich

Meistgenutzte / am wenigsten genutzte Sicherheitsmaßnahmen; Verbraucherinnen und Verbraucher ab 16 Jahren (n=2 000+); Deutschland; 2023; in Prozent

am meisten genutzt

74,8 Verwendung starker Passwörter

73,0 regelmäßige Updates von Apps

72,6 regelmäßige Updates des Betriebssystems

72,4 Schutz mit PIN etc.

am wenigsten genutzt

31,5 Auslesen der E-Mail-Header

31,5 Überprüfung fremder elektronischer Signaturen

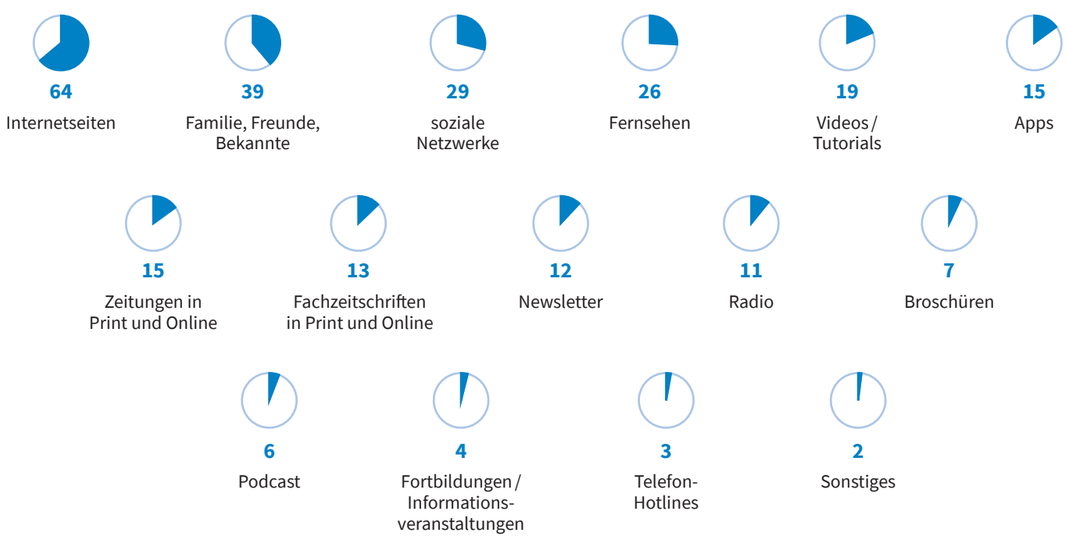
30,6 Verschlüsselung der Festplatte

26,0 Einsatz eigener elektronischer Signaturen

Quelle: DsiN

Erstaunlich

Genutzte Informationskanäle zum Thema Cybersicherheit; Personen ab 16 Jahren, die das Internet nutzen und gezielt nach Informationen suchen (n=2 345); Deutschland; 2023; in Prozent *



* Mehrfachnennungen möglich. Quelle: BSI

Wichtig

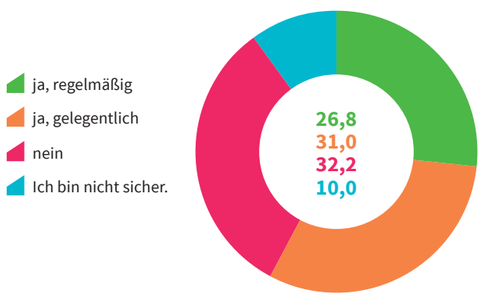
Wichtigkeit der Sicherheit bei Anwendungen und Online-Aktivitäten; Personen in Deutschland ab 16 Jahren, die das Internet nutzen (n=3 012); Deutschland; 2023; in Prozent

Quelle: BSI

Regelmäßig

Nutzung von VPN-Diensten; Deutschland; 2023; in Prozent

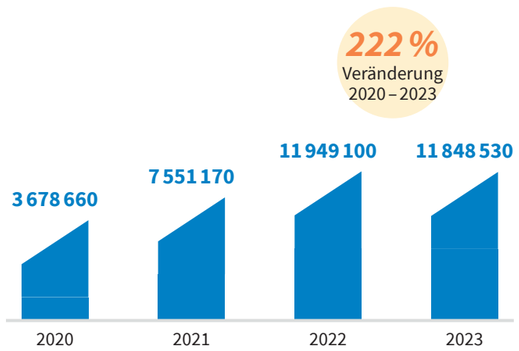
Nutzen Sie ein VPN (virtuelles privates Netzwerk)?



Quelle: Forbes Advisor

Stetig

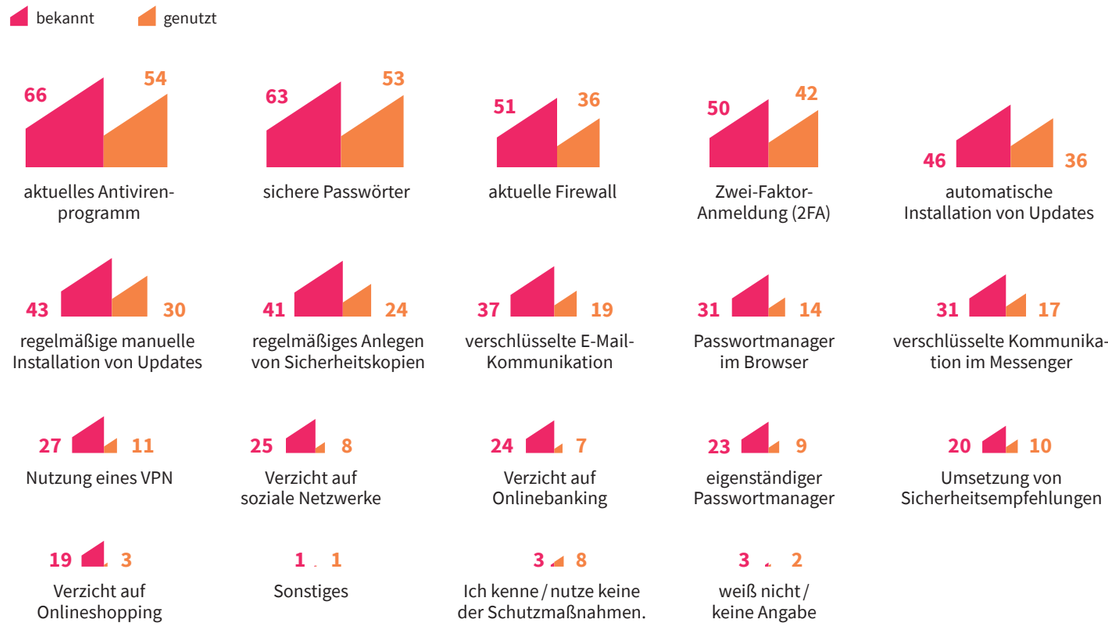
Zahl der VPN-Downloads; Deutschland



Quelle: Atlas VPN

Happig

Bekannte und genutzte Maßnahmen für weniger Gefahren im Internet; Personen in Deutschland ab 16 Jahren, die das Internet nutzen (n=3 012); Deutschland; 2023; in Prozent *

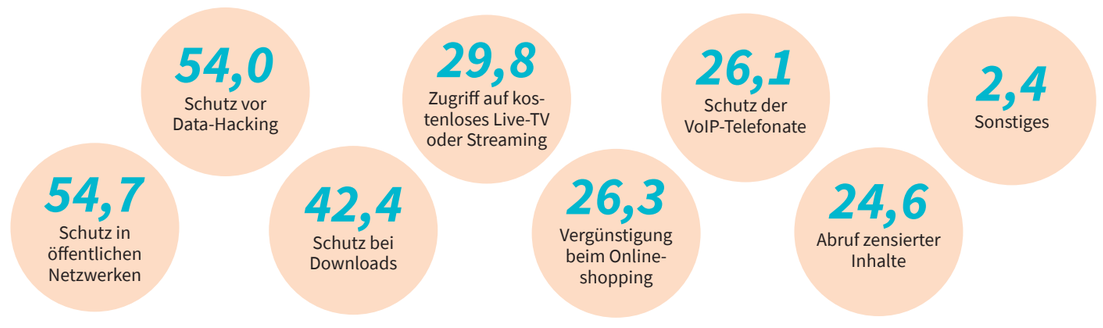


* Mehrfachnennungen möglich. Quelle: BSI

Vernünftig

Gründe für die Nutzung eines VPN-Dienstes; Nutzerinnen und Nutzer von VPN-Diensten (n=578) Deutschland; 2023; in Prozent *

Warum nutzen Sie ein VPN (virtuelles privates Netzwerk)?



* Mehrfachnennungen möglich. Quelle: Forbes Advisor

Behäbig

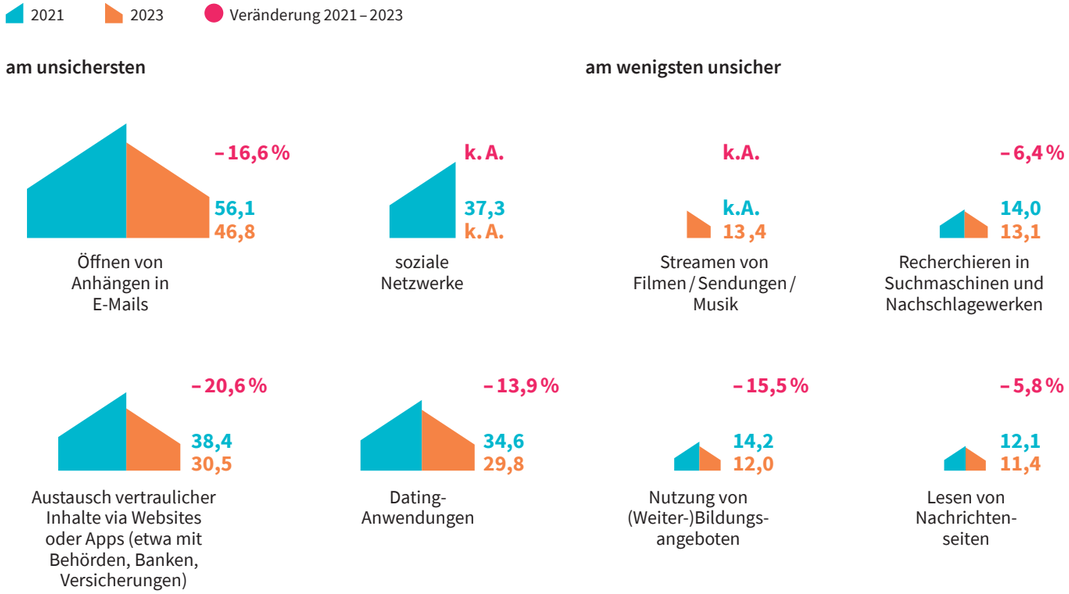
Reaktionen auf Sicherheitsvorfälle; Befragte, die in den vergangenen zwölf Monaten Opfer von Internetkriminalität geworden sind (n=313); Deutschland; 2023; in Prozent *

Wie haben Sie auf die Straftaten reagiert?

* Mehrfachnennungen möglich. Quelle: BSI

Leichtsinnig

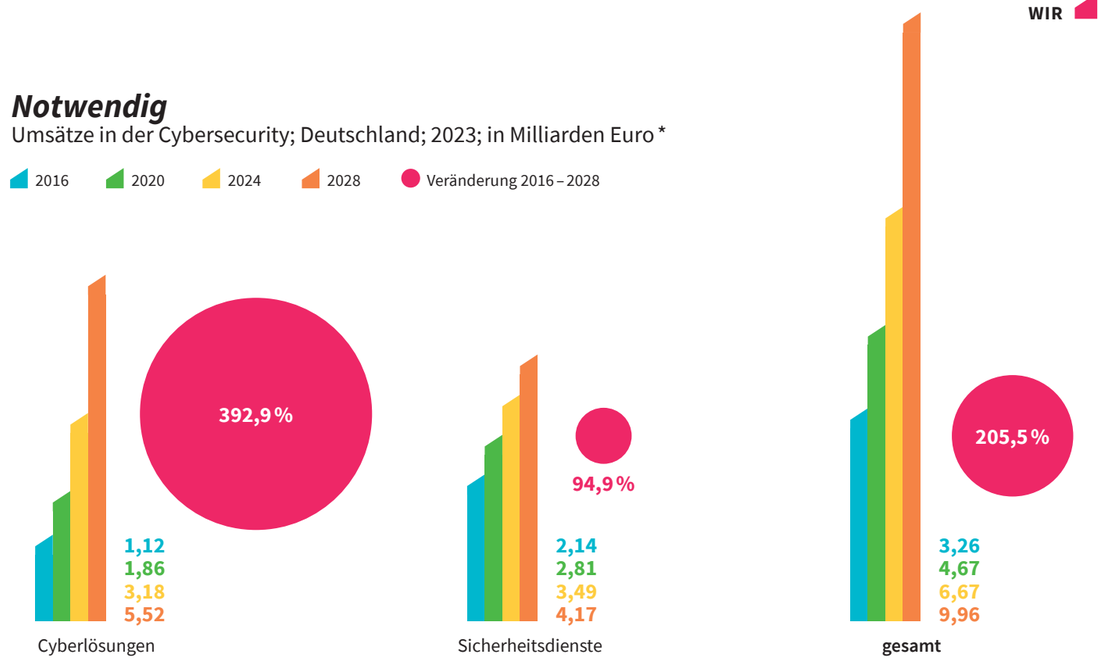
Sicherheitsgefühl im Internet nach Aktivitäten; Verbraucherinnen und Verbraucher ab 16 Jahren (n=2 000+); Deutschland; in Prozent



Quelle: DsiN

Notwendig

Umsätze in der Cybersecurity; Deutschland; 2023; in Milliarden Euro *

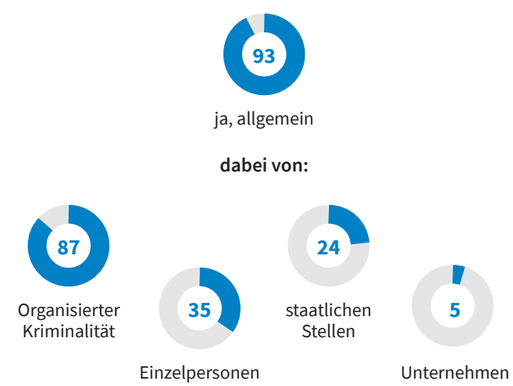


* Daten werden in aktuellen Wechselkursen gezeigt und reflektieren die Einflüsse des Russland-Ukraine Kriegs auf den Markt. Quelle: Statista Market Insights

Unruhig

Angst und Bedrohungsgefühl im Internet; Internetnutzerinnen und -nutzer ab 16 Jahren (n=1 018); Deutschland; 2023; in Prozent *

Fühlen Sie sich im Internet bedroht?

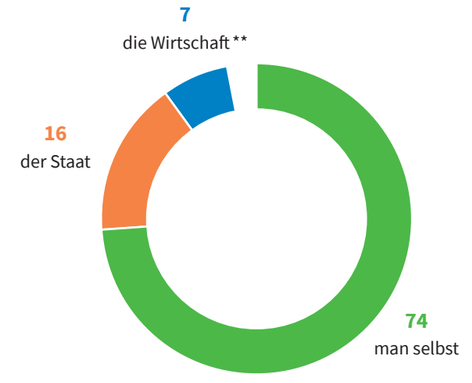


* Mehrfachnennungen möglich. Quelle: Bitkom

Zuständig

Zuständigkeitsgefühl für die Sicherheit im Internet; Internetnutzerinnen und -nutzer ab 16 Jahren (n=1 018); Deutschland; 2023; in Prozent *

Wer ist verantwortlich für die Sicherheit im Internet?



* Fehlende Prozent zu 100: weiß nicht / keine Angabe. ** z. B. Internetanbieter oder die Hersteller von Soft- und Hardware. Quelle: Bitkom

GLOSSAR

Advanced Persistent Threats (APT): Bei APT handelt es sich um zielgerichtete Cyberangriffe auf ausgewählte Institutionen, bei denen sich ein Angreifer dauerhaften Zugriff zu einem Netz verschafft und diesen in der Folge auf weitere Systeme ausweitet.

Backdoor (Deutsch: Hintertür): Eine Backdoor ist ein üblicherweise durch Viren, Würmer oder Trojaner installiertes Programm, das Dritten unbefugten Zugang zum Computer verschafft, jedoch versteckt und unter Umgehung der üblichen Sicherheitseinrichtungen.

Brute-Force-Angriff: Wählen Nutzerinnen und Nutzer ein schwaches Passwort und ist der Benutzername bekannt, kann sich eine Angreifergruppe unter Umständen auch durch wiederholtes Ausprobieren von Passwörtern (Brute-Force-Angriff) Zugang zu einem Benutzerkonto verschaffen. Mittels Brute-Force-Techniken können Cyberkriminelle auch versuchen, kryptografisch geschützte Daten, z. B. eine verschlüsselte Passwort-Datei, zu entschlüsseln.

Business E-Mail Compromise (BEC): Bei BEC versuchen Cyberkriminelle, andere Personen durch betrügerische E-Mails dazu zu bringen, Geld zu überweisen oder vertrauliche Unternehmensdaten preiszugeben. Die Akteure geben sich als vertrauenswürdige Personen aus und verlangen die Bezahlung einer gefälschten Rechnung oder die Herausgabe vertraulicher Daten, die sie für weitere betrügerische Aktivitäten missbrauchen können.

Computervirus: Ein Computervirus ist eine nicht selbstständige Programmroutine, die sich selbst reproduziert und dadurch von den Anwenderinnen und Anwendern nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. Der Begriff hat sich als Sammelbezeichnung für alle Arten von Schadsoftware durchgesetzt – auch für Schadprogramme, die in ihrer eigentlichen Definition keine Viren mehr sind.

Cookie: Zeichenfolge, die mit einer Webseite vom Server geladen werden kann und bei einer erneuten Anfrage an den Server mitgesendet wird. Sinn ist unter anderem, Besucherinnen und Besucher wiederzuerkennen, sodass es beispielsweise nicht erforderlich ist, Nutzerdaten neu einzugeben.

Cyberabwehr: Cyberabwehr umfasst alle Maßnahmen mit dem Ziel der Wahrung oder Erhöhung der Cybersicherheit.

Cyberangriff: Ein Cyberangriff ist eine Einwirkung auf ein oder mehrere andere informationstechnische Systeme im oder durch den Cyberraum, die zum Ziel hat, deren IT-Sicherheit durch informationstechnische Mittel ganz oder teilweise zu beeinträchtigen.

Cybermobbing: Cybermobbing steht für verschiedene Formen der Diffamierung, Belästigung, Bedrängung und Nötigung anderer Menschen oder Firmen über das Internet. Das Opfer wird durch aggressive oder beleidigende Texte, kompromittierende Fotos oder Videos angegriffen oder der Lächerlichkeit ausgesetzt.

Cyberstalking: Cyberstalking (auch Digital Stalking oder Onlinestalking) bezeichnet das Nachstellen, Verfolgen und auch Überwachen einer Person mit digitalen Hilfsmitteln.

Cybervault: Ein Cybervault ist ein mehrschichtiger Schutz gegen Cyberangriffe.

Data Breach: Ein Data Breach ist das Offenlegen vertraulicher Daten von einer externen Quelle. Es handelt sich dabei um einen direkten Angriff von außen mit dem Ziel des Datendiebstahls. Hauptmerkmal eines Data Breaches ist, dass es von außen nach innen passiert.

Data Leak: Data Leaks sind nicht autorisierte Übertragungen von Informationen innerhalb eines Unternehmens nach außen. Dabei wird nicht zwischen der physischen (USB-Stick) und der digitalen (E-Mail) Übertragung unterschieden. Das kann beispielsweise eine Kollegin oder ein Kollege sein, die oder der Kundendaten an andere Unternehmen oder Hackerinnen und Hacker verkauft. Hauptmerkmal eines Data Leaks ist, dass es von innen nach außen passiert. Deshalb ist diese Art des Datendiebstahls für Unternehmen schwer zu verhindern.

Defacement / Defacing: Ein Defacement bezeichnet die – meist plakative – Veränderung von Webseiten-Inhalten durch Dritte.

Denial-of-Service-Angriffe (DoS / DDoS): DoS-Angriffe richten sich gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen. Wird ein solcher Angriff mittels mehrerer Systeme parallel ausgeführt, spricht man von einem verteilten DoS- oder DDoS-Angriff (DDoS = Distributed Denial of Service). DDoS-Angriffe erfolgen häufig durch eine sehr große Zahl von Computern oder Servern.

DevSecOps: Das Kunstwort setzt sich aus den Einzelbegriffen Entwicklung (Development), Sicherheit (Security) und Betrieb (Operations) zusammen. Es handelt sich um einen ganzheitlichen Ansatz, der die Sicherheit in allen Phasen des Lebenszyklus einer Software berücksichtigt und in die Prozesse integriert.

Distributed-Ledger-Technologie (DLT): Bei DLT handelt es sich um ein digitales System zur Aufzeichnung von Transaktionen, bei dem die Transaktionen und ihre Details an mehreren Stellen gleichzeitig aufgezeichnet werden. Im Gegensatz zu herkömmlichen Datenbanken gibt es bei einem Distributed Ledger (verteiltes Hauptbuch oder Kassenbuch) keine zentrale Datenhaltung oder Verwaltungsfunktion.

Doxing: Doxing oder Doxxing („Dox" als Abkürzung für „Documents") bezeichnet das internetbasierte Zusammentragen und Veröffentlichen von personenbezogenen Daten an einem zentralen Ort wie einer Datenbank. Hierzu gehören Kontaktdaten und -adressen, Informationen zu Kontakten, Beziehungen oder Gruppenzugehörigkeit, aber auch freizügige Fotos oder intime Aussagen.

Ende-zu-Ende-Verschlüsselung: Die Ende-zu-Ende-Verschlüsselung ist eine durchgängige Verschlüsselung zwischen Absenderinnen und Absendern und Empfängerinnen und Empfängern. Den Begriff trifft man vor allem bei der E-Mail-Kommunikation an. Um Ende-zu-Ende-Verschlüsselung verwenden zu können, benötigen beide Parteien entsprechende Verschlüsselungssoftware und müssen den jeweils öffentlichen Schlüssel des Kommunikationspartners besitzen. Die bekanntesten Verfahren sind S/MIME und PGP.

Endpoint Security: Endpoint Security schützt die verschiedenen Endgeräte in einem Netzwerk vor diversen Bedrohungen. Technische und organisatorische Maßnahmen verhindern den unbefugten Zugriff auf Geräte oder die Ausführung schädlicher Software. Der Endpunktschutz stellt sicher, dass die Endgeräte das gewünschte Sicherheitsniveau erreichen.

Exploit: Als Exploit bezeichnet man eine Methode oder einen Programmcode, mit dem über eine Schwachstelle in Hardware- oder Software-Komponenten nicht vorgesehene Befehle oder Funktionen ausgeführt werden können. Je nach Art der Schwachstelle kann mithilfe eines Exploits z. B. ein Programm zum Absturz gebracht oder ein beliebiger Programmcode ausgeführt werden.

Firewall: Die Firewall besteht aus Hard- und Software, die den Datenfluss zwischen dem internen Netzwerk und dem externen Netzwerk kontrolliert. Alle Daten, die das Netz verlassen, können ebenso überprüft werden wie die, die hineinwollen.

Fuzzing: Fuzzing ist eine automatisierte Testmethode für Software, bei der ein Programm eine Vielzahl automatisch generierter Eingabedaten verarbeiten muss, ohne dabei eine Fehlfunktion zu zeigen. Findet ein Hacker durch Fuzzing ein Eingabemuster, das eine Fehlfunktion erzeugt, muss überprüft werden, ob sich der gefundene Fehler als Sicherheitslücke ausnutzen lässt.

Hacker: Computernutzerinnen und -nutzer mit überdurchschnittlichem Fachwissen, die sich mit dem Erstellen und Verändern von Computersoftware oder -hardware beschäftigen. Im Bereich der Computersicherheit gelingt es ihnen häufig, Sicherheitslücken in Computerprogrammen aufzuspüren und dabei zu helfen, diese zu beseitigen. Hacker, die Sicherheitslücken ausnutzen, um illegalen Zugriff auf fremde Systeme zu erlangen und dort eventuell Schaden anzurichten, werden in der Hackerszene als „Cracker" bezeichnet.

Hack-and-Leak-Angriffe: Bei Hack-and-Leak-Operationen versuchen Bedrohungsakteure mittels cybergestützter Angriffstechniken in private oder berufliche Computersysteme vorzudringen („Hack"), um diskreditierendes oder belastendes Material über das Opfer zu erlangen. Dieses wird anschließend im Original oder in verfälschender Form beispielsweise in Online-Foren oder über Social-Media-Kanäle veröffentlicht („Leak").

Identitätsdiebstahl: Nutzerinnen und Nutzer identifizieren sich im Internet meist über eine Kombination aus Identifikations- und Authentisierungsdaten, z. B. Benutzername und Passwort. Verschafft sich ein unberechtigter Dritter Zugang zu solchen Daten, so wird von einem Identitätsdiebstahl gesprochen.

Identity and Access Management (IAM): Unter IAM versteht man in der IT alle Aufgaben rund um die Verwaltung von digitalen Identitäten (Identity) und den damit verknüpften Zugriffsrechten (Access). IT-Berechtigungen legen fest, welche Dateien ein Benutzer öffnen kann, welche Applikationen er verwenden kann und welche Bereiche des Netzwerks ihm zugänglich sind.

Information Stealer: Ein Info Stealer (Information Stealer) ist ein Schadprogramm, das darauf spezialisiert ist, bestimmte Arten von persönlichen Daten, beispielsweise Log-in-Daten, zu erkennen, zu sammeln und an eine fremde Quelle zu senden. Dies geschieht in der Regel unbemerkt und über einen langen Zeitraum.

Internet der Dinge / Internet of Things (IoT): Im Gegensatz zu „klassischen" IT-Systemen umfasst das Internet der Dinge „intelligente" Gegenstände, die zusätzliche „smarte" Funktionen enthalten. Diese Geräte werden in der Regel an Datennetze angeschlossen, in vielen Fällen drahtlos, und können sogar oft auf das Internet zugreifen und darüber erreicht werden.

Intrusion Detection & Prevention System (IDS / IPS): Ein IDS ist ein System, das ein Netzwerk oder eine Netzwerkkomponente überwacht und verdächtige Aktivitäten wie Angriffe oder schadhafte Datenübertragung anhand von Mustern und Heuristik erkennen kann. Über die reine Erkennung hinaus kann ein Intrusion-Prevention-System (IPS) auch aktiv abwehrende Maßnahmen einleiten.

Keylogger: Als Keylogger wird Hard- oder Software zum Mitschneiden von Tastatureingaben bezeichnet. Sie zeichnen alle Tastatureingaben auf, um sie möglichst unbemerkt an Angreiferinnen und Angreifer zu übermitteln. Diese können dann aus diesen Informationen für sie wichtige Daten wie etwa Anmeldeinformationen oder Kreditkartennummern filtern.

Krypto-Mining / Kryptowährungen schürfen: Unter Krypto-Mining wird das Generieren (Schürfen) von neuen Einheiten einer Kryptowährung verstanden. Dadurch erhöht sich die im Umlauf befindliche Menge. Dieser Prozess ist vergleichbar mit der Erhöhung der Geldmenge durch Zentralbanken.

Malware: Die Begriffe Schadfunktion, Schadprogramm, Schadsoftware und Malware werden häufig synonym benutzt. Malware ist ein Kunstwort, abgeleitet aus „Malicious software", und bezeichnet Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. Beispiele sind Computerviren, Würmer und Trojaner. Schadsoftware ist üblicherweise für eine bestimmte Betriebssystemvariante konzipiert und wird daher meist für verbreitete Systeme und Anwendungen geschrieben.

Managed Detection & Response (MDR) Services: Bei MDR lagern Unternehmen ihre IT-Sicherheit in Bezug auf Erkennung und Reaktion auf Bedrohungen an Dienstleister aus. Je nach MDR-Angebot installiert die Anbieterin oder der Anbieter Technologie lokal beim Kunden und bietet zusätzliche externe und automatisierte Dienste über Software an.

Multi-Factor-Authentifizierung (MFA): Bei der MFA werden zwei oder mehr unabhängige Berechtigungsnachweise kombiniert: etwas, das die Nutzerinnen und Nutzer wissen, zum Beispiel ein Kennwort; etwas, das die Nutzerinnen und Nutzer besitzen, zum Beispiel ein Sicherheits-Token; und etwas, das die Nutzerinnen und Nutzer sind, zum Beispiel durch die Verwendung biometrischer Verifizierungsmethoden.

Network Acces Control: Die Netzwerkzugangskontrolle ist eine Methode, mit der die Sicherheit eines proprietären Netzwerks verbessert werden kann. Man schränkt dabei die Verfügbarkeit der Netzwerk-Ressourcen auf entsprechende Endgeräte ein, die definierte Sicherheitsrichtlinien erfüllen.

〉

Paketfilter-/Proxy-Firewall: Eine Proxy-Firewall ist ein Security-System für das Netzwerk. Es schützt die Ressourcen im Netzwerk, indem Kommunikation auf der Anwendungsschicht gefiltert wird. Man bezeichnet eine Proxy-Firewall auch als Application Firewall oder Gateway Firewall.

Patch (Deutsch: Flicken): Kleines Programm, das Fehler in Anwendungsprogrammen oder Betriebssystemen behebt.

Penetrationstest: Mit einem Penetrationstest kann herausgefunden werden, ob die Sicherheit innerhalb einer kritischen Umgebung gewährleistet ist. In beliebigen Systemen und Applikationen, z. B. Webseiten oder Warenwirtschaftssystemen, werden Schwachstellen identifiziert, die es einer Angreiferin oder einem Angreifer ermöglichen, in das System einzudringen. Hierfür werden automatisierte und manuelle Angriffsschritte kombiniert und mithilfe von realistischen und kontrollierten Angriffen Sicherheitslücken im IT-System aufgedeckt. Die genutzten Angriffsmethoden entsprechen denen realer Angreiferinnen und Angreifer und decken deren gesamte Bandbreite an Methoden ab.

Personal Firewall: Programm, das auf einer Arbeitsplatzmaschine installiert wird. Sie soll genau wie eine Hardware-Firewall, die im Unternehmensumfeld zum Einsatz kommt, den Rechner vor Angriffen von außen schützen und wird vorwiegend im privaten Bereich eingesetzt.

Pharming: Wie beim Phishing sind auch beim Pharming meist Zugangsdaten das Ziel eines Angriffs. Der Unterschied zum Phishing besteht darin, dass beim Pharming die Infrastruktur so manipuliert wird, dass das Opfer auch dann auf einer gefälschten Webseite landet, wenn es die korrekte Adresse des Dienstes eingegeben hat. Technisch geschieht das in der Regel durch eine Manipulation der DNS-Einträge in der lokalen Hosts-Datei, an einem Zwischenspeicher oder an der zentralen DNS-Infrastruktur.

Phishing: Das Wort setzt sich aus „Password“ und „Fishing“ zusammen, zu Deutsch „nach Passwörtern angeln“. Beim Phishing wird z. B. mittels gefälschter E-Mails und / oder Webseiten versucht, Zugangsdaten für einen Dienst oder eine Webseite zu erlangen. Wird diese Manipulation vom Opfer nicht erkannt und die Authentizität einer Nachricht oder Webseite nicht hinterfragt, gibt das Opfer seine Zugangsdaten unter Umständen selbst unwissentlich in unberechtigte Hände. Bekannte Beispiele sind Phishing-Angriffe gegen Bankkunden, die in einer E-Mail aufgefordert werden, ihre Zugangsdaten auf der Webseite der Bank einzugeben und validieren zu lassen. Mit dem gleichen Verfahren werden aber auch Nutzerinnen und Nutzer von E-Commerce-Anwendungen angegriffen, z. B. Onlineshops oder Online-Dienstleister.

Ransomware: Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (englisch: „ransom“) wieder freigeben. Es handelt sich dabei um eine Form digitaler Erpressung.

Remote Access Trojaner (RAT): Ein RAT ist ein Fernzugriffs-Trojaner, ein Malware-Programm, das eine Hintertür für die administrative Kontrolle über den Zielcomputer enthält. RATs werden in der Regel unsichtbar mit einem von Benutzerinnen und Benutzern angeforderten Programm – z. B. einem Tool – heruntergeladen oder als E-Mail-Anhang versandt.

Remote Desktop Protocol (RDP): RDP ist ein Netzwerk-Kommunikationsprotokoll, das von Microsoft entwickelt wurde. Es ermöglicht Administratoren, aus der Ferne auf Computer von Benutzern zuzugreifen, um Probleme zu identifizieren und zu lösen.

Rootkit: Als Rootkit wird eine Sammlung von Softwarewerkzeugen bezeichnet, die die Präsenz schädlicher oder unerwünschter Software auf einem Rechner verschleiert und verdächtige Aktivitäten versteckt. Sie greift tief in das Betriebssystem des betroffenen Rechners ein, verschafft Angreifern erweiterte Rechte und bietet Remote-Zugriffsmöglichkeiten.

Scam (Deutsch: Betrug, Schwindel): Beispiel für eine Scam-Mail ist eine E-Mail, die Empfängerinnen und Empfängern einen Gewinn vorgaukelt, für die Überweisung desselben aber eine Gebühr verlangt. Natürlich existiert der Gewinn nicht wirklich.

Schwachstelle: Eine Schwachstelle oder Sicherheitslücke ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird.

Security Information and Event Management (SIEM): Es handelt sich um ein softwarebasiertes Technologiekonzept aus dem Bereich des Sicherheits-Managements, mit dem ein ganzheitlicher Blick auf die IT-Sicherheit möglich wird. SIEM stellt eine Kombination aus Security Information Management (SIM) und Security Event Management (SEM) dar. Durch das Sammeln, Korrelieren und Auswerten von Meldungen, Alarmen und Logfiles verschiedener Geräte, Netzkomponenten, Anwendungen und Security-Systemen in Echtzeit werden Angriffe, außergewöhnliche Muster oder gefährliche Trends sichtbar.

Sinkhole: Als Sinkhole wird ein Computersystem bezeichnet, auf das Anfragen von botnetzinfizierten Systemen umgeleitet werden. Sinkhole-Systeme werden typischerweise von Sicherheitsforschern betrieben, um Botnetz-Infektionen aufzuspüren und betroffene Anwender zu informieren.

Skimming: Skimming bezeichnet das unbemerkte Auslesen von Zahlungskarten durch physikalische Manipulation von Zahlungs-Terminals. Mit den ausgelesenen Daten werden Kopien der Karten erstellt. Um auf das Konto des Opfers zugreifen zu können, wird meist auch die Eingabe der zugehörigen PIN aufgezeichnet, mithilfe einer unauffälligen Kamera oder einer manipulierten Tastatur.

Smishing: Smishing ist eine Form des Phishings, bei dem überzeugende Phishing-SMS / -Textnachrichten verwendet werden, um ein potenzielles Opfer dazu zu verleiten, auf einen Link zu klicken und private Informationen zur Angreiferin oder zum Angreifer zu senden oder Malware auf das Handy zu laden.

Social Engineering: Bei Cyberangriffen durch Social Engineering versuchen Kriminelle ihre Opfer dazu zu verleiten, eigenständig Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadprogramme auf ihren Systemen zu installieren. Sowohl im Bereich der Cyberkriminalität als auch bei der Spionage gehen die Täter geschickt vor, um vermeintliche menschliche Schwächen wie Neugier oder Angst auszunutzen und so Zugriff auf sensible Daten und Informationen zu erhalten.

Software Bundler: Ein Software Bundler ist ein Programm, das unerwünschte Software auf einem PC installiert, und zwar gleichzeitig mit der Software, die man zu installieren versucht.

Spam: Unter Spam versteht man unerwünschte Nachrichten, die massenhaft und ungezielt per E-Mail oder über andere Kommunikationsdienste versendet werden. In der harmlosen Variante enthalten Spam-Nachrichten meist unerwünschte Werbung. Häufig enthält Spam jedoch auch Schadprogramme im Anhang, Links zu verseuchten Webseiten oder wird für Phishing-Angriffe genutzt.

Spear-Phishing: Beim Spear-Phishing wird nicht breitflächig attackiert, sondern nur ein kleiner Empfängerkreis (häufig Führungskräfte oder Wissensträgerinnen und Wissensträger auf Leitungsebene). Voraussetzung für einen erfolgreichen Angriff ist die Einbettung in einen für das Opfer glaubwürdigen Kontext. Spear-Phishing richtet sich in der Regel nicht gegen allgemein nutzbare Dienste wie Onlinebanking, sondern gegen Dienste, die für Angreifergruppen einen besonderen Wert haben.

Spoofing (Deutsch: manipulieren, vortäuschen): Spoofing nennt man in der Informationstechnik verschiedene Täuschungsversuche zur Verschleierung der eigenen Identität und zum Fälschen übertragener Daten. Das Ziel besteht darin, die Integrität und Authentizität der Informationsverarbeitung zu untergraben.

Spyware: Als Spyware werden Programme bezeichnet, die heimlich, also ohne darauf hinzuweisen, Informationen über eine Benutzerin oder einen Benutzer bzw. die Nutzung eines Rechners sammeln und an die Urheberin oder den Urheber der Spyware weiterleiten. Dabei können auch sicherheitsrelevante Informationen wie Passwörter ausgeforscht werden.

SQL Injection: SQL Injection ist eine Sicherheitslücke, bei der die Angreiferin oder der Angreifer eine Anfrage über ein Web-Formular per Structured Query Language (SQL) erweitert, um auf Ressourcen zuzugreifen oder Daten zu verändern. Eine SQL-Abfrage ist eine Anforderung, die eine Aufgabe in einer Datenbank ausführt.

Telephone-Oriented Attack Delivery (TOAD): TOAD ist eine Phishing-Variante, bei der die Angreifer am Telefon als angebliche vertrauenswürdige Autoritätsperson (z. B. eines anerkannten Unternehmens oder einer Organisation) auftreten und versuchen, ihre Opfer zur Preisgabe vertraulicher Informationen (z. B. Anmeldedaten oder Finanzdaten) zu verleiten. Anschließend senden sie dem Opfer eine E-Mail, die einen Phishing-Link oder -Anhang enthält.

Threat Monitoring: Threat Monitoring ist die gezielte und kontinuierliche Analyse und Bewertung von Online-Daten, um Cyberbedrohungen oder Datenschutzverletzungen zu erkennen. Die Überwachung umfasst in der Regel einen hochgradigen Zugriff auf Netzwerke und Benutzeraktionen, um unerwünschte Eindringlinge leicht identifizieren oder stoppen zu können oder die Bedrohung verhindern zu können.

Trojaner: EinTrojaner ist ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung. Es verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer.

Virenschutzprogramm: Ein Virenschutzprogramm überprüft neue Dateien (z. B. E-Mail-Anhänge) und den gesamten Computer auf Schadsoftware. Dazu vergleicht es in erster Linie die Daten auf dem Rechner mit den „Fingerabdrücken“ bekannter Schadprogramme.

Virensignatur: Eine Virensignatur ist der Fingerabdruck eines Virus. Technisch gesehen, ist es eine kurze Byte-Folge, die aus dem betreffenden Virus extrahiert wird und ihn eindeutig identifiziert. Virenschutzprogramme, die mit Signatur-Scanning arbeiten, besitzen eine Datenbank mit den Fingerabdrücken aller bekannten Viren.

Virtual Private Network (VPN): VPNs verschlüsseln die Datenkommunikation zwischen zwei Endpunkten – z. B. zwischen einem Endgerät und einem VPN-Server. Auf diese Weise kann die Kommunikation nicht ohne Weiteres mitgelesen oder verändert werden.

Vishing: Betrugsmasche von Datendieben (Kombination aus der englischen Bezeichnung für Internettelefonie „Voice over Internet Protocol“ (VoIP) und dem Namen der Betrugstechnik „Phishing“). Die geringen Kosten der Internettelefonie werden dazu genutzt, um automatisch eine große Zahl von Telefongesprächen zu führen. In diesen wird beispielsweise behauptet, eine Kreditkarte sei verloren gegangen. Die Opfer sollen dann persönliche Daten wie PIN- oder TAN-Codes über die Telefontastatur eingeben.

Zero-Day-Exploit: Die Ausnutzung einer Schwachstelle, die nur der Entdeckerin oder dem Entdecker bekannt ist, charakterisiert man mit dem Begriff Zero-Day-Exploit. Die Öffentlichkeit und insbesondere die Herstellerin oder der Hersteller des betroffenen Produktes erlangen in der Regel erst dann Kenntnis von der Schwachstelle, wenn Angriffe entdeckt werden, die auf dieser Schwachstelle basieren. Die Bezeichnung „zero day“ leitet sich also davon ab, dass ein entsprechender Exploit bereits vor dem ersten Tag der Kenntnis der Schwachstelle durch die Herstellerin oder den Hersteller existierte – also an einem fiktiven „Tag null“. Die Herstellerin oder der Hersteller hat somit keine Zeit, die Nutzerinnen und Nutzer vor den ersten Angriffen zu schützen.

Zero-Trust-Modell: Das Zero-Trust-Sicherheitskonzept geht davon aus, dass nichts sicher ist – auch nicht hinter der Firmen-Firewall. Deshalb prüft das Modell jede Anforderung so, als käme sie aus einem offen zugänglichen Netzwerk. Bevor der Zugriff gewährt wird, muss eine Anforderung vollständig authentifiziert, autorisiert und verschlüsselt sein.

Quellen: ADAN, Bundesamt für Sicherheit in der Informationstechnik (BSI), Cloudflare, ComputerWeekly, Dataversity, Externetworks, Gabler Wirtschaftslexikon, Google, IT-Service.Network, LSI Bayern, Microsoft, NIST, Proofpoint, Rapid7, RiskXchange, Security Insider, TechTarget, Wiener Börse

QUELLENVERZEICHNIS

(ISC)²
Allianz
ARD
Atlas VPN
Bitkom e. V.
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Bundeskriminalamt (BKA)
Bundesverband IT-Mittelstand e. V. (bitmi)
Capgemini
Civey, neue fische
ComputerWeekly
CVE
CyberEdge
Deutsche Telekom
Deutschland sicher im Netz (DsiN)
DIHK
Domo
DSGVO-Portal
Fastly
Forbes Advisor
Gabler Wirtschaftslexikon
Gartner
G DATA CyberDefense AG
Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GdV)
HLB
HPI
Hiscox
IBM
ISACA
Lünendonk
McKinsey
Microsoft
Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK)
Postbank
Proofpoint
PwC
Sapio Research
Shodan.io
Statcounter
Statista
teleResearch
TÜV Verband
vbw
ZDF

IMPRESSUM

Herausgeber: G DATA CyberDefense AG • G DATA Campus • Königsallee 178 a, 44799 Bochum, vertreten durch die Vorstände Kai Figge, Frank Heisler, Andreas Lüning
G DATA-Projektteam: Verantwortlich: Vera Haake & Dr. Daniela Kalkühler
Kathrin Beckert-Plewka, Marita Bierhoff, Stefan Karpenstein, Joy Linders, Julia Schürmann
Konzept: brand eins Medien AG / Redaktion Corporate Publishing, statista.com
Chefredaktion: Susanne Risch
Artdirektion: Britta Max, Deborah Tyllack
Infografik: Deborah Tyllack
Chefin vom Dienst: Michaela Streimelweger
Redaktion: Renate Hensel (freie Mitarbeit), Dorit Kowitz (fM), Kathrin Lilienthal (fM), Margitta Schulze Lohoff, Daniel Ramm (fM)
Autoren (fM): Daniel Erk, Christoph Koch, Peter Lau, Stefan Scheytt
Marktforschung, Recherche, Daten und Quellen:
Cindy Karwowski, Robin Rehfeldt, Tobias Steddin, Daniel Tippel, Katrin Von Soosten

brand eins

G DATA CyberDefense

statista