2023/2024

CYBERSICHERHEIT IN ZAHLEN

Lernen. Wissen. Handeln.

Liebe Leserinnen und Leser,

in der digitalen Welt gewinnt ein Thema immer mehr an Bedeutung: Verantwortung. Wir alle tragen eine gemeinsame Verantwortung – gegenüber unseren Mitarbeiterinnen und Mitarbeitern, unseren Kundinnen und Kunden, der Gesellschaft und der Umwelt. Dabei unterliegt unternehmerisches Handeln immer auch einem Wandel und muss sich neuen Herausforderungen stellen. Etwa bei der Frage, wie es gelingen kann, dass sich in Zukunft niemand mehr von Cybercrime oder digitalen Bedrohungen ablenken lassen muss.

Was aber, wenn Verantwortliche ihrer Verantwortung nicht gerecht werden? Wenn sie beispielsweise die unternehmenseigene IT unzureichend vor Cyberattacken absichern und wider besseres Wissen um die aktuelle Bedrohungslage handeln. Dann ist es hilfreich, wenn die Politik Mindeststandards schafft. Dies geschieht aktuell mit der neuen europäischen NIS2-Direktive (Network and Information Security). Sie wird derzeit in nationales Recht umgesetzt und hat das Ziel, das Sicherheitslevel sowie den Umgang mit IT-Notfällen und Bedrohungen in den Ländern der EU zu vereinheitlichen. Der Handlungsdruck wird größer, aber am Ende steht in vielen Unternehmen auch ein höheres Maß an Sicherheit.

Zur Wahrheit gehört aber auch, dass IT-Sicherheit ein komplexes Themenfeld ist und es vielen Unternehmen an personellen, zeitlichen und finanziellen Ressourcen mangelt. Sie sind gut beraten, Verantwortung abzugeben und Fachleute mit ausgewiesener Expertise ins Boot zu holen. Ein entscheidender Vorteil: Sie wissen, mit welchen Hebeln sich IT-Sicherheit verbessern lässt – oft auch ohne zusätzliches Budget.

Bereits zum dritten Mal haben wir gemeinsam mit brand eins und Statista für dieses Magazin zentrale Daten zu allen Aspekten der Sicherheit in der virtuellen Welt zusammengetragen. Und wie in den Vorjahren steht am Anfang unseres Heftes unsere exklusive Umfrage. Sie widmet sich natürlich auch der Verantwortung und Verankerung von Cybersicherheit im Unternehmen. Aber auch Einschätzungen zu den Themen Weiterbildung und Fehlerkultur oder zu Cloud-Diensten finden sich auf den ersten Seiten dieses Magazins.

Neben dem umfangreichen Zahlenwerk gibt es außerdem wieder spannende Geschichten zu wichtigen und aktuellen Themen wie künstlicher Intelligenz, Quantencomputern und Nachhaltigkeit.

Ich lade Sie herzlich zu einer spannenden Lektüre ein.

Mit herzlichem Gruß

Ihr Andreas Lüning
Vorstand und Mitgründer G DATA CyberDefense AG

Was kommt, was bleibt

Keine Frage, die NIS2-Richtlinie, die in der Europäischen Union ein hohes Cybersicherheitsniveau garantieren soll, ist ein Meilenstein. Die darin definierten Maßnahmen bürden den Herstellern mehr Verantwortung auf, indem sie diese bei festgestellten Schwachstellen zur Bereitstellung von Sicherheitsunterstützung und Software-Aktualisierungen verpflichten. Den Verbrauchern wiederum bieten sie deutlich mehr Informationen über die Cybersicherheit der Produkte, die sie kaufen und nutzen.

Beides wird helfen, aber machen wir uns nichts vor: Sicherheit lässt sich nicht verordnen und nicht delegieren. Sicherheit ist ein immerwährender Prozess, der neben klugen Systemen, klaren Strukturen, definierten Prozessen und kompetenten Experten die Wachsamkeit und Umsicht jeder und jedes Einzelnen erfordert.

Cybersicherheit ist schließlich auch in der Vergangenheit nicht an zu wenig Informationen gescheitert. Was gemeinhin fehlt, ist das Gefühl für die Gefahren in der digitalen Welt – und die Bereitschaft, sich mit der Materie auseinanderzusetzen.

Wir haben deshalb auch für dieses Heft nach Gesprächspartnern gesucht, die in ihrem Fachgebiet führend sind, sorgsam abwägen und die Chancen und Risiken der aktuellen technologischen Entwicklungen für uns einordnen können.

Womit müssen wir beispielsweise bei Quantencomputern rechnen, die uns vielleicht schon sehr bald die Simulation komplexer Systeme ermöglichen, aber auch ganz neue Sicherheitsprobleme bescheren werden (*Seite 28*)? Wohin führt unser Hunger nach immer neuen, effizienteren IT-Systemen? Werden Sicherheit und Nachhaltigkeit irgendwann zusammengehen (*Seite 54*)? Und wie wird das werden mit künstlichen Intelligenzen? Sie werden unsere gesellschaftlichen Grundlagen verändern, die Art, wie wir leben, lernen und arbeiten. Sie werden uns in vielen Bereichen enorm voranbringen, aber bei allen erfreulichen Perspektiven sind künstliche Intelligenzen eben auch Technologien mit Schwächen, die für kriminelle Zwecke eingesetzt werden können (*Seite 78*).

Gesetze und Richtlinien werden nichts daran ändern: Die neuen Technologien sorgen für eine Vielzahl positiver Entwicklungen und Chancen – aber sie entlassen uns nicht aus der Pflicht. Cybersicherheit bleibt Aufgabe von uns allen. Die Verantwortung jeder und jedes Einzelnen.

Susanne Risch
Chefredakteurin

Inhalt

So weit alles gut?

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 2023 Auskunft – über ihr Wissen, ihre Einschätzungen und Erfahrungen im Umgang mit IT. Die repräsentative Umfrage zeigt das aktuelle Stimmungsbild.

Je mehr Wissen, desto mehr Risikobewusstsein

Bereiche für Bewusstsein schaffen bei Mitarbeiterinnen und Mitarbeitern; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2023; in Prozent *

In welchen Bereichen sollte Ihr Unternehmen für Mitarbeiterinnen und Mitarbeiter mehr Bewusstsein schaffen?

insgesamt

Phishing / Datendiebstahl

Umgang mit Passwörtern

DSGVO / Datenschutz

Malware / Ransomware

mobiles bzw. remote Arbeiten

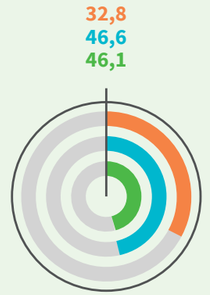
Social Engineering

in keinem der genannten Bereiche

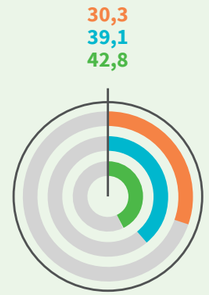
* Mehrfachnennungen möglich (max. 3 Antworten). Quelle: Statista im Auftrag von G DATA

Antworten nach persönlicher Kompetenz im Bereich IT-Sicherheit

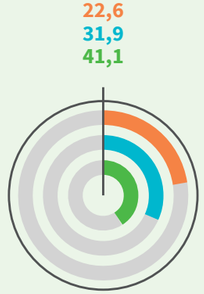
(sehr) geringe Kompetenz · mittlere Kompetenz · (sehr) große Kompetenz



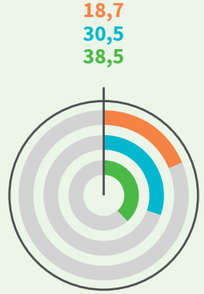
Phishing / Datendiebstahl



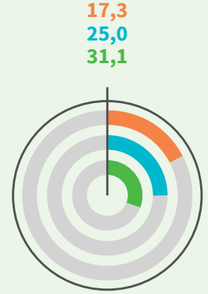
Umgang mit Passwörtern



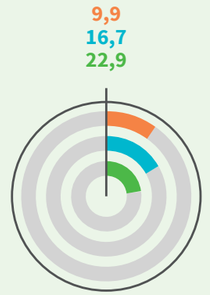
DSGVO / Datenschutz



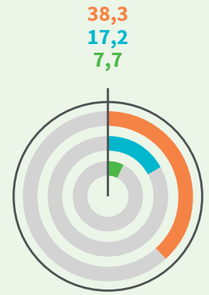
Malware / Ransomware



mobiles bzw. remote Arbeiten



Social Engineering



in keinem der genannten Bereiche

Glossar der Cyberbegriffe auf Seite 100 – 103

Da geht noch was

Einschätzung der persönlichen Kompetenz zum Thema IT-Sicherheit; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2023; in Prozent

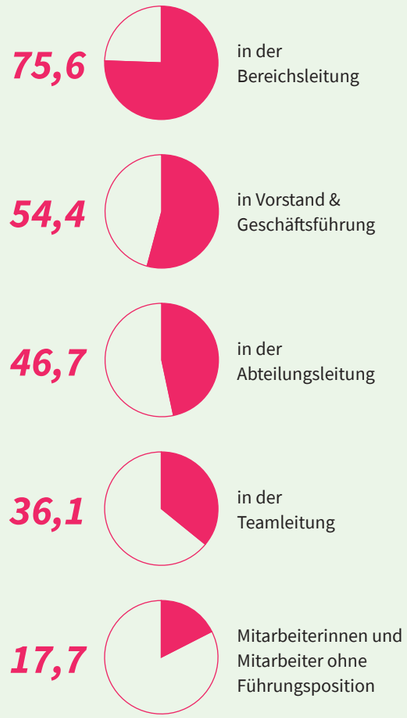
Wie schätzen Sie Ihre persönliche Kompetenz beim Thema IT-Sicherheit ein?

insgesamt

nach Abteilungen

nach Positionen

Anteil der Mitarbeiterinnen und Mitarbeiter, die ihre persönliche Kompetenz als (sehr) groß einschätzen



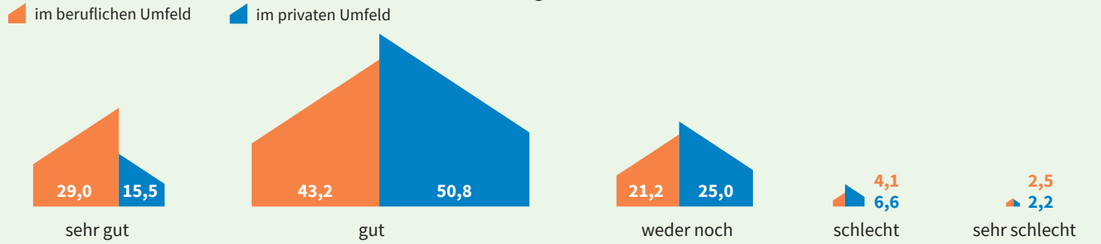
Quelle: Statista im Auftrag von G DATA

Da kommt noch was

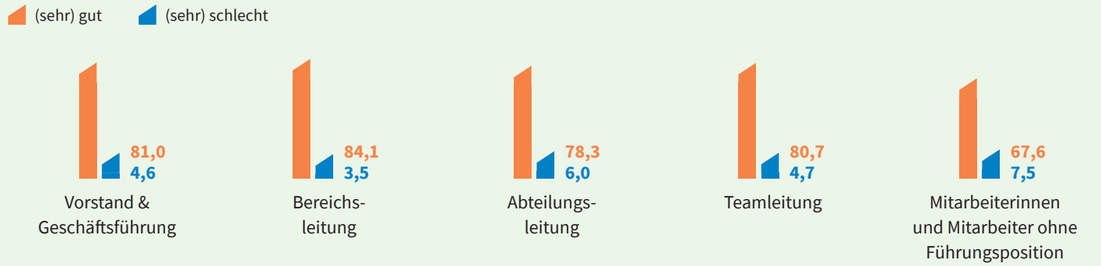
Schutzgefühl durch IT-Sicherheitsmaßnahmen im beruflichen und privaten Umfeld; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2023; in Prozent

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

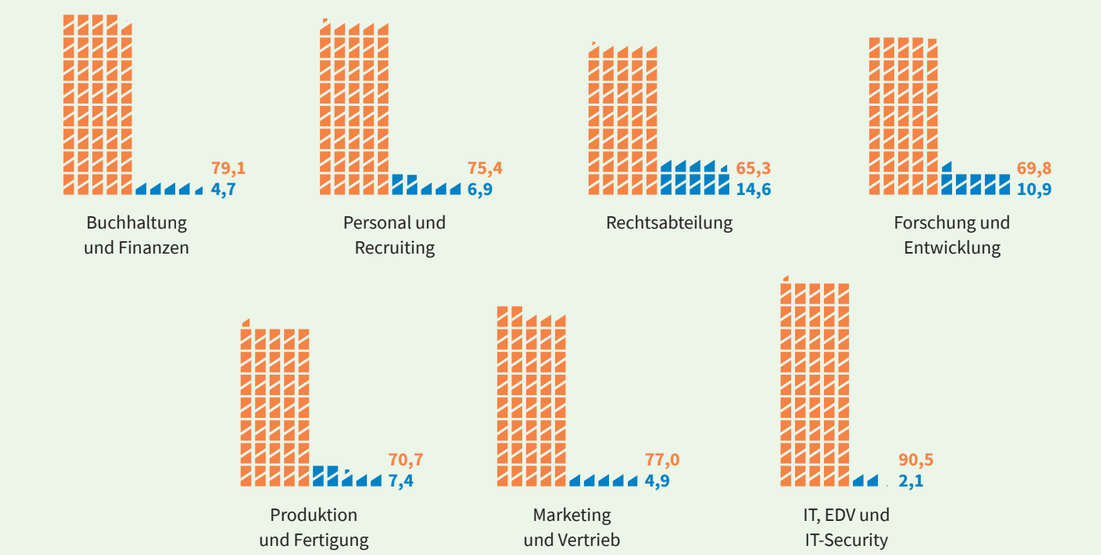
insgesamt



nach Positionen, im beruflichen Umfeld



nach Abteilungen, im beruflichen Umfeld



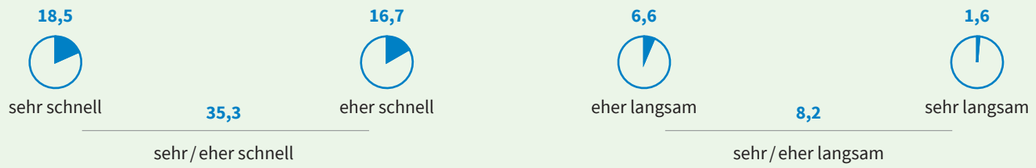
Quelle: Statista im Auftrag von G DATA

Gefahr erkannt, Gefahr verkannt

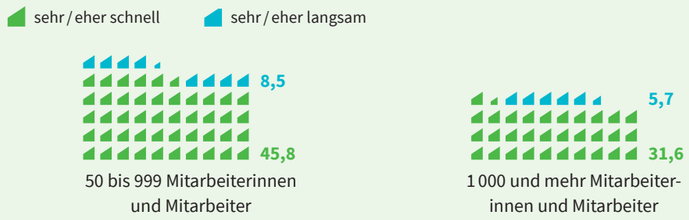
Eine IT-Sicherheitslücke erkennen und darauf hinweisen – oder nicht; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2023; in Prozent

Haben Sie in Ihrem Unternehmen schon einmal eine IT-Sicherheitslücke erkannt und darauf hingewiesen? Wenn ja, wie schnell hat Ihr Unternehmen darauf reagiert?

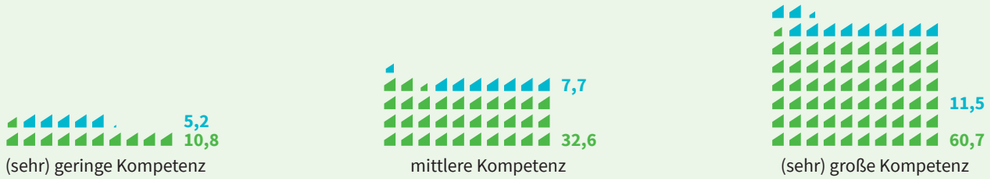
insgesamt



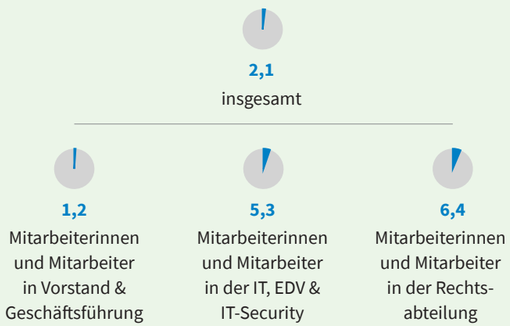
nach Unternehmensgröße



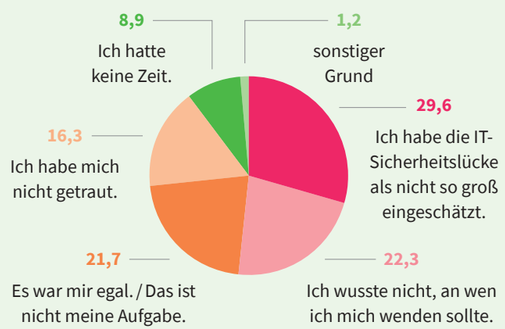
nach persönlicher Kompetenz im Bereich IT-Sicherheit



Ich habe schon mal eine IT-Sicherheitslücke erkannt, aber nicht darauf hingewiesen.



Warum haben Sie nicht auf die IT-Sicherheitslücke hingewiesen?



Quelle: Statista im Auftrag von G DATA

Gefahr erkannt, Gefahr gebannt

Hinweise auf eine IT-Sicherheitslücke; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die in ihrem Unternehmen eine IT-Sicherheitslücke erkannt und darauf hingewiesen haben; 2023; in Prozent

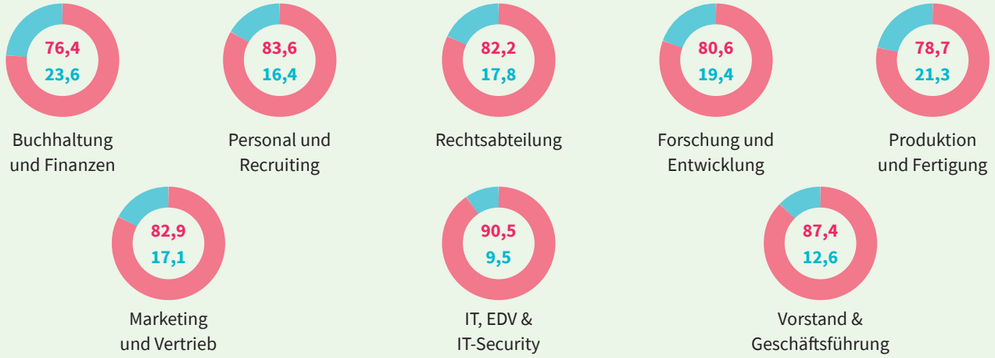
Wie schnell hat Ihr Unternehmen auf Ihren Hinweis auf eine IT-Sicherheitslücke reagiert?

sehr / eher schnell — sehr / eher langsam

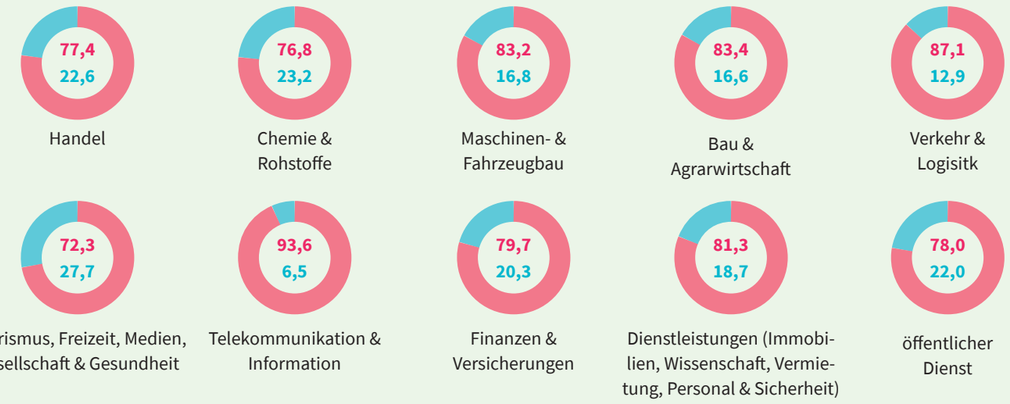
insgesamt

nach Unternehmensgröße

nach Abteilungen



nach Branchen

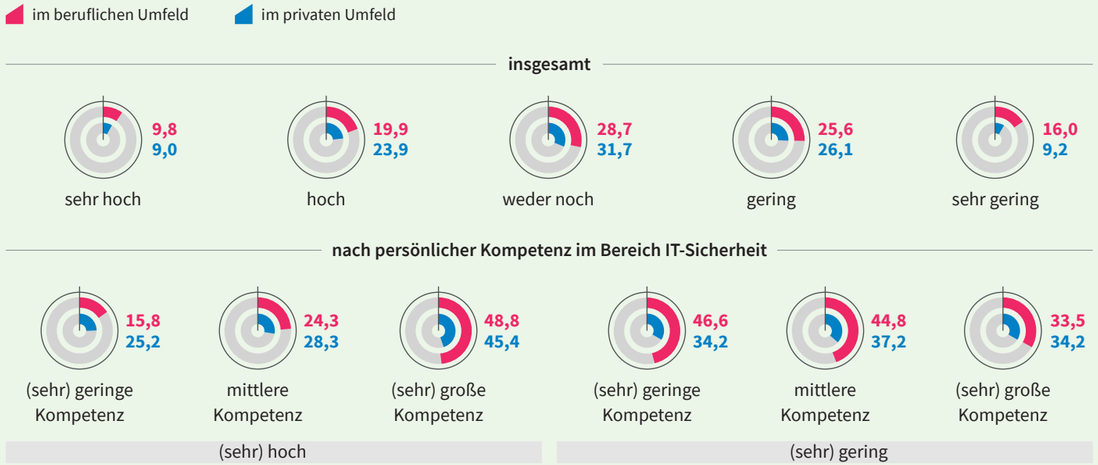


Quelle: Statista im Auftrag von G DATA

Der Schein trügt

Risikoeinschätzung zum Thema Cyberkriminalität im privaten und beruflichen Umfeld; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2023; in Prozent

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

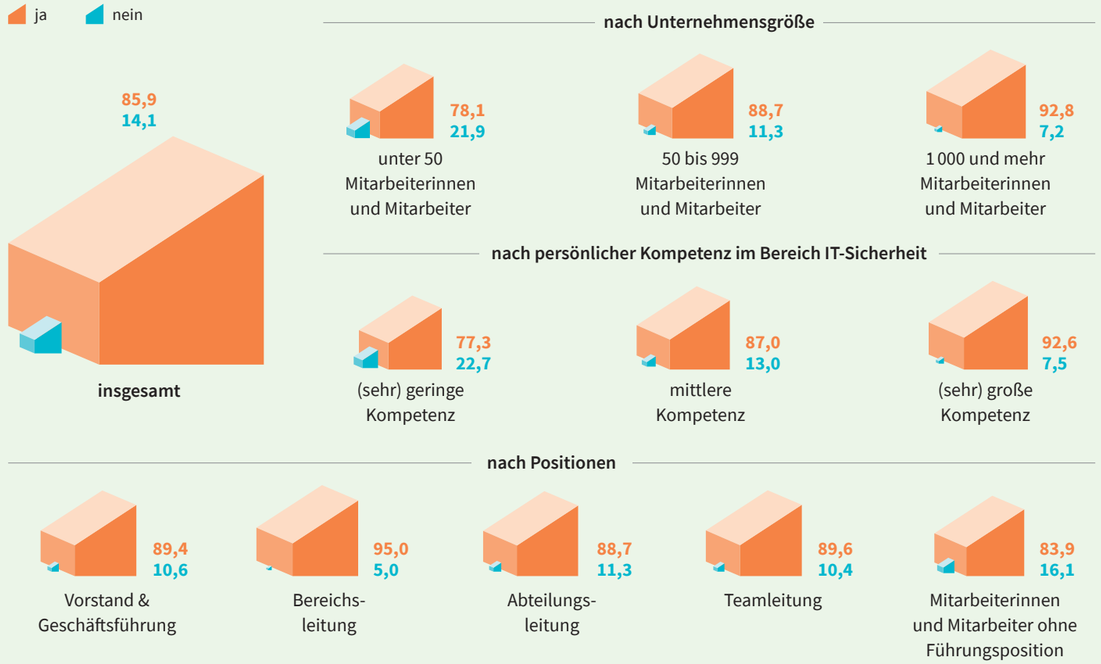


Quelle: Statista im Auftrag von G DATA

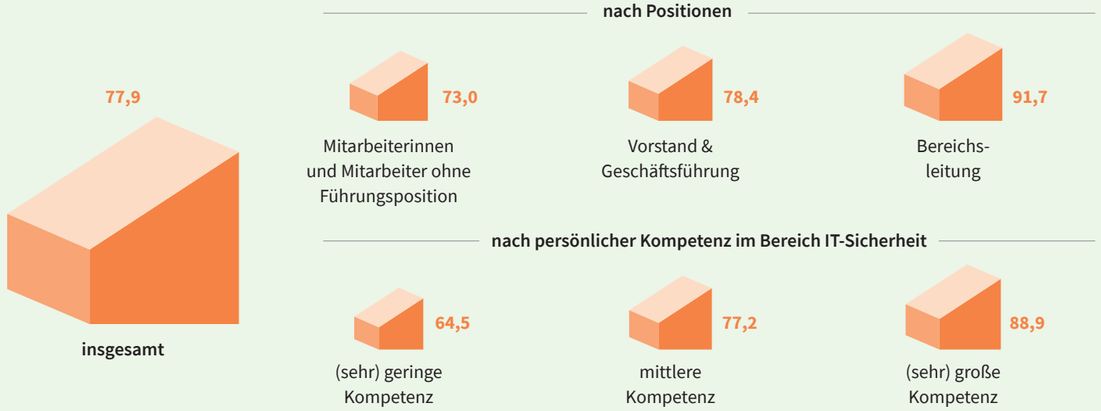
Das Bewusstsein wächst

Einschätzung, ob Cybersicherheit im Unternehmen ernst genommen wird; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2023; in Prozent

Haben Sie das Gefühl, dass das Thema Cybersicherheit in Ihrem Unternehmen ernst genommen wird?



Sie haben angegeben, dass das Thema Cybersicherheit in Ihrem Unternehmen ernst genommen wird. Hat das in den vergangenen Jahren zugenommen? (Zustimmung in Prozent)



Quelle: Statista im Auftrag von G DATA

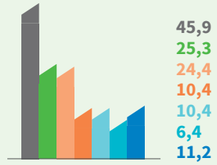
Verantwortlich?

Verantwortliche Instanz für IT-Sicherheit im Unternehmen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2023; in Prozent *

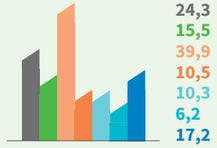
Wer ist in Ihrem Unternehmen für IT-Sicherheit verantwortlich?

IT-Abteilung · IT-Security-Team (unternehmensintern) · Geschäftsführung / Vorstand · IT-Systemhaus / IT-Dienstleister (extern) · IT-Security Beratung (extern) · Hersteller von IT-Security-Lösungen bzw. -Services (extern) · sonstige Instanz

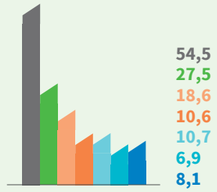
nach Unternehmensgröße



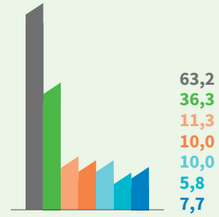
insgesamt: 45,9 · 25,3 · 24,4 · 10,4 · 10,4 · 6,4 · 11,2



unter 50 Mitarbeiterinnen und Mitarbeiter: 24,3 · 15,5 · 39,9 · 10,5 · 10,3 · 6,2 · 17,2

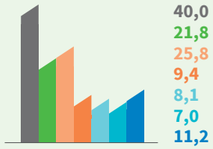


50 bis 999 Mitarbeiterinnen und Mitarbeiter: 54,5 · 27,5 · 18,6 · 10,6 · 10,7 · 6,9 · 8,1

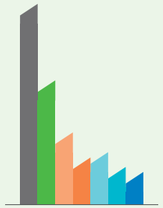


1 000 und mehr Mitarbeiterinnen und Mitarbeiter: 63,2 · 36,3 · 11,3 · 10,0 · 10,0 · 5,8 · 7,7

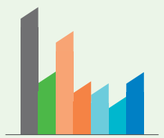
nach Branchen



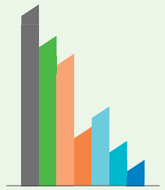
Handel: 40,0 · 21,8 · 25,8 · 9,4 · 8,1 · 7,0 · 11,2



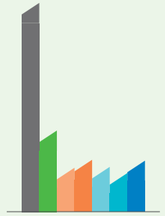
Maschinen- & Fahrzeugbau: 61,2 · 35,3 · 17,7 · 9,2 · 11,0 · 6,0 · 4,3



Bau & Agrarwirtschaft: 36,4 · 14,6 · 28,3 · 11,3 · 10,6 · 6,1 · 14,4



Telekommunikation & Information: 54,6 · 44,0 · 37,9 · 13,2 · 20,1 · 8,4 · 2,3



öffentlicher Dienst: 63,9 · 20,7 · 8,1 · 10,8 · 8,4 · 6,3 · 10,5

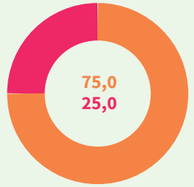
* Mehrfachnennungen möglich. Quelle: Statista im Auftrag von G DATA

Leichtsinnig?

Sinn einer Cyberversicherung * für Unternehmen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2023; in Prozent

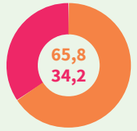
Für wie sinnvoll erachten Sie eine Cyberversicherung für Ihr Unternehmen?

sehr / eher sinnvoll · wenig / überhaupt nicht sinnvoll

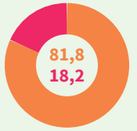


insgesamt: 75,0 · 25,0

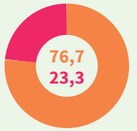
nach Positionen



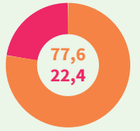
Vorstand & Geschäftsführung: 65,8 · 34,2



Bereichsleitung: 81,8 · 18,2



Abteilungsleitung: 76,7 · 23,3

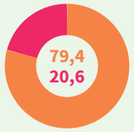


Teamleitung: 77,6 · 22,4

Mitarbeiterinnen und Mitarbeiter ohne Führungsposition: 75,3 · 24,7

nach Abteilungen

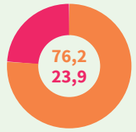
Buchhaltung und Finanzen: 77,1 · 23,0



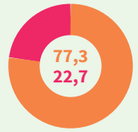
Personal und Recruiting: 79,4 · 20,6

Rechts-abteilung: 71,1 · 29,0

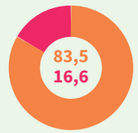
Forschung und Entwicklung: 68,3 · 31,7



Produktion und Fertigung: 76,2 · 23,9

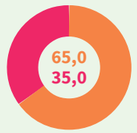


Marketing und Vertrieb: 77,3 · 22,7

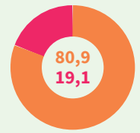


IT, EDV & IT-Security: 83,5 · 16,6

nach Unternehmensgröße



unter 50 Mitarbeiterinnen und Mitarbeiter: 65,0 · 35,0



50 bis 999 Mitarbeiterinnen und Mitarbeiter: 80,9 · 19,1

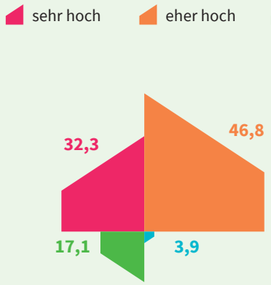
1 000 und mehr Mitarbeiterinnen und Mitarbeiter: 79,8 · 20,2

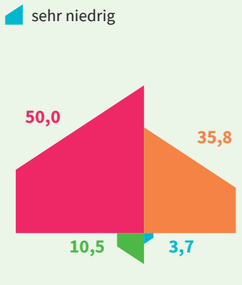
* Eine Versicherung für Unternehmen, die Schäden durch Cyberkriminalität (z. B. Hackerangriffe) absichert. Quelle: Statista im Auftrag von G DATA

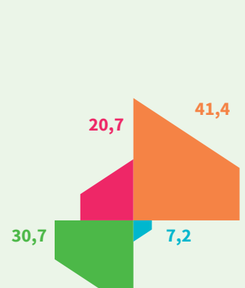
Kein Thema für Mitarbeiterinnen und Mitarbeiter

Verantwortungsbewusstsein für IT-Sicherheit; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2023; in Prozent

Wie bewerten Sie für folgende Gruppen in Ihrem Unternehmen das Verantwortungsbewusstsein für IT-Sicherheit?

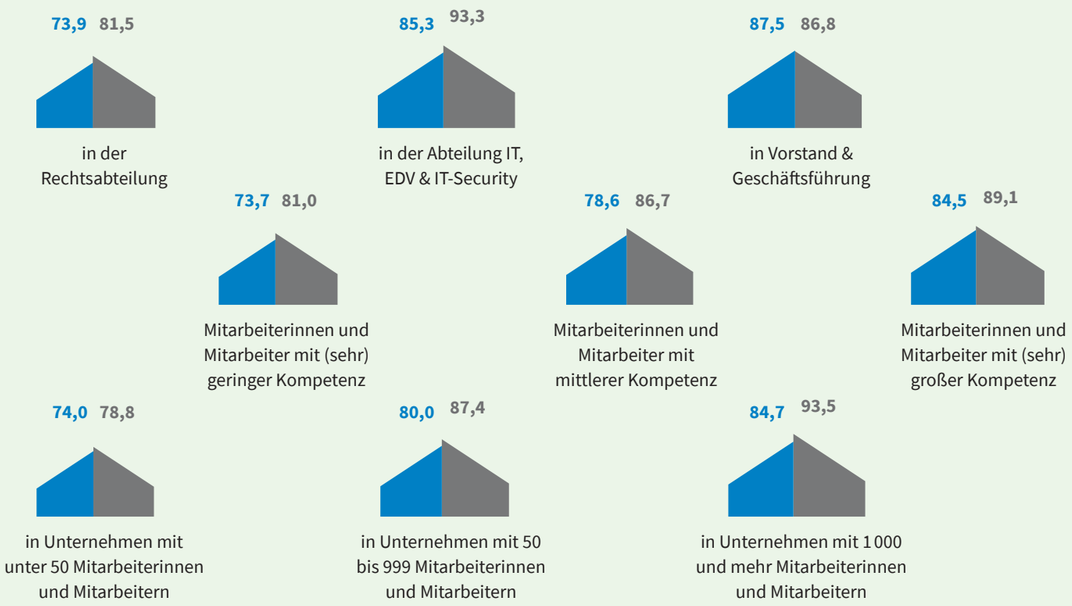






Anteil der Befragten, die das Verantwortungsbewusstsein von Geschäftsführung / Vorstand sehr / eher hoch bewerten …

Anteil der Befragten, die das Verantwortungsbewusstsein in der IT-Abteilung sehr / eher hoch bewerten …

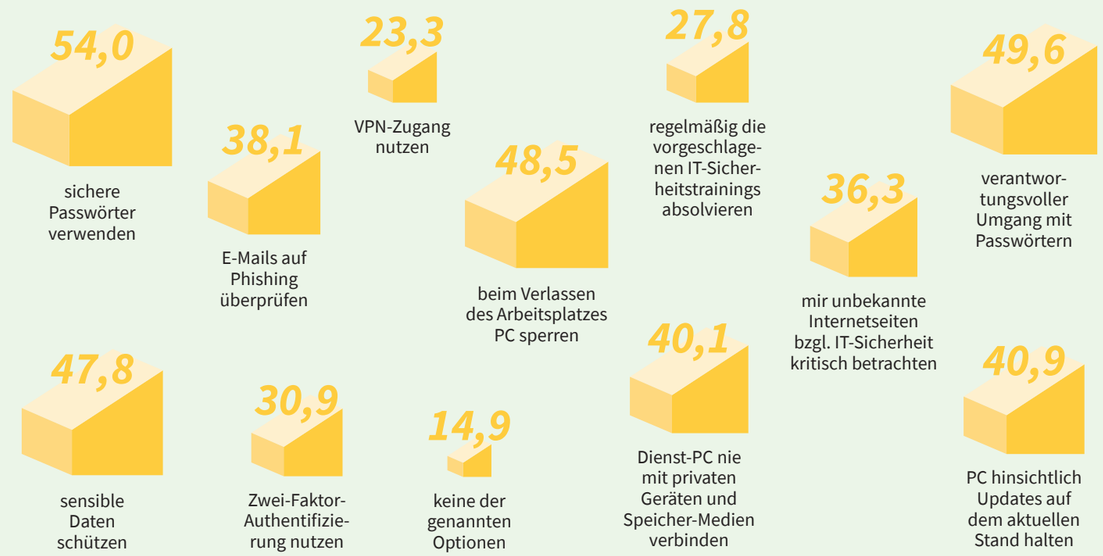


Quelle: Statista im Auftrag von G DATA

Ein Thema für Mitarbeiterinnen und Mitarbeiter

Zuständigkeit am Arbeitsplatz; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2023; in Prozent *

Wofür fühlen Sie sich an Ihrem Arbeitsplatz zuständig?



Anteil der Befragten, die sich für keine der genannten Optionen zuständig fühlen …

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

Der Faktor Mensch I

Möglichkeit und Häufigkeit der Durchführung von Sicherheitsmaßnahmen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2023; in Prozent

Wie häufig haben Sie in den vergangenen zwei Monaten im beruflichen Umfeld die nachfolgenden Sicherheitsmaßnahmen durchgeführt? („trifft nicht zu“ = wenn eine Sicherheitsmaßnahme grundsätzlich nicht umgesetzt werden kann)

Quelle: Statista im Auftrag von G DATA

Der Faktor Mensch II

Häufigkeit der Durchführung von Sicherheitsmaßnahmen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2023; in Prozent

Wie häufig haben Sie in den vergangenen zwei Monaten im beruflichen Umfeld die nachfolgenden Sicherheitsmaßnahmen durchgeführt? (nur Arbeitnehmerinnen und Arbeitnehmer, die die Sicherheitsmaßnahme grundsätzlich umsetzen können)

Quelle: Statista im Auftrag von G DATA

Das sollte es uns wert sein

Investitionen in Unternehmensbereiche; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2023; in Prozent *

In welche Bereiche Ihres Unternehmens sollte Ihrer Meinung nach mehr investiert werden?

insgesamt

- 36,1 — IT-Sicherheit
- 33,1 — Mitarbeiterentwicklung / HR
- 28,4 — Nachhaltigkeit
- 27,4 — IT-Tools / Software
- 24,4 — Büroausstattung
- 18,1 — Forschung / (Produkt-) Entwicklung
- 13,8 — Marketing
- 18,6 — In keinen der genannten Bereiche

Investitionen in IT-Sicherheit nach Branche

- 46,6 — Maschinen- & Fahrzeugbau
- 45,9 — Telekommunikation & Information
- 42,8 — Finanzen & Versicherungen
- 42,2 — Energie & Umwelt
- 38,9 — Chemie & Rohstoffe
- 35,7 — Dienstleistungen (Immobilien, Wissenschaft, Vermietung, Personal & Sicherheit)
- 35,3 — Verkehr & Logistik
- 34,8 — Bau & Agrarwirtschaft
- 34,3 — öffentlicher Dienst
- 33,4 — Handel
- 32,9 — Tourismus, Freizeit, Medien, Gesellschaft & Gesundheit

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

Das sollte uns zu denken geben

Schulungsangebote zum Thema Cybersicherheit; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2023; in Prozent

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

ja | nein

insgesamt

53,9 | 46,1

nach Positionen

- 64,6 | 35,4 — Vorstand & Geschäftsführung
- 83,7 | 16,3 — Bereichsleitung
- 65,4 | 34,6 — Abteilungsleitung
- 64,0 | 36,0 — Teamleitung
- 43,5 | 56,5 — Mitarbeiterinnen und Mitarbeiter ohne Führungsposition

nach Unternehmensgröße

- 37,8 | 62,2 — unter 50 Mitarbeiterinnen und Mitarbeiter
- 61,4 | 38,6 — 50 bis 999 Mitarbeiterinnen und Mitarbeiter
- 65,0 | 35,0 — 1 000 und mehr Mitarbeiterinnen und Mitarbeiter

nach persönlicher Kompetenz im Bereich IT-Sicherheit

- 27,7 | 72,4 — (sehr) geringe Kompetenz
- 54,4 | 45,7 — mittlere Kompetenz
- 77,3 | 22,7 — (sehr) große Kompetenz

nach Abteilungen

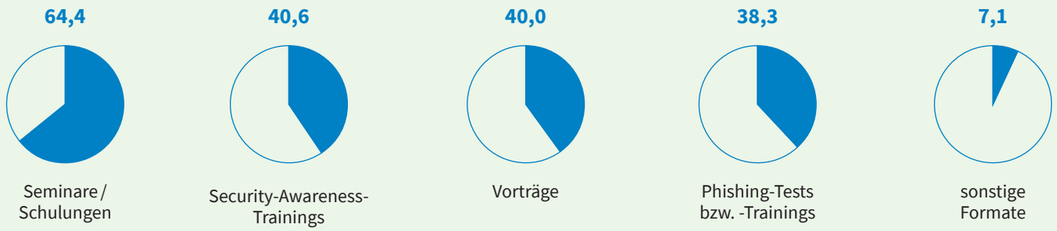
- 63,1 | 36,9 — Buchhaltung und Finanzen
- 63,0 | 37,0 — Personal und Recruiting
- 56,1 | 43,9 — Rechtsabteilung
- 60,1 | 39,9 — Forschung und Entwicklung
- 48,9 | 51,1 — Produktion und Fertigung
- 61,8 | 38,2 — Marketing und Vertrieb
- 82,9 | 17,1 — IT, EDV & IT-Security

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

Seminare und Schulungen

Angebotene Formate für (Online-)Schulungen zum Thema Cybersicherheit; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, deren Unternehmen (Online-)Schulungen / Veranstaltungen / Trainings rund um Cybersicherheit für alle Mitarbeiterinnen und Mitarbeiter anbietet; 2023; in Prozent *

Welche Formate sind Ihnen in Ihrem Unternehmen rund um das Thema Cybersicherheit bekannt?

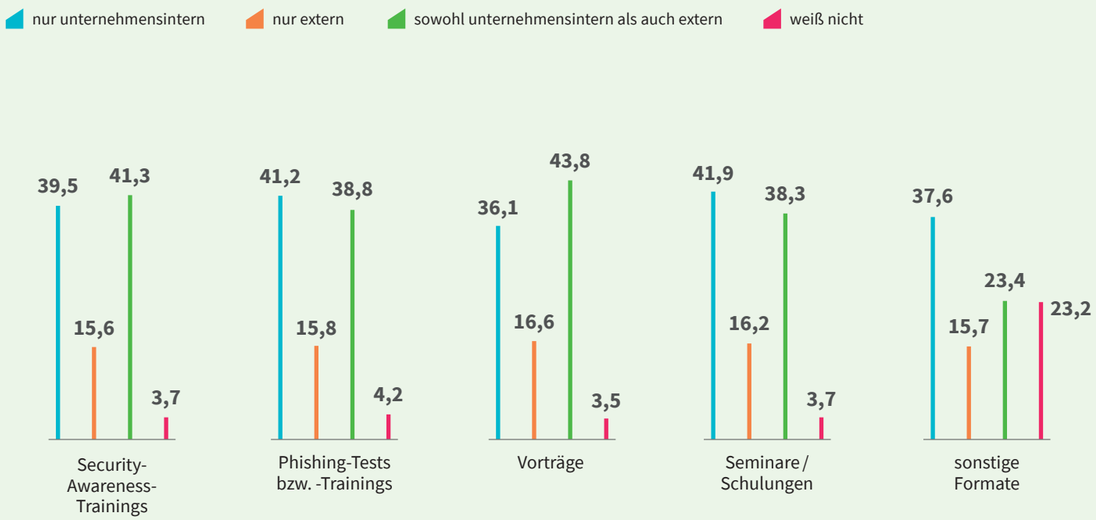


* Mehrfachnennungen möglich. Quelle: Statista im Auftrag von G DATA

Intern und extern

Angebot an internen bzw. externen (Online-)Schulungen zum Thema Cybersicherheit; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, deren Unternehmen (Online-)Schulungen / Veranstaltungen / Trainings rund um Cybersicherheit für alle Mitarbeiterinnen und Mitarbeiter anbietet; 2023; in Prozent

Werden die Formate unternehmensintern oder extern angeboten?

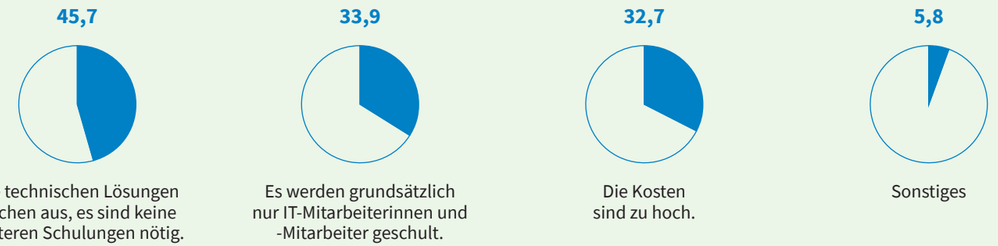


Quelle: Statista im Auftrag von G DATA

Irrtümer und Ungereimtheiten

Gründe, warum nicht für alle Mitarbeiterinnen und Mitarbeiter (Online-)Schulungen angeboten werden; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die im Bereich IT / EDV, IT-Security, Vorstand / Gesellschafterinnen und Gesellschafter / Geschäftsführung / Geschäftsleitung oder Personal und Recruiting arbeiten, und deren Unternehmen nicht für alle Mitarbeiterinnen und Mitarbeiter Schulungen anbietet; 2023; in Prozent *

Warum werden nicht für alle Mitarbeiterinnen und Mitarbeiter (Online-)Schulungen / Veranstaltungen / Trainings angeboten?

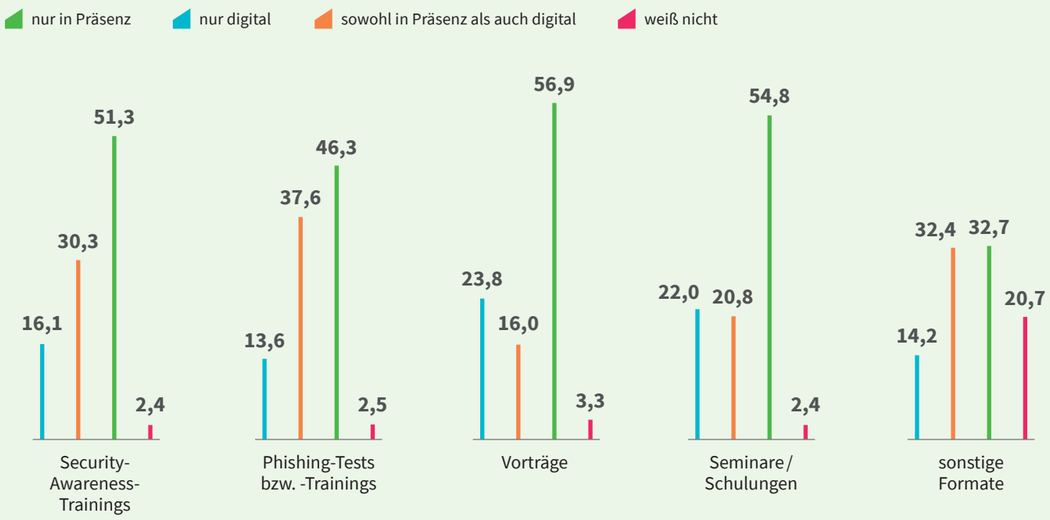


* Mehrfachnennungen möglich. Quelle: Statista im Auftrag von G DATA

Online und offline

Angebot an Präsenz- und digitalen (Online-)Schulungen zum Thema Cybersicherheit; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, deren Unternehmen (Online-)Schulungen / Veranstaltungen / Trainings rund um Cybersicherheit für alle Mitarbeiterinnen und Mitarbeiter anbietet; 2023; in Prozent

Werden die Formate in Präsenz oder digital angeboten?

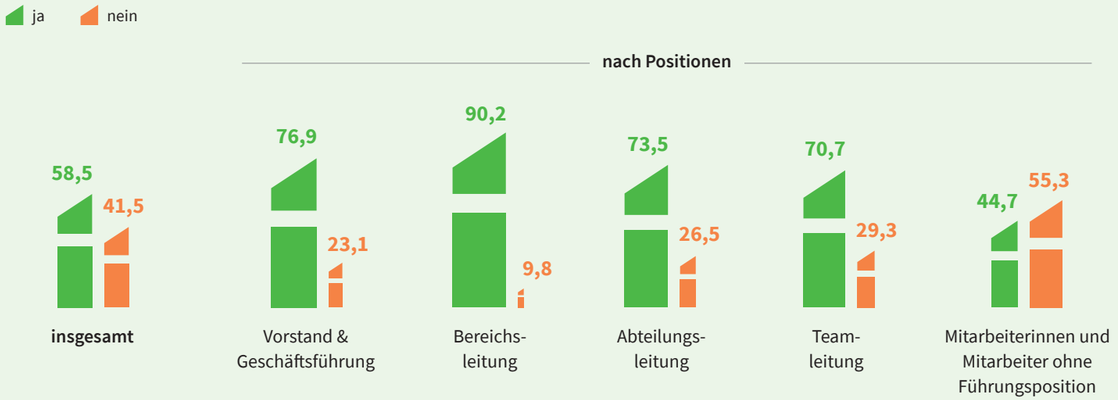


Quelle: Statista im Auftrag von G DATA

Eher hierarchisch

Regelmäßiges Informieren rund um Cybersicherheit; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2023; in Prozent

Informieren Sie sich regelmäßig über das Thema Cybersicherheit?



Quelle: Statista im Auftrag von G DATA

Eher individuell

Informationsquellen für das Thema Cybersicherheit; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die sich regelmäßig über das Thema Cybersicherheit informieren; 2023; in Prozent *

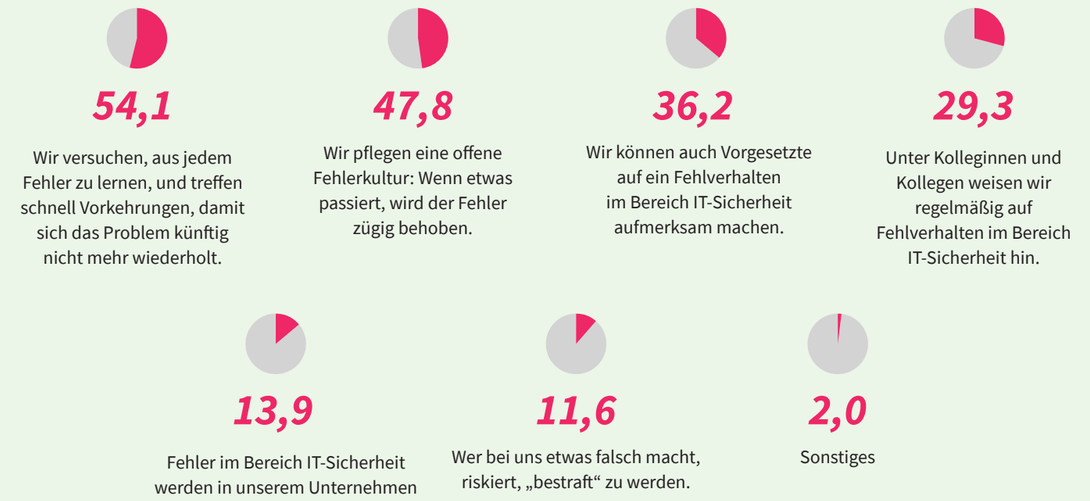
Wie informieren Sie sich über das Thema Cybersicherheit?

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

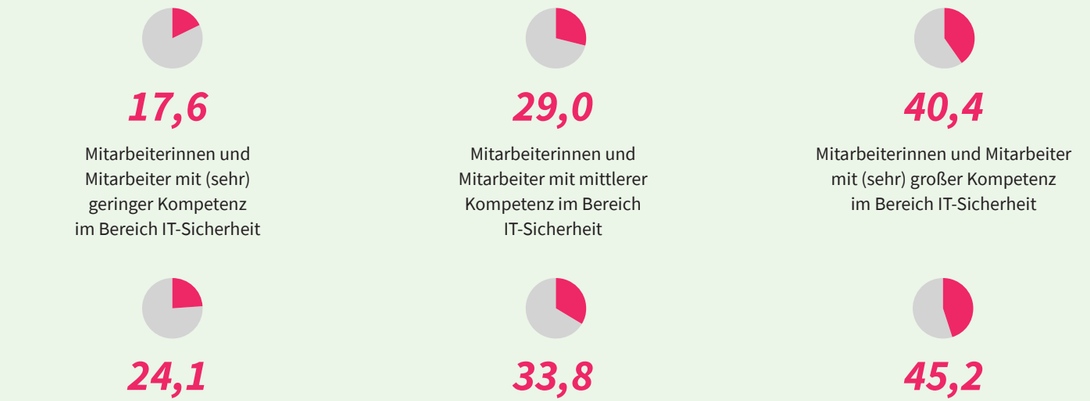
Eher vorsichtig

Umgang mit Fehlern im Unternehmen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2023; in Prozent *

Wie würden Sie den Umgang mit Fehlern in Ihrem Unternehmen beschreiben?



Unter Kolleginnen und Kollegen weisen wir regelmäßig auf Fehlverhalten im Bereich IT-Sicherheit hin:



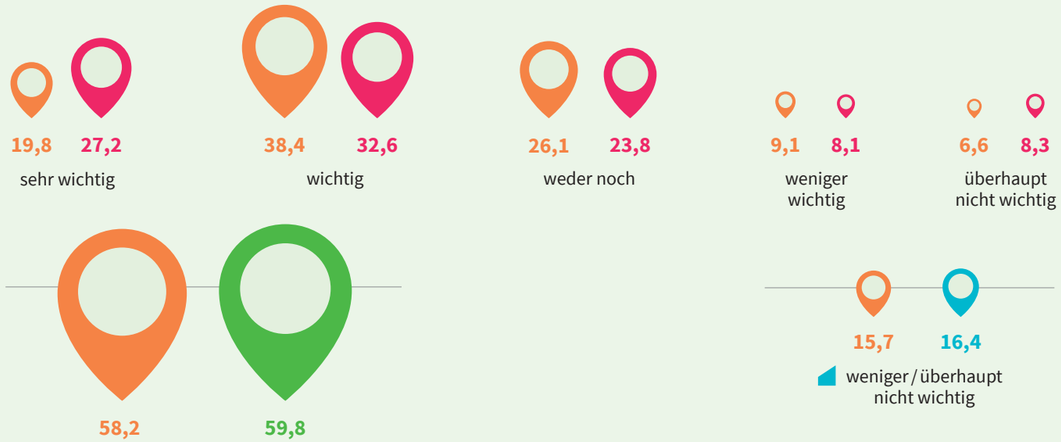
* Mehrfachnennungen möglich. Quelle: Statista im Auftrag von G DATA

Eine Frage des Standortes

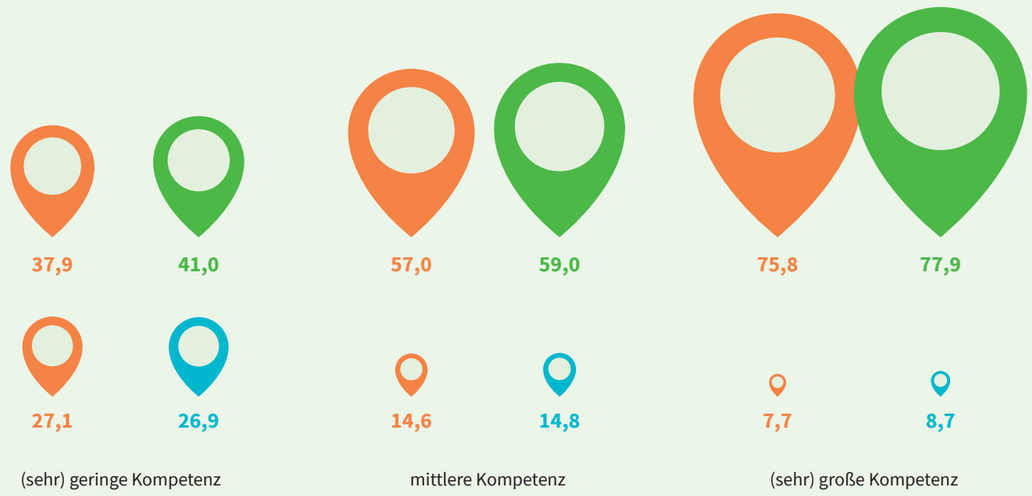
Relevanz des Standortes von IT-Sicherheitsanbietern; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2023; in Prozent

Wie wichtig ist es Ihnen, wo eine Anbieterin oder ein Anbieter von IT-Sicherheitslösungen seinen Standort hat?

Vergleichswerte aus dem Vorjahr (2022)



nach persönlicher Kompetenz im Bereich IT-Sicherheit

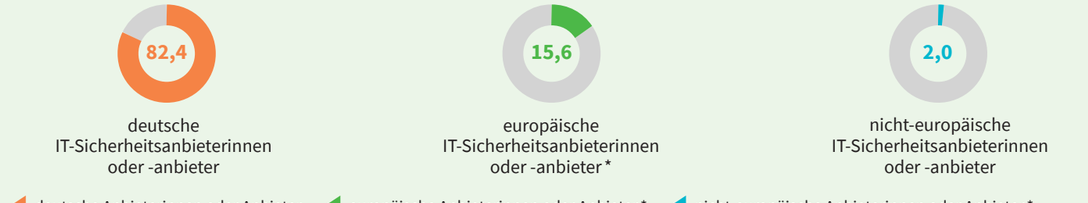


Quelle: Statista im Auftrag von G DATA

Eine Frage der Herkunft

Bevorzugter Standort für IT-Sicherheitsanbieter; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, denen der Standort sehr wichtig oder wichtig ist; 2023; in Prozent

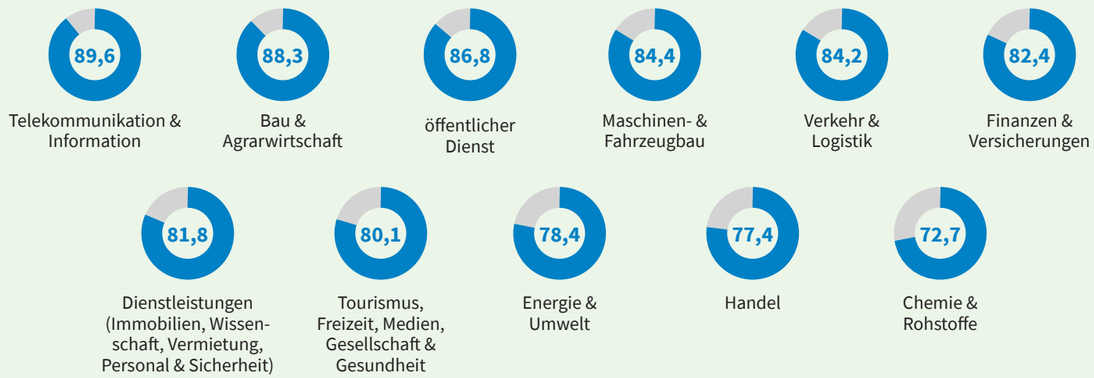
Welche IT-Sicherheitsanbieterinnen oder -Anbieter würden Sie bevorzugen?



nach Positionen

nach persönlicher Kompetenz im Bereich IT-Sicherheit

Bevorzugung deutscher IT-Sicherheitsanbieterinnen und -anbieter nach Branchen

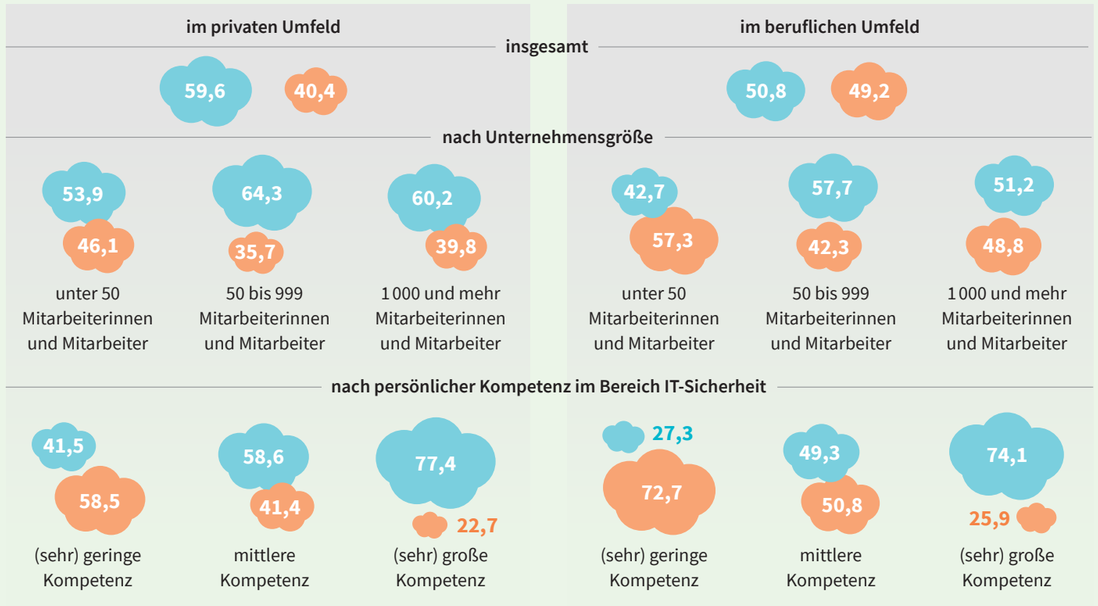


* ausgenommen Deutschland. Quelle: Statista im Auftrag von G DATA

Wolkig

Nutzung von Cloud-Diensten; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2023; in Prozent

Nutzen Sie Cloud-Dienste im privaten Umfeld oder in Ihrer Abteilung?

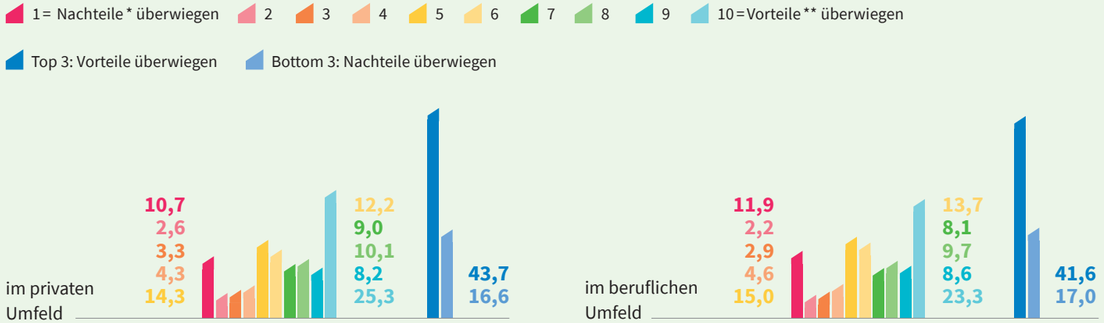


Quelle: Statista im Auftrag von G DATA

Eindeutig

Bewertung von Cloud-Diensten; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2023; in Prozent

Wie bewerten Sie Cloud-Dienste im Rahmen des privaten und beruflichen Umfelds?



* z. B. Datensicherheit, fehlende Individualisierungsmöglichkeiten. ** z. B. ortsunabhängiger Zugriff, verbesserte Zusammenarbeit. Quelle: Statista im Auftrag von G DATA

Mehrdeutig

Wichtige Entscheidungskriterien bei der Auswahl von Cloud-Anbieterinnen oder -Anbietern; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die im Bereich IT / EDV, IT-Security oder Vorstand / Gesellschafter / Geschäftsführung / Geschäftsleitung arbeiten und in deren Unternehmen Cloud-Dienste genutzt werden; 2023; in Prozent

Was sind in Ihrem Unternehmen wichtige Entscheidungskriterien bei der Auswahl von Cloud-Anbieterinnen oder -Anbietern?

Quelle: Statista im Auftrag von G DATA

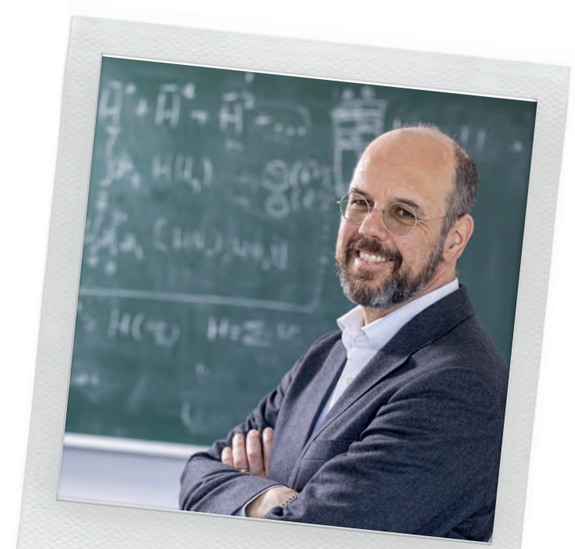
QUANTENCOMPUTER

Faszinierend, gefährlich, unberechenbar

Die Forschung zu Quantencomputern macht rasante Fortschritte. Was bedeutet das für die Cybersicherheit? Ein Gespräch mit dem Leiter des Instituts für Quantenkontrolle am Forschungszentrum Jülich: Tommaso Calarco ist einer der führenden Forscher auf diesem Gebiet.

Text: Christoph Koch

Blackbox: Was und wie Quantencomputer rechnen, können Forscherinnen und Forscher bislang nicht immer in einem verständlichen Maß auslesen. Vor diesem Dilemma stehen auch die Wissenschaftlerinnen und Wissenschaftler des Fraunhofer Instituts im baden-württembergischen Ehningen, die mit diesem Modell von IBM arbeiten.



Von Qubits und Labyrinthen

Der Quantenkontrolleur
Der gebürtige Italiener Tommaso Calarco ist als Physiker auf die Optimierung von Quantenprozessen spezialisiert. Der Professor für Theoretische Physik an der Universität Köln leitet das Quantum Community Network und ist Direktor des Instituts für Quantenkontrolle am Forschungszentrum Jülich.
Der 53-Jährige ist zudem Initiator einer europäischen Forschungsinitiative zu Quantentechnologien und Verfasser des europäischen „Quantum Manifest". Der Musik gilt seine zweite große Leidenschaft: Tommaso Carlarco hat einen Bachelor in Klassischer Gitarre.

Herr Professor Calarco, wenn Sie Ihren Eltern Ihre Arbeit erklären wollen: Wie beschreiben Sie ihnen, was ein Quantencomputer eigentlich ist und wie er funktioniert?

Tommaso Calarco: Ich würde damit anfangen, dass sie ja wahrscheinlich wissen, dass normale Computer aus Transistoren und Schaltkreisen bestehen, die mit Nullen und Einsen arbeiten. Also sogenannten Bits. Alle unsere digitalen Geräte, vom Smartphone bis zur Digitaluhr, arbeiten so. In der Quantentechnologie verwenden wir statt dieser Transistoren einzelne Teilchen. Also Atome – Ionen oder Photonen. Und damit ändert sich alles.

Warum?

Weil diese einzelnen Teilchen nicht nur die beiden Zustände eins und null kennen, sondern auch alle Möglichkeiten dazwischen. Sie können sogar zwei Zustände gleichzeitig haben. Das ist für uns Menschen schwer vorstellbar. Wir nennen diese Teilchen Quantenbits oder Qubits. Und sie ermöglichen eine völlig neue Art von Rechenoperationen.

Okay. Und wenn Sie es beispielsweise für Ihre Großeltern noch anschaulicher machen wollen?

Dann würde ich ein Labyrinth als Metapher wählen. Wenn ein Mensch in einem Labyrinth steht und hinausfinden will, entscheidet er sich an der Weggabelung für links oder rechts. Wie ein Computer, eins oder null. Wenn er nicht weiterkommt, geht er zu einer früheren Abzweigung zurück und entscheidet sich für die andere Option. Das ist die alte Methode.

Die Arbeitsweise von Quantencomputern kann man sich so vorstellen, als würde man das Labyrinth mit riesigen Mengen Wasser fluten. Das Wasser kann an jeder Abzweigung gleichzeitig in beide Richtungen fließen und kommt dadurch immer ans Ziel. Aber genau darin liegt auch das aktuelle Problem der Quantenforschung.

Welches ist das?

Gewissermaßen sehen wir zwar, wie das Wasser aus dem Labyrinth kommt, also dass es seinen Weg gefunden hat. Aber wir wissen nicht, wie. Wir wissen nicht, welcher Weg der richtige war. Auf die Quantenforschung übertragen bedeutet das: Wir können nicht immer in einem für Menschen verständlichen Maß auslesen, was die derzeitigen Quantencomputer berechnen.

Was sind die größten Hindernisse dabei? Woran forschen Sie gerade?

Was uns bremst, sind vor allem zwei Dinge: Zum einen fehlen uns oft noch die praktischen Anwendungsfälle, in denen Quantencomputer tatsächlich einen Vorteil bringen. Zum anderen brauchen wir eine starke Fehlerkorrektur. Denn im Gegensatz zu herkömmlichen Computern, die sehr zuverlässig arbeiten, wird kein Qubit je vollkommen fehlerfrei sein. Und wenn man sehr viele Rechenoperationen durchführt, pflanzt sich ein einziger kleiner Fehler immer weiter fort. Deshalb reicht es nicht, nur ein Qubit zu verwenden, sondern man braucht drei oder fünf oder siebzehn. Je mehr, desto zuverlässiger. Wenn also ein Qubit einen Fehler macht, kommen wir immer noch zu dem richtigen Ergebnis.

In wie vielen Firmen und Universitäten wird an Quantencomputern gearbeitet?

Mehrere Hundert Organisationen arbeiten an der Entwicklung von Bauteilen und Teilsystemen. Komplette Quantencomputersysteme gibt es an mehreren Dutzend Orten weltweit. Es sind inzwischen sicherlich mehrere Hunderttausend Menschen, die daran arbeiten.

Wo stehen wir denn aktuell, was ist der leistungsfähigste Quantencomputer?

Das ist schwer zu sagen. Die Leistung herkömmlicher Rechner können wir sehr gut messen und vergleichen. Da gibt es zum Beispiel die Taktfrequenz des Prozessors in Gigahertz oder die Rechenoperationen pro Sekunde, die etwa in Teraflops gemessen werden.

Bei Quantencomputern sind drei Faktoren wichtig: die Zahl der Qubits, die Qualität dieser Qubits, also die Fehlerhäufigkeit, und die Konnektivität, also mit wie vielen Qubits jeder Qubit verbunden ist. Diese drei Größen in einer einzelnen Kennzahl zusammenzufassen ist nicht einfach. Deshalb gibt es zurzeit sehr hitzige Diskussionen darüber, was eine gute Vergleichsgröße wäre.

IBM sagt beispielsweise, „Quantenvolumen" sei die beste Metrik, um die Leistungsfähigkeit eines Quantencomputers zu messen. Nun stehen IBMs Quantencomputer zufälligerweise genau in dieser Metrik sehr gut da. Die nächste Firma hingegen schlägt vielleicht eine andere Gewichtung vor, die eher ihr einen Vorsprung verschafft.

Wie groß ist so ein Quantencomputer?

Normalerweise etwa so groß wie ein etwas geräumigerer Kleiderschrank. Aber es gibt auch kleinere Versionen. Ein Modell passt sogar in ein klassisches 19-Zoll-Rack, wie man es aus gewöhnlichen Serverräumen kennt. Er hat nur vier Qubits, aber er existiert.

Weshalb können wir derzeit noch nicht gut genug auslesen, was die Quantencomputer rechnen. Woran liegt das?

An der Tatsache, dass die Beobachtung von einem quantenmechanischen System dessen Zustand unvermeidbar verändert – das ist sogar einer der Grundsätze der Quantenmechanik. 〉

„In der Quantentechnologie verwenden wir statt Transistoren Atome. Und damit ändert sich alles."

Foto: Forschungszentrum Jülich / Sascha Kreklau

Heißt das, dass wir Quantencomputer nutzen werden, ohne sie auszulesen wie einen herkömmlichen Rechner?

Nicht wirklich. Wir müssen Ergebnisse auslesen können, wenn wir die Lösung der Probleme, die wir einem Quantencomputer gestellt haben, nutzen möchten. Das heißt also, dass wir die Quantencomputer programmieren müssen, damit sie während des Rechenprozesses zwar gleichzeitig mehrere, miteinander verschränkte Lösungswege ausloten – es uns aber am Ende ermöglichen, das Ergebnis direkt auszulesen. Also Quantenverarbeitung ja, aber mit klassischem Output.

Welche Probleme werden wir in zehn Jahren mit Quantum Computing lösen – oder zumindest angehen können?

Ich bin recht zuversichtlich, dass wir in zehn Jahren erste Anwendungen für die Simulation komplexer Vorgänge sehen werden. Das heißt, wir werden beobachten, wie sich gewisse Chemikalien oder Materialien verhalten, bevor wir sie wirklich entwickelt haben. Bisher ist uns diese Vorabberechnung von Eigenschaften neuer Stoffe unmöglich. Welche Wirkung kann ein bestimmtes Molekül als Medikament auslösen? Mithilfe von Quantensimulatoren werden wir das langfristig effizient ausrechnen können.

Werden Quantencomputer das können, weil sie einfach leistungsfähiger, also schneller sind als die herkömmlichen Rechner? Oder weil sie völlig anders arbeiten?

Beides, man kann damit ganz neue Dinge machen. Oder alte Dinge anders. Wenn ein Quantencomputer einfach nur schneller rechnen kann als herkömmliche Supercomputer, sprechen wir von „Quantum Supremacy“, also der Quantenüberlegenheit. Google hat das 2019 mit einem Rechner mit 53 Qubits geschafft. Aber das hatte keinerlei praktischen Nutzen, das war einfach ein extrem komplexes mathematisches Problem. Wenn ein Quantencomputer eine wirklich relevante Aufgabe lösen kann, die ein herkömmlicher Rechner nicht schafft, sprechen wir vom „Quantenvorteil“. Davon sind wir noch einige Jahre entfernt.

Welche Art von Aufgaben werden Quantencomputer besser lösen können als herkömmliche Supercomputer?

Ein wichtiges Beispiel ist die Faktorisierung von Zahlen, also ihre Zerlegung in Primzahlen. In welche Primzahlen ist 21 zerlegbar? Das lässt sich noch im Kopf machen: drei mal sieben. Bei der Zahl 7391 wird es für Menschen schon schwierig, ein Computer bekommt auch das noch recht schnell durchprobiert.

Aber bei einer 32-stelligen Zahl kommen selbst Supercomputer an ihre Grenzen. Quantencomputer hingegen werden auch solche Zahlen sehr schnell zerlegen können. Und das ist in Zukunft ganz entscheidend für das Thema Cybersicherheit.

„Wir müssen Verfahren zur Dekodierung entwickeln, die nicht von Quantencomputern geknackt werden können.“

Weil ein superschneller Quantencomputer einfach in ein paar Sekunden alle Passwörter der Welt durchprobieren könnte? Dann könnte er auch mein Online-Banking knacken, oder?

Das ist zwar eine häufige Sorge, aber das ist nicht wirklich ein Problem. Ihre Bank und alle anderen professionellen Systeme würden ja nach einigen Fehlversuchen den Zugriff sperren. Aber ein funktionierender Quantencomputer würde die häufigsten Algorithmen für Verschlüsselungen knacken. Denn unsere heutigen Verschlüsselungsalgorithmen basieren eben darauf, dass die Faktorisierung einer großen Zahl in Primzahlen wie gesagt sehr schwierig ist. Gleichzeitig aber ist es sehr einfach, Primzahlen miteinander zu multiplizieren. Das kann jeder mit dem Taschenrechner.

Die Verschlüsselung ist also einfach, aber die Dekodierung ist sehr schwierig. So soll es ja sein. Aber diese Primzahl-Faktorisierung ist ein Problem, für dessen Lösung sich Quantencomputer dummerweise besonders gut eignen.

Sie werden also die gängigen Verschlüsselungen von Messengern wie WhatsApp über E-Commerce bis hin zu digitalen Signaturen knacken können?

Davon ist auszugehen. Noch ist das vollkommen unmöglich, zehn bis fünfzehn Jahre wird es mindestens noch dauern. Aber das klingt nach mehr Zeit, als es ist. Denn wir müssen bis dahin neue Verschlüsselungsverfahren entwickelt haben, die nicht auf Faktorisierung setzen und dagegen resistent sind, von Quantencomputern geknackt zu werden.

Dieses Feld nennt man „Post-Quantum Cryptography“. Und daran wird schon mit Hochdruck geforscht. Denn wir müssen diese neuen Methoden ja nicht nur erfinden, wir müssen sie auch testen und alle Systeme damit ausstatten. Jedes Smartphone nutzt heute Verschlüsselungen, also müssen wir auch eine neue Generation von Verschlüsselungs-Algorithmen auf jedes Smartphone bringen.

Wie muss man sich diese Verschlüsselung für das Post-Quantum-Cryptography-Zeitalter vorstellen?

Sie wird im Prinzip auf eine ähnliche Art funktionieren müssen wie die bisherige: Die Verschlüsselung muss einfach sein, die Entschlüsselung komplex. „Schwer reversibel“ nennen wir das in der Mathematik.

Statt der Primzahlenzerlegung werden wir aber komplexere mathematische Operationen dafür verwenden müssen. Es gibt beispielsweise Ansätze, die mit elliptischen Kurven und deren algebraischer Struktur arbeiten.

Können Sie die Verschlüsselung einer Mail mithilfe einer elliptischen Kurve so erklären, dass ein Laie wie ich es noch verstehen kann?

Es tut mir leid, aber ich fürchte: nein (lacht).

Das klingt nach einem drohenden Wettlauf zwischen Gut und Böse – zwischen Sicherheitsforschenden und kriminellen Hackern. Wird man Quantencomputer reglementieren müssen wie Atomwaffen?

Oh ja! Es gibt bereits eine engagierte Debatte, wer Quantencomputer nutzen darf, welche Ausfuhrkontrollen für bestimmte Bauteile existieren sollten und so weiter. Aktuell diskutieren die US-Regierung und die EU-Kommission, welche Regeln sinnvoll sind und wer sie aufstellen darf. Naturgemäß finden solche Gespräche oft hinter verschlossenen Türen statt, deshalb können wir über ihren genauen Stand nicht reden. Aber das „Quantum Industry Consortium“ und das Gremium „Quantum Community Network“, dem ich selbst vorstehe, beschäftigen sich mit guten und sinnvollen Kriterien, wie man diese Kontrolle angehen sollte.

In der Digitalwirtschaft wirkt Europa oft abgehängt. Wie groß ist seine Rolle im Bereich Quantencomputer?

IBM und Google sind zwei große amerikanische Player in diesem Bereich. Daneben gibt es zahlreiche US-Start-ups oder Ausgründungen von US-Unternehmen wie Honeywell, die mit Quantinuum ein sehr erfolgreiches Unternehmen gestartet haben. Aber Europa muss sich nicht verstecken – mit Start-ups wie Pasqal und Quandela aus Frankreich oder Alpine Quantum Technologies (AQT) aus Österreich und IQM aus Finnland.

Auch auf wissenschaftlicher Ebene tut sich eine Menge, es gibt eine sehr rege Zusammenarbeit. So bauen wir zum Beispiel gerade eine europäische Infrastruktur auf, bei der sich sieben Hochleistungsrechenzentren in Europa zusammenschließen. Europäische Start-ups können dort ihre Quantencomputer gewissermaßen auf den Prüfstand stellen, testen und einer breiten User-Community zur Verfügung stellen. Europas große Chance liegt in der Kollaboration.

Wo steht China in der Quantenforschung?

Die chinesischen Forschenden sind extrem stark dabei. Lange Zeit waren sie nicht besonders relevant, aber sie haben aufgeholt. Das liegt vor allem an der staatlichen Förderung, nennenswerte Privatunternehmen gibt es kaum. Aber einige Zahlen, die man aus China hört, sind Fantasiezahlen. Oft ist zum Beispiel von zehn Milliarden Dollar die Rede, die vom Staat in den Sektor investiert werden. Realistisch ist vermutlich ein Viertel davon. Das ist immer noch eine Menge, und es gibt mittlerweile Gruppen, die sehr gute Arbeit leisten. Aber sie sind im Gegensatz zu Forschenden in den USA und Europa eher nur untereinander vernetzt. Das ist für die Cybersicherheit nicht unbedingt ideal.

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.

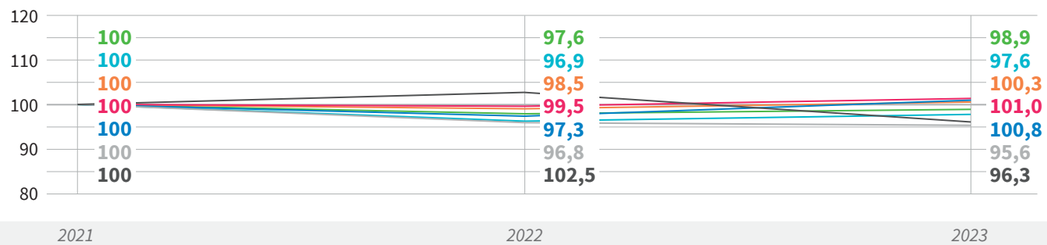
Weniger Ahnung, weniger Schutz, weniger Sorgen

Index-Veränderung gegenüber dem Basisjahr 2021; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2023

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 %)

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

Index



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

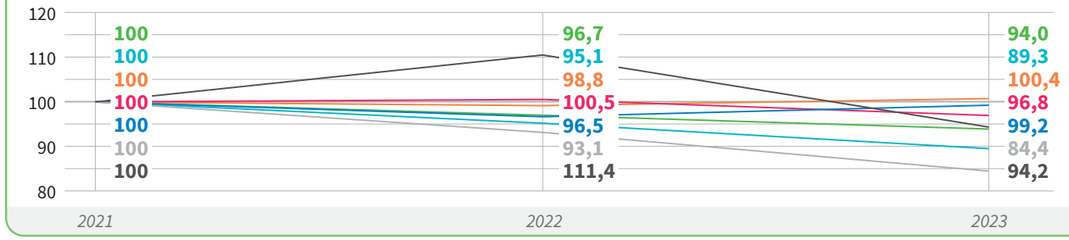
Wissen:
Wie schätzen Sie Ihre Kompetenz / Ihren Wissensstand zum Thema IT-Sicherheit ein?
Antworten auf einer Skala:
1 = sehr geringe Kompetenz,
5 = sehr große Kompetenz

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

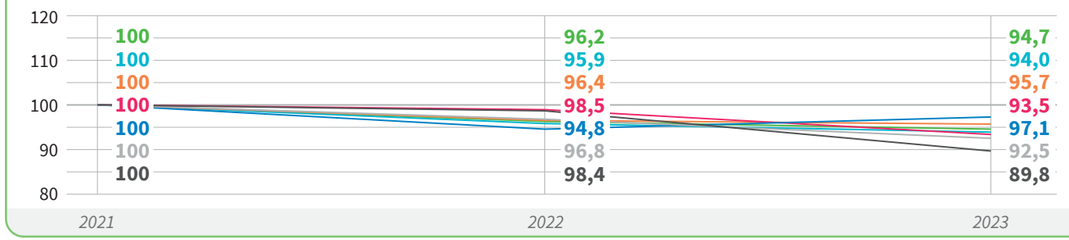
Risiko:
Wie hoch schätzen Sie das Risiko ein, Opfer von Cyberkriminalität oder Datenklau zu werden? (persönlich / beruflich)
Antworten auf einer Skala:
1 = sehr gering, 5 = sehr hoch

Quelle: Statista im Auftrag von G DATA

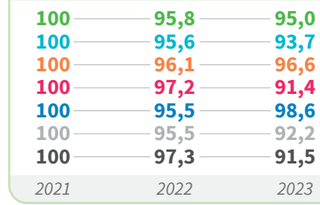
1 Wissenskompetenz Je höher der Wert, desto höher ist die Wissenskompetenz.



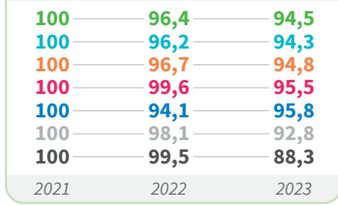
2 Sicherheitsgefühl gesamt Je höher der Wert, desto höher ist das Sicherheitsgefühl.



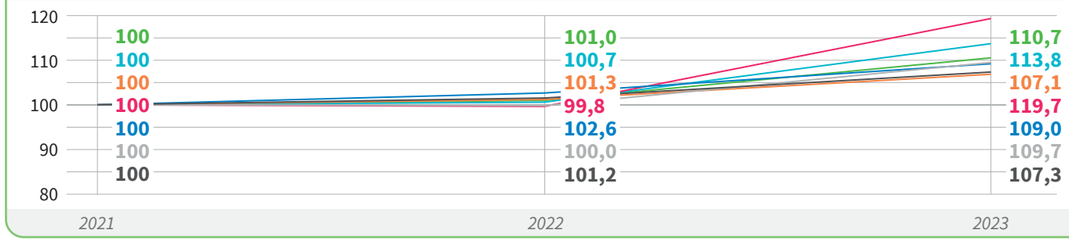
Sicherheitsgefühl privates Umfeld



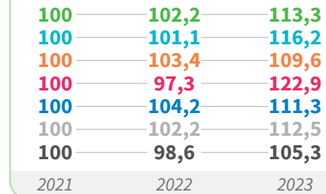
Sicherheitsgefühl berufliches Umfeld



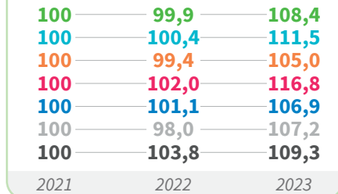
3 Risikoempfinden gesamt Je höher der Wert, desto geringer ist das Risikoempfinden.



Risikoempfinden privates Umfeld



Risikoempfinden berufliches Umfeld



WELT

Die Menschheit digitalisiert sich. Immer mehr Daten, immer neue Vernetzungen und immer komplexere Systeme führen leider auch zu immer neuen Schwachstellen und Einfallstoren für kriminelle Machenschaften. Zum Schutz fehlt es vielerorts an Know-how, Personal und an den nötigen Mitteln. Was bedeutet das – und wo führt das hin?

Es dauert … und dauert … und dauert …

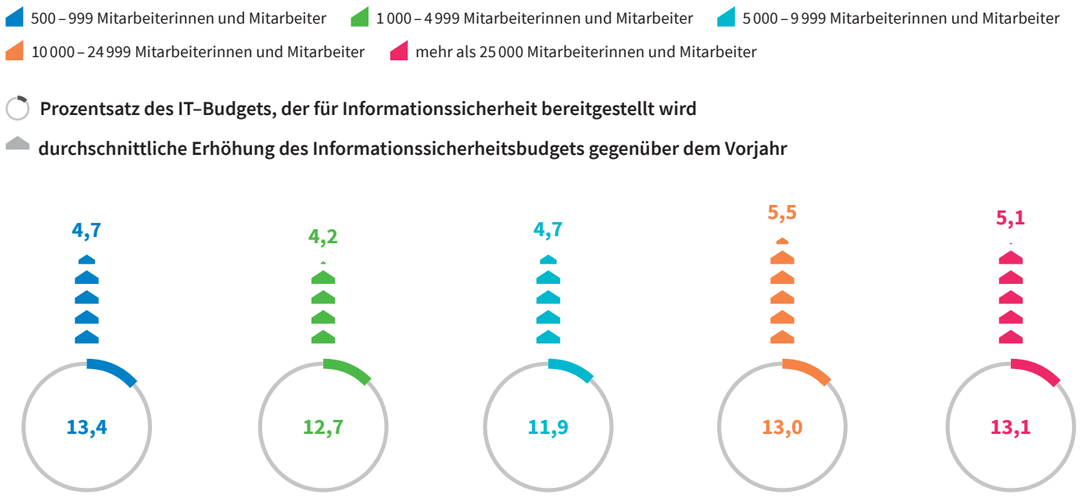
Vergehende Zeit bis zur Entdeckung und Eindämmung eines Datenlecks nach Angriffsart; Unternehmen, die von einem Datenleck betroffen waren; weltweit; 2022; in Tagen

Quelle: IBM

Glossar der Cyberbegriffe auf Seite 100 – 103

Zu wenig Budget

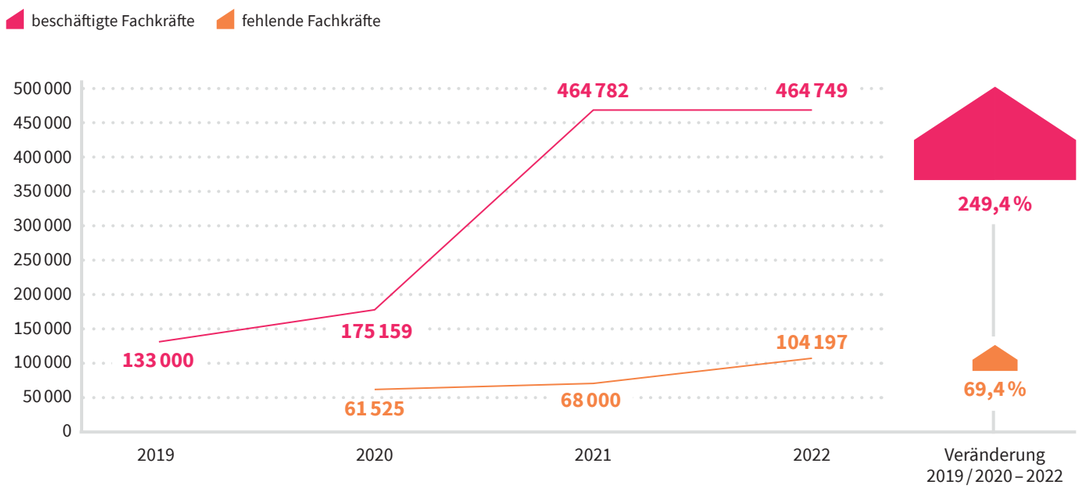
Durchschnittliche Jahresausgaben für Cybersicherheit nach Unternehmensgröße; Entscheidungsträgerinnen und Entscheidungsträger im IT-Sicherheitsbereich (n=1 200); ausgewählte Länder *; 2021; in Prozent



* Belgien, Frankreich, Deutschland, Irland, Niederlande, Spanien, Großbritannien, USA. Quelle: CyberEdge

Zu wenig Personal

Zahl der Fachkräfte und Personalmangel im Bereich Cybersicherheit; Deutschland

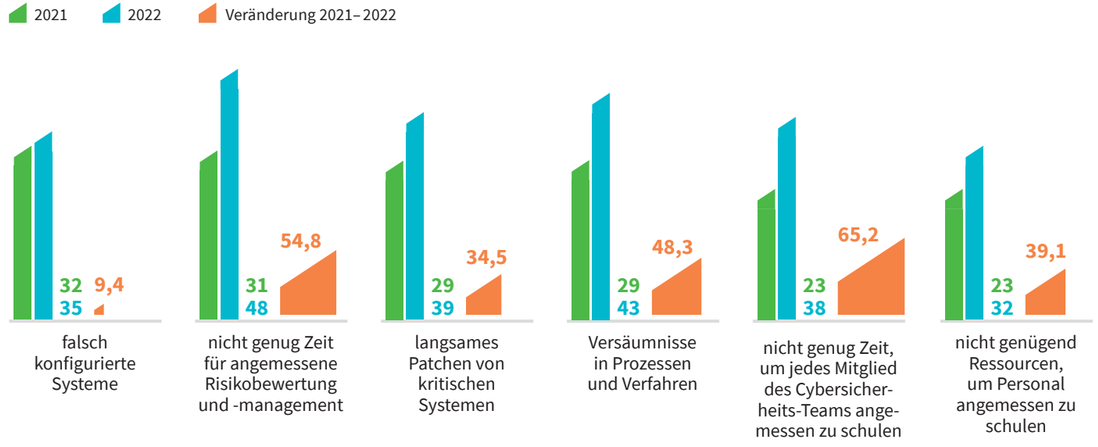


Quelle: (ISC)²

Zu wenig Zeit

Konsequenzen von Personalmangel im Bereich Cybersicherheit; globale Cybersicherheits-Expertinnen und -Experten, in deren Teams Personalmangel herrscht (n=4 967); 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?

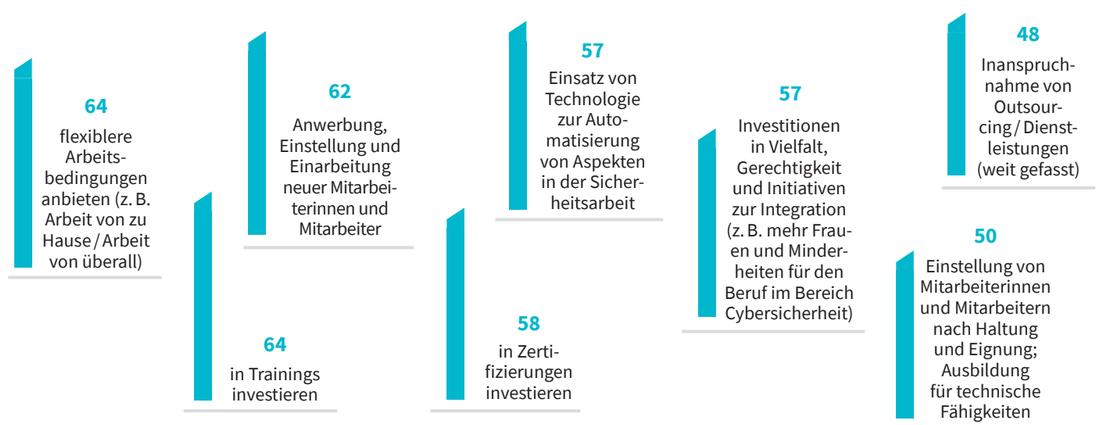


Quelle: (ISC)²

Zu wenig Engagement

Maßnahmen, um dem Personalmangel entgegenzuwirken; globale Fachleute für Cybersicherheit (n=11 525); weltweit; 2022; in Prozent

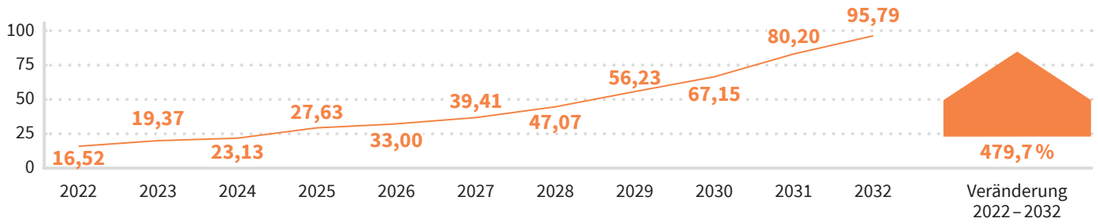
Welche der folgenden Maßnahmen ergreift Ihre Organisation oder plant sie zu ergreifen, um den Personalmangel im Bereich der Cybersicherheit in Ihrer Organisation zu verhindern oder abzumildern?



Quelle: (ISC)²

Eindrücklich

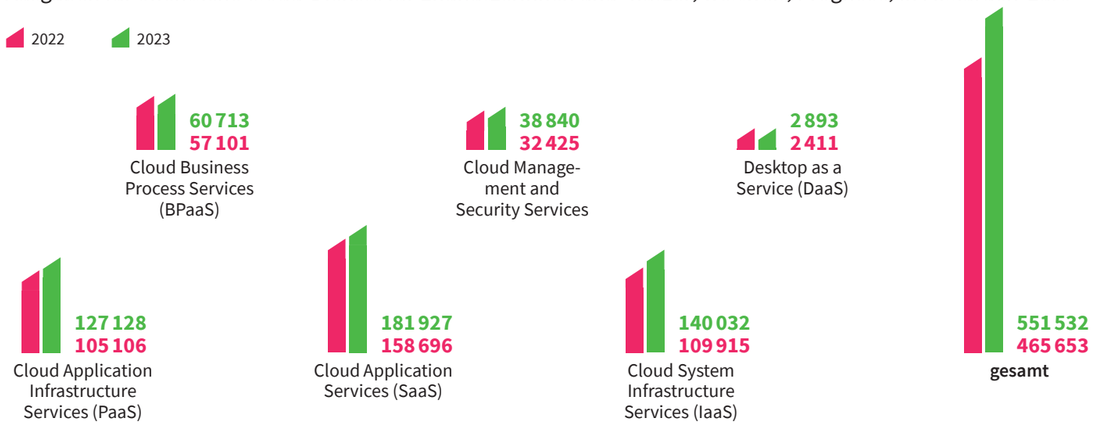
Entwicklung der Marktgröße von KI in der Zukunft; weltweit; Prognose; in Milliarden Euro



Quelle: Precedence Research

Öffentlich

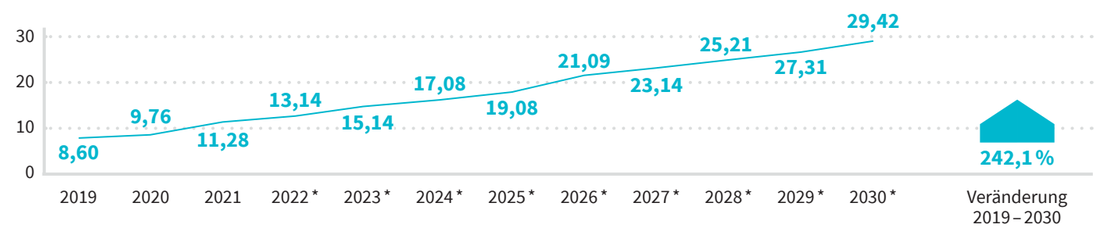
Ausgaben für öffentliche Cloud-Dienste für Endnutzerinnen und -nutzer; weltweit; Prognose; in Milliarden Euro



Quelle: Transforma Insights

Reichlich

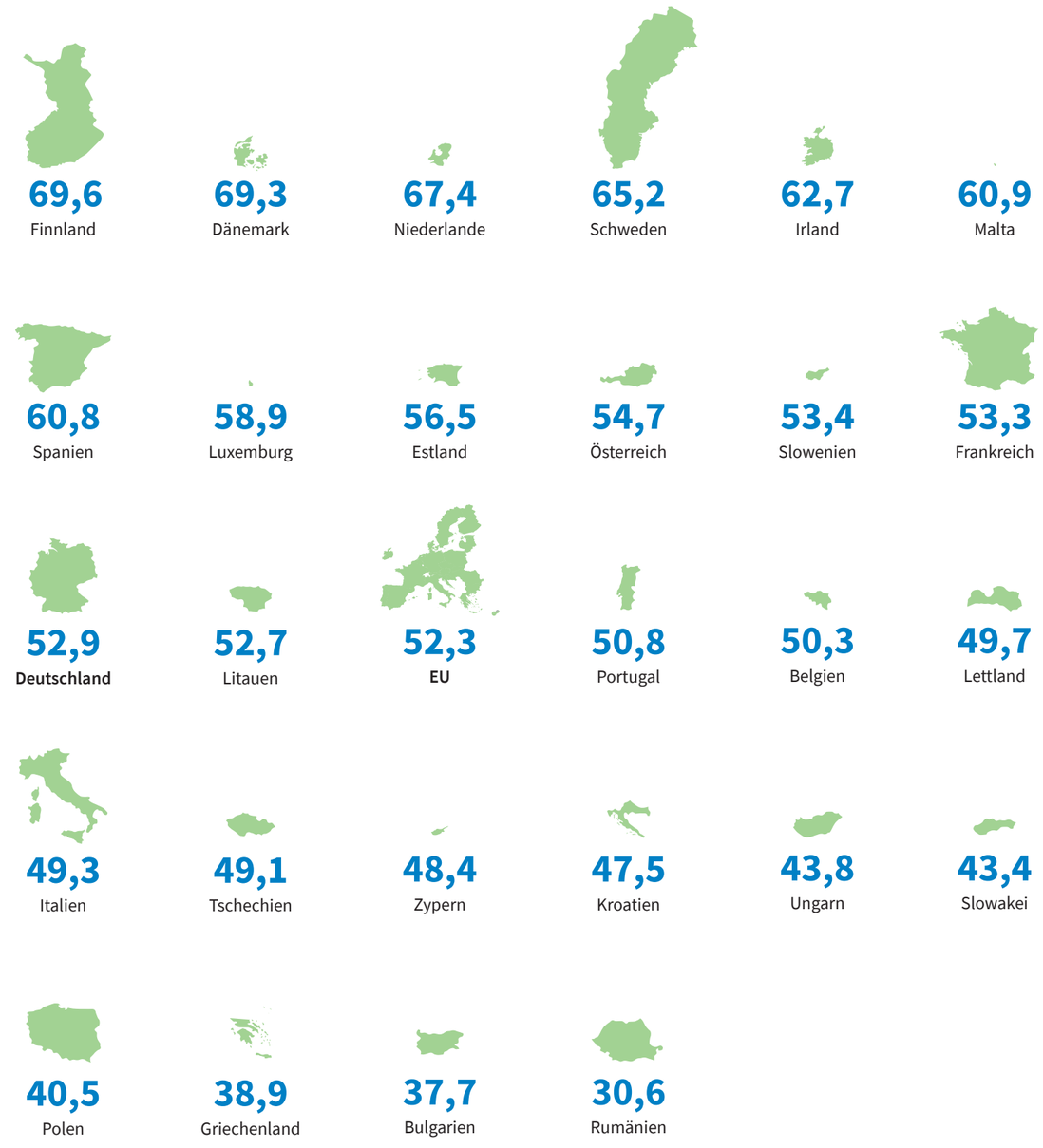
Zahl der mit dem IoT verbundenen Geräte; weltweit; in Milliarden



* Prognose. Quelle: Transforma Insights

Anschaulich

Digitalisierungsgrad nach DESI-Index *; Länder in Europa; 2022; Index

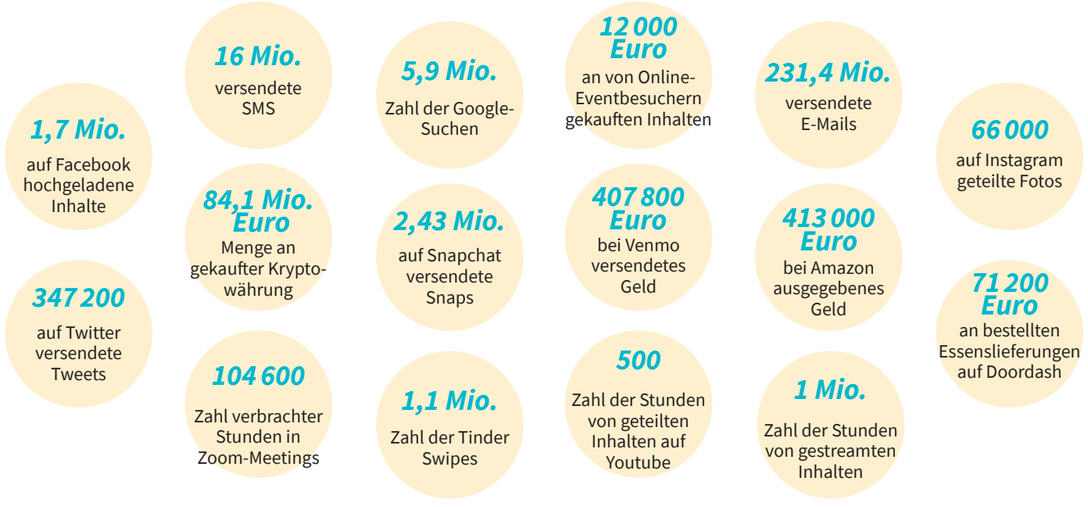


* DESI = Digital Economy and Society Index. Der DESI-Gesamtindex wird berechnet als gewichteter Durchschnitt der vier DESI-Hauptdimensionen: 1 Humankapital (25 %), 2 Konnektivität (25 %), 3 Integration digitaler Technologie (25 %) und 4 Digitale öffentliche Dienste (25 %).

Quelle: Europäische Kommission

Pro Minute

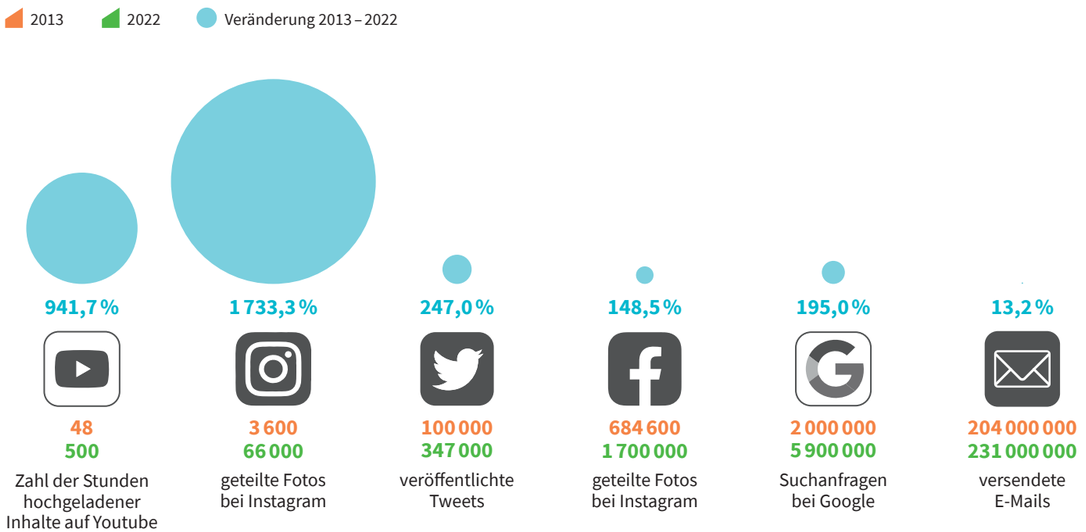
Geschätzte Menge an neu kreierten Daten im Internet pro Minute; weltweit; 2022



Quelle: Domo

Pro Dekade

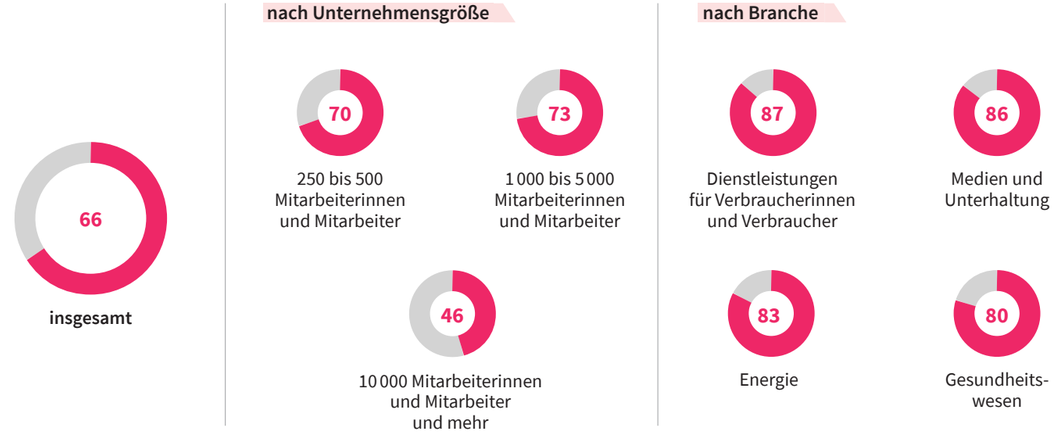
Geschätzte Menge an neu kreierten Daten im Internet pro Minute im Jahresvergleich 2013 / 2022; weltweit



Quelle: Domo

Pro Unternehmen und Branche

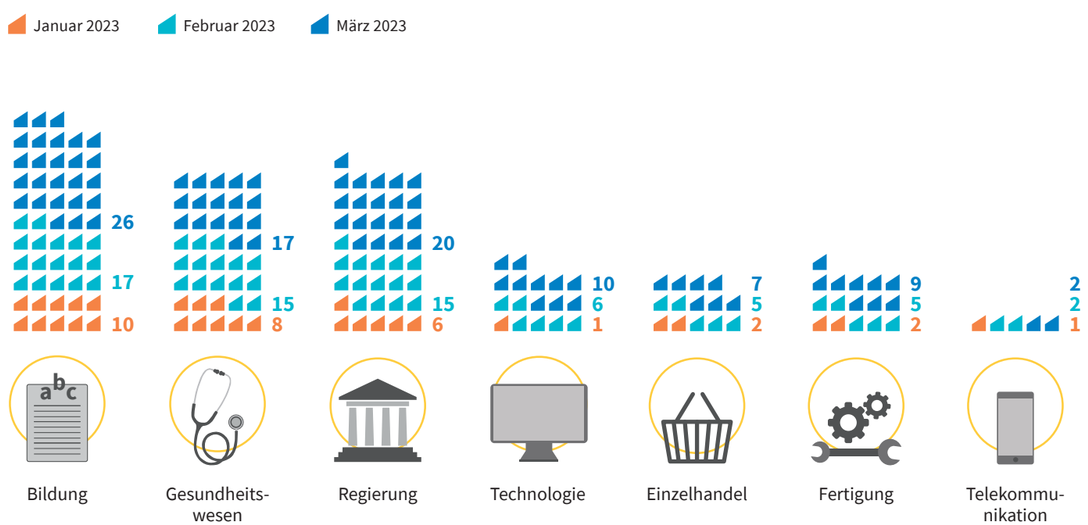
Anteil der Unternehmen, deren Geschäftsbetrieb von Ransomware gestört wurde; weltweit *; 2022; in Prozent



* Die Umfrage lief im Oktober und November 2022 und umfasste Teilnehmerinnen und Teilnehmer aus insgesamt 13 Ländern (USA, Kanada, Großbritannien, Frankreich, Deutschland, Niederlande, Schweden, Dänemark, Saudi-Arabien, Vereinigte Arabische Emirate, Südafrika, Singapur und Australien). Quelle: Mimecast

Pro Sektor und Monat

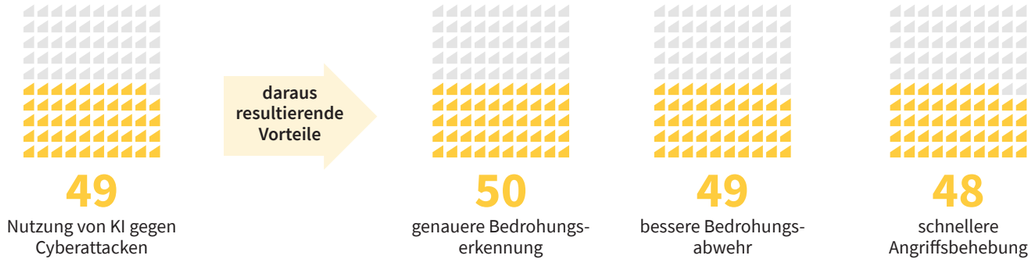
Zahl der Ransomware-Attacken nach Industriesektor pro Monat; weltweit; 2023



Quelle: Blackfog

Hilfreich

Vorteile von KI bei der Abwehr von Cyberattacken; IT- und Cybersicherheits-Fachleute (n=1 700); weltweit *; 2022; in Prozent



* Die Umfrage lief im Oktober und November 2022 und umfasste Teilnehmerinnen und Teilnehmer aus insgesamt 13 Ländern (USA, Kanada, Großbritannien, Frankreich, Deutschland, Niederlande, Schweden, Dänemark, Saudi-Arabien, Vereinigte Arabische Emirate, Südafrika, Singapur und Australien). Quelle: Mimecast

Schutzbedürftig

Zahl kompromittierter Accounts *; weltweit

	2022	2023	Veränderung 2022 – 2023
identifizierte kompromittierte Accounts	12 769 188 186	13 301 678 581	4,2 %
geleakte Accounts pro Tag	1 616 604	1 589 334	– 1,7 %
Zahl der Leaks	1 457	1 768	21,3 %

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

Besorgt

Meist gefürchtete Gründe für Betriebsunterbrechungen von Unternehmen; weltweit; 2022; in Prozent *

* Mehrfachnennungen möglich. Quelle: Allianz

Verurteilt

Top-10-Bußgelder für Datenschutzverstöße 2019 – 2023 *; weltweit; in Euro

1
4 536 999 350
USA
Facebook Inc.
24.7.2019
Verstoß gegen frühere FTC-Datenschutz-anordnungen und 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
Rekordbußgeld 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
265 000 000
Irland
Meta Platforms Ireland Ltd.
28.11.2022
Entscheidung im Data-Scraping-Verfahren gegen Meta

10
259 482 921
USA
Epic Games Inc.
20.12.2022
Rekordvergleich nach Verstoß gegen Jugendschutzgesetz

* Datenabruf am 21.08.2023. ** FTC: Federal Trade Commission (Bundesbehörde der USA). Quelle: DSGVO-Portal

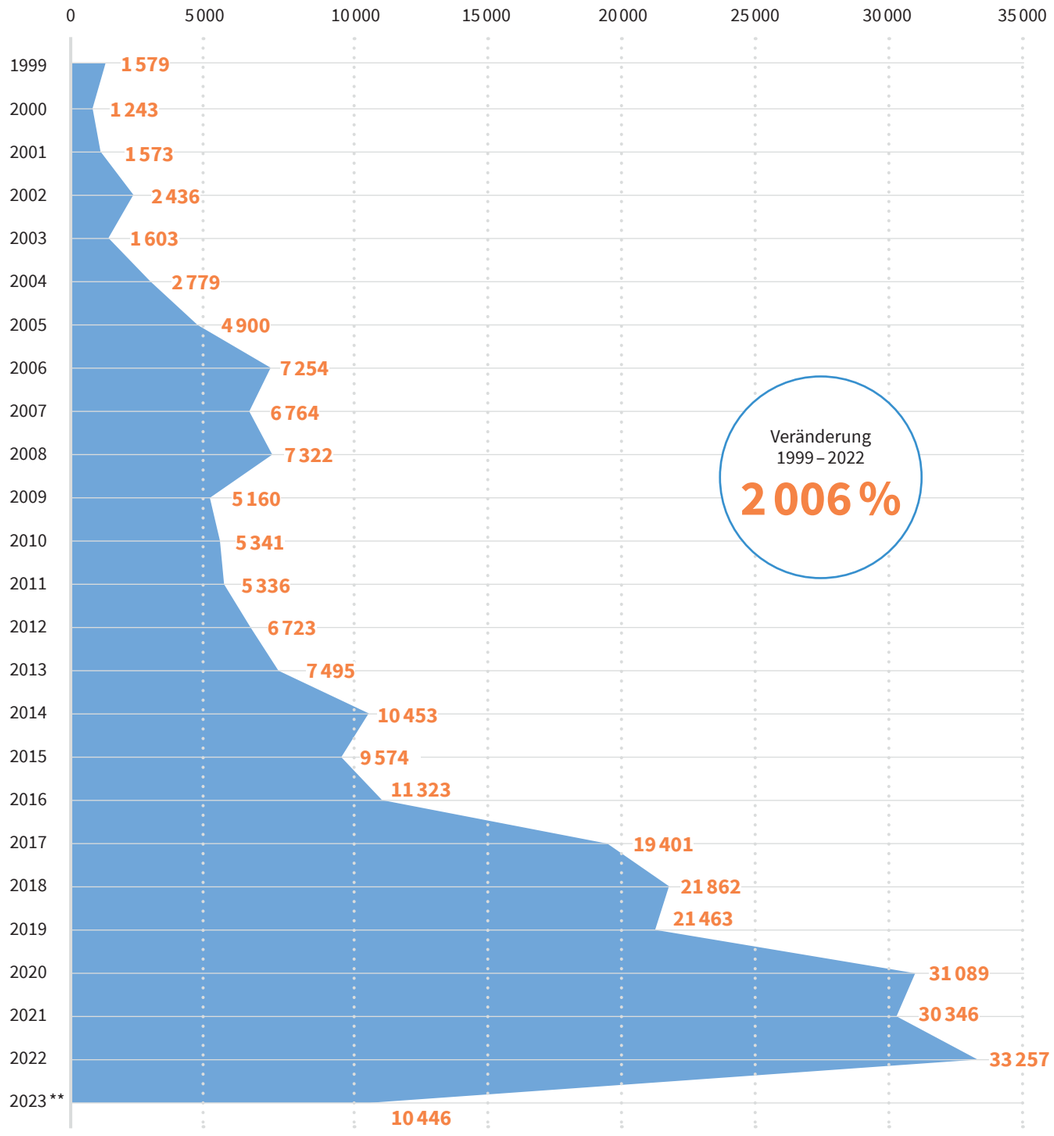
Vernachlässigt

Ursachen für Sicherheitsvorfälle; Sicherheitsverantwortliche (n=872); weltweit; 2022; in Prozent

Quelle: Foundry

Wachsende Risiken

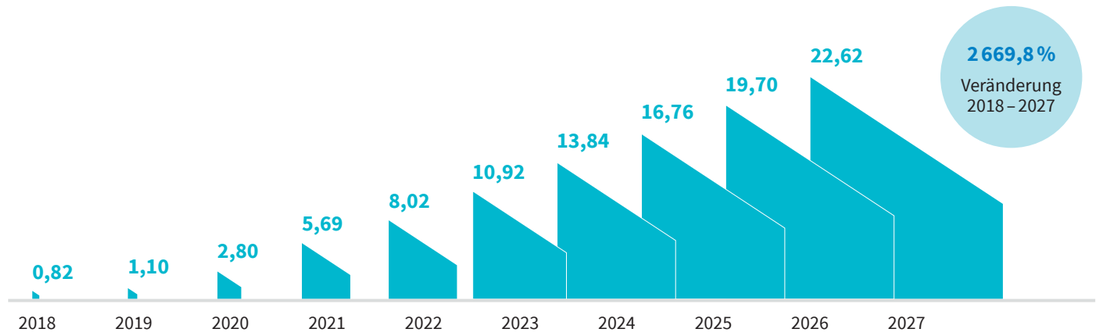
Zahl der von CVE * dokumentierten Schwachstellen in der IT-Sicherheit; weltweit



* 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. Fachleute aus den Bereichen Informationstechnologie und Cybersicherheit verwenden CVE-Datensätze, um sicherzustellen, dass sie über das gleiche Problem sprechen, und um ihre Bemühungen zu koordinieren, die Schwachstellen zu priorisieren und zu beheben.
** Stand 28.3.2023. Quelle: CVE unterstützt durch U.S. Department of Homeland Security und Cybersecurity and Infrastructure Security Agency

Steigende Kosten

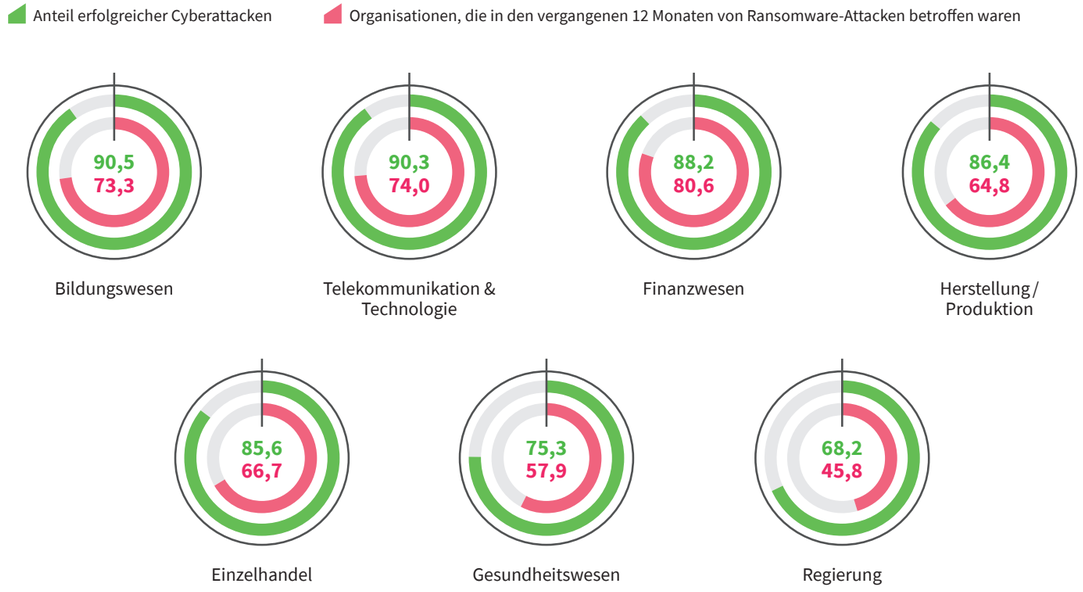
Geschätzte * zukünftige durch Cybercrime verursachte Kosten; weltweit; in Milliarden Euro



* Ab 2022. Die Daten basieren auf Wechselkursen aus November 2022. Quelle: Statista

Identifizierte Opfer

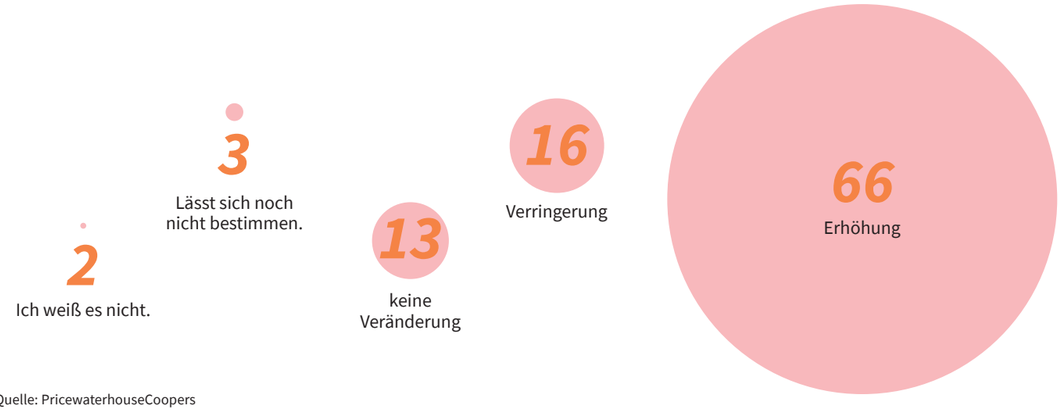
Anteil erfolgreicher Cyberattacken je Branche; qualifizierte Entscheidungsträgerinnen und Entscheidungsträger in der IT-Sicherheit (n=1 200) und Organisationen, die in den vergangenen 12 Monaten von Ransomware-Attacken betroffen waren, nach Branchen; weltweit; 2022; in Prozent



Quelle: CyberEdge

Im Fokus

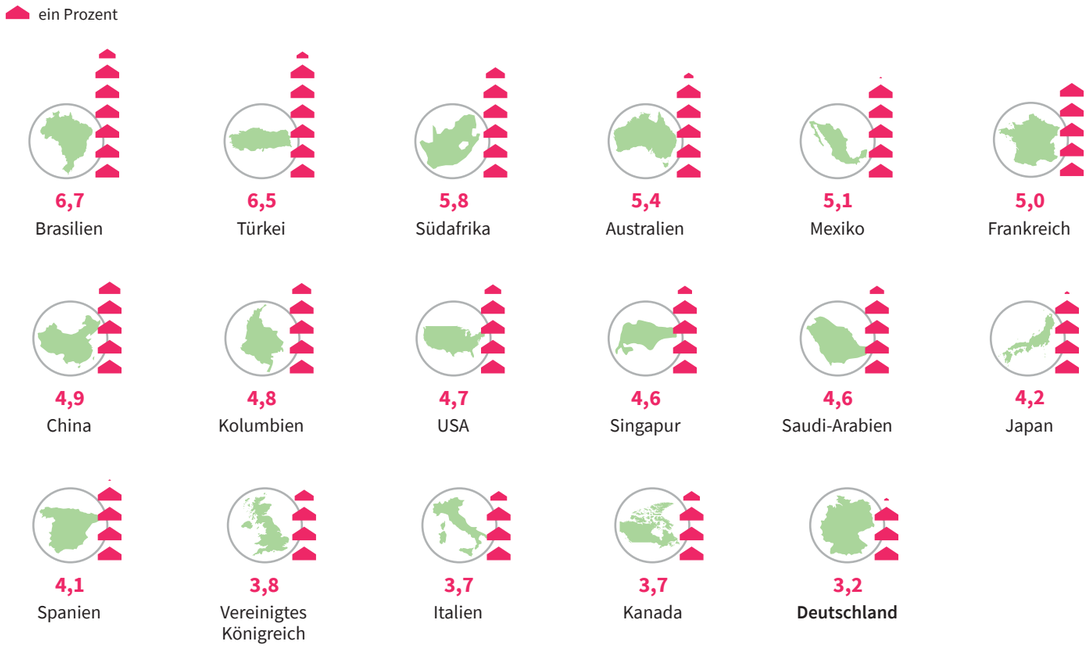
Veränderung des Cybersecurity-Budgets im Jahr 2023 im Vergleich zum Vorjahr; Führungskräfte aus dem Wirtschafts- und Technologie-Umfeld (n=3 522); weltweit; 2022; in Prozent



Quelle: PricewaterhouseCoopers

Im Schnitt

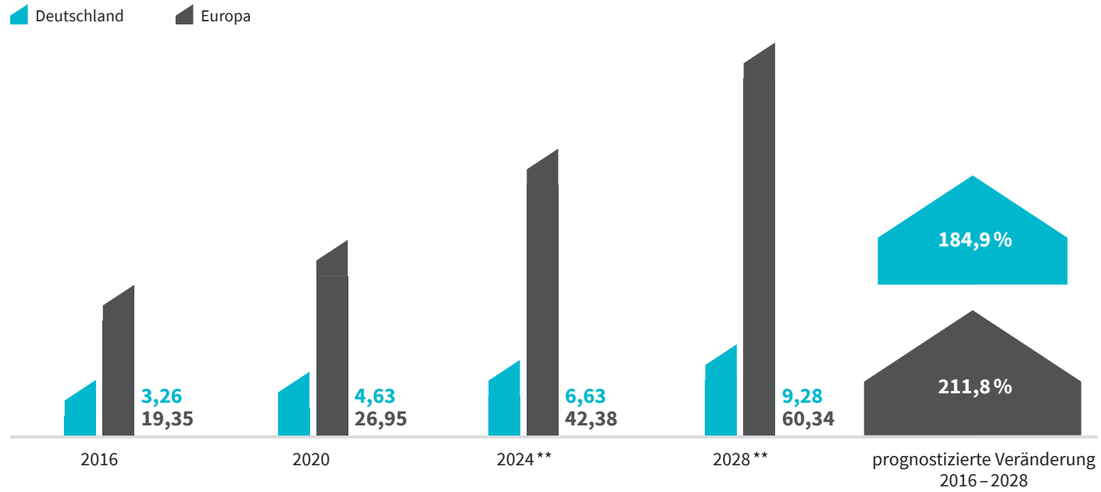
Durchschnittliche Zunahme des Cybersecurity-Budgets nach Ländern; qualifizierte Entscheidungsträgerinnen und Entscheidungsträger in der IT-Sicherheit (n=1 200); weltweit; 2022; in Prozent



Quelle: CyberEdge

Im Ganzen

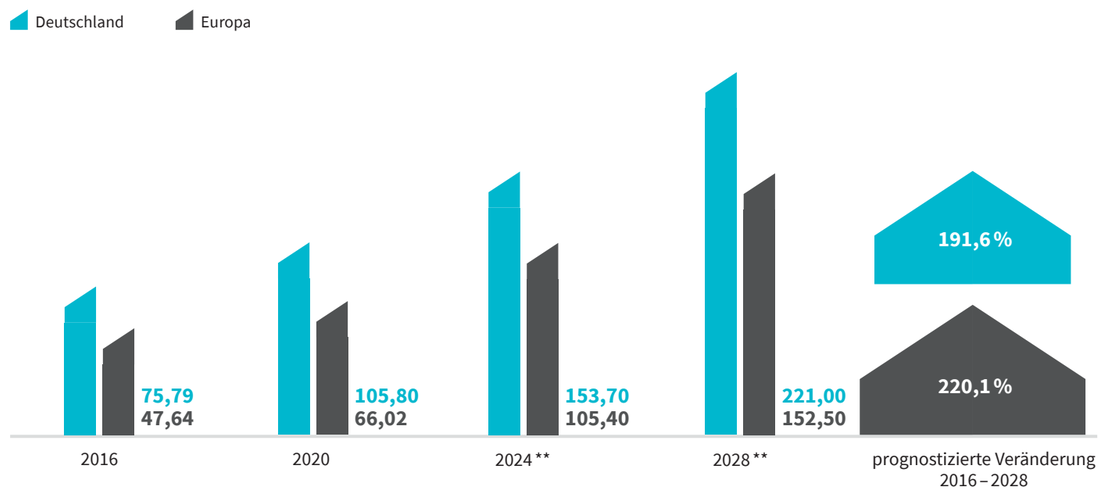
Umsatz des Cybersicherheitsmarktes; Deutschland & Europa; in Milliarden Euro *



* Die Daten werden in aktuellen Wechselkursen gezeigt und reflektieren die Einflüsse des Russland-Ukraine-Kriegs auf den Markt. ** Prognose. Quelle: Cybersecurity Outlook Statista

Im Einzelnen

Durchschnittliche Ausgaben je Arbeitskraft für Cyber Solutions und Security Services; Deutschland & Europa; in Euro *



* Die Daten werden in aktuellen Wechselkursen gezeigt und reflektieren die Einflüsse des Russland-Ukraine-Kriegs auf den Markt. ** Prognose. Quelle: Cybersecurity Outlook Statista

Unterstützt

Anteil Unternehmen, die Managed Security Service Provider in Anspruch nehmen, nach Unternehmensgröße; qualifizierte Entscheidungsträgerinnen und Entscheidungsträger in der IT-Sicherheit (n=1 200); weltweit; 2022; in Prozent

500 – 999 Mitarbeiterinnen und Mitarbeiter	87,4
1 000 – 4 999 Mitarbeiterinnen und Mitarbeiter	92,7
5 000 – 9 999 Mitarbeiterinnen und Mitarbeiter	96,9
10 000 – 24 999 Mitarbeiterinnen und Mitarbeiter	96,0
mehr als 25 000 Mitarbeiterinnen und Mitarbeiter	94,3

Quelle: CyberEdge

Gewappnet

Maßnahmen von Unternehmen zur Erhöhung der Cybersicherheit; qualifizierte Entscheidungsträgerinnen und Entscheidungsträger in der IT-Sicherheit (n=1 200); weltweit; 2022; in Prozent

Sicherheitstraining für Anwendungsentwickler	63,0
Überprüfung von Webanwendungen	53,4
Sicherheitstests von Dritten / Bug Bounties	52,2
DevSecOps-Teams und Methodiken	49,1
Penetrationstests	42,4

Quelle: CyberEdge

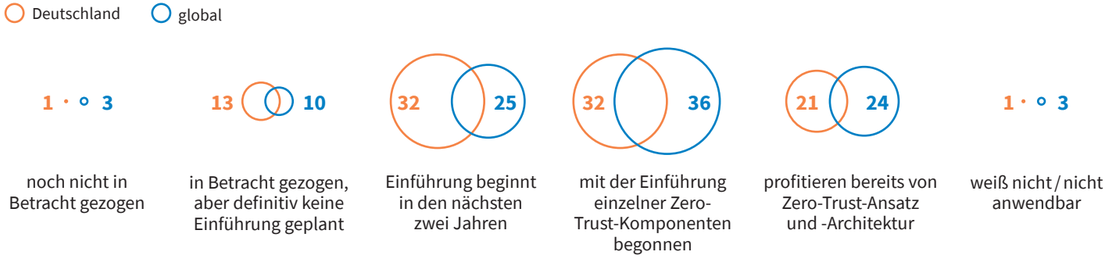
Versichert

Abschluss einer Cyberversicherung; qualifizierte Verantwortliche in Unternehmen für die Cybersicherheitsstrategie (n=5 181); ausgewählte Länder weltweit; 2022; in Prozent

Quelle: Hiscox

Verzögert

Umsetzung eines Zero-Trust-Ansatzes; Führungskräfte aus Wirtschafts- und Technologie-Umfeld (global: n=1 253, Deutschland: n=76); weltweit; 2022; in Prozent

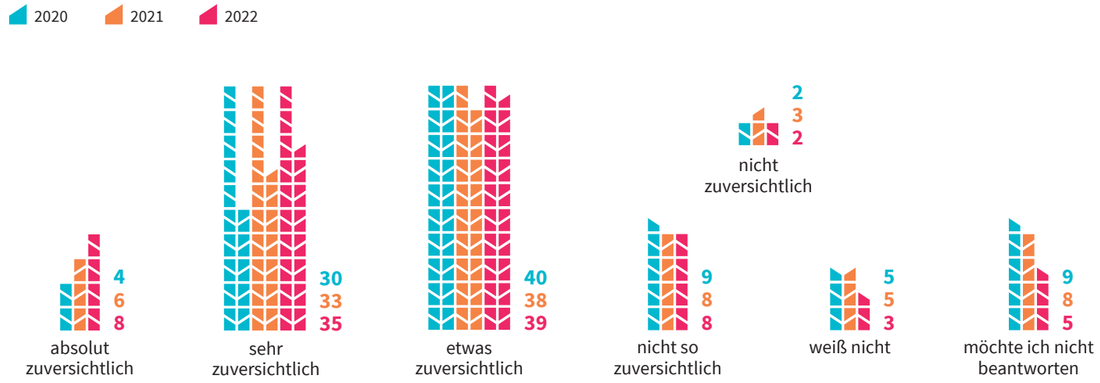


Quelle: PricewaterhouseCoopers

Überschätzt?

Zuversicht in Bedrohungserkennung und -reaktion; Fachleute für Cybersicherheit (n=2 031); weltweit; in Prozent

Wie zuversichtlich sind Sie, dass das Cybersicherheitsteam Ihres Unternehmens in der Lage ist, Cyberbedrohungen zu erkennen und auf sie zu reagieren?

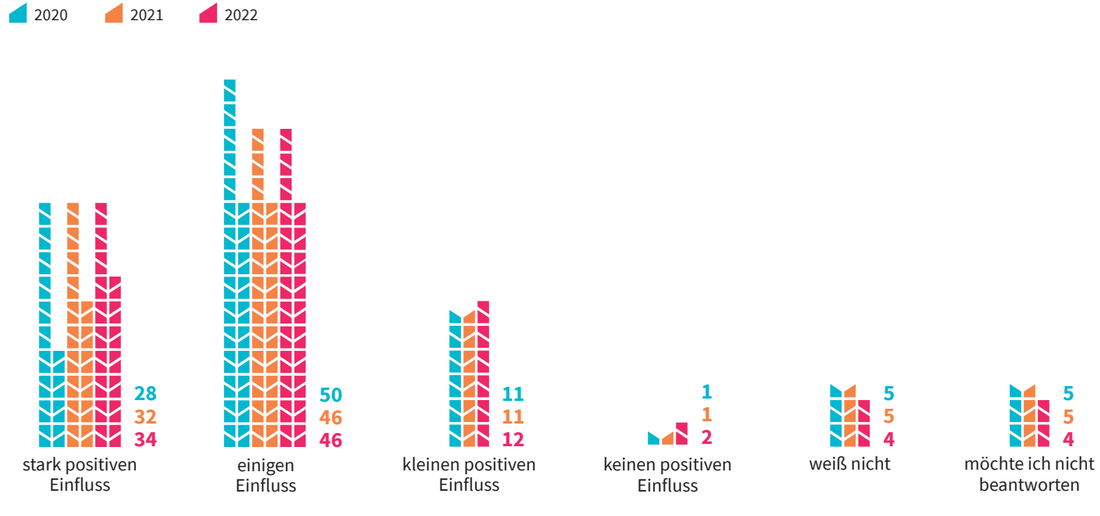


Quelle: ISACA

Überrascht?

Einfluss von Cybersicherheitstraining auf Awareness der Mitarbeiterinnen und Mitarbeiter für Cybersicherheit; Fachleute für Cybersicherheit (n=2 031); weltweit; in Prozent

Welchen Einfluss haben Ihrer Meinung nach die Schulungen und Sensibilisierungsprogramme für Cybersicherheit auf das allgemeine Bewusstsein der Mitarbeiterinnen und Mitarbeiter für Cybersicherheit in Ihrem Unternehmen?



Quelle: ISACA

Keine Ahnung

Security Awareness: Bekanntheit verschiedener Arten von Cyberbedrohungen bei berufstätigen Erwachsenen (n=4 000) und IT-Sicherheits-Expertinnen und -Experten (n=650) aus 15 Ländern; weltweit; 2022; in Prozent

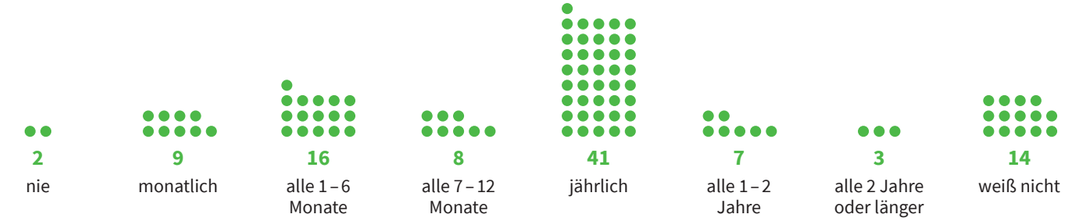
Unternehmen mit einem Security-Awareness-Programm, die alle Mitarbeiterinnen und Mitarbeiter in Security-Awareness-Trainings schulen: ..... 56 %

Quelle: Proofpoint

Keine Übung

Häufigkeit von Cybersicherheits-Assessments; Fachleute für Cybersicherheit (n=2 031); weltweit; 2022; in Prozent

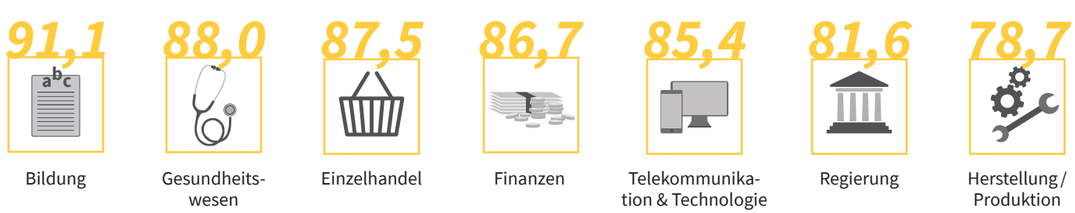
Wie oft wird eine Bewertung der Cyberrisiken in Ihrer Organisation durchgeführt?



Quelle: ISACA

Keine Leute

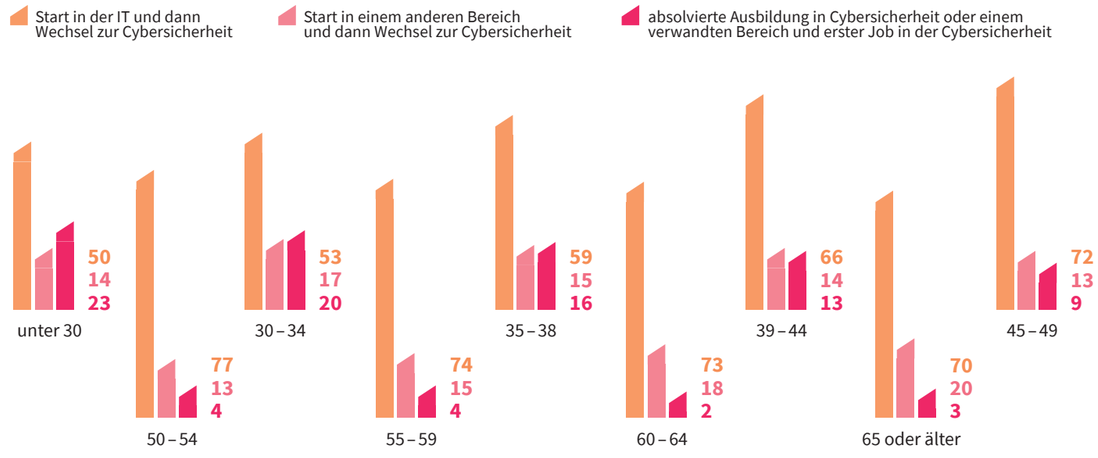
Branchen, in denen IT-Fachkräfte fehlen; qualifizierte Entscheidungsträgerinnen und Entscheidungsträger in der IT-Sicherheit (n=1 200); weltweit; 2022; in Prozent



Quelle: CyberEdge

Keine Ausbildung

Werdegang von Cybersicherheits-Fachkräften nach Alter; globale Cybersicherheits-Expertinnen und -Experten, in deren Teams Personalmangel herrscht (n=4 967); weltweit; 2022; in Prozent

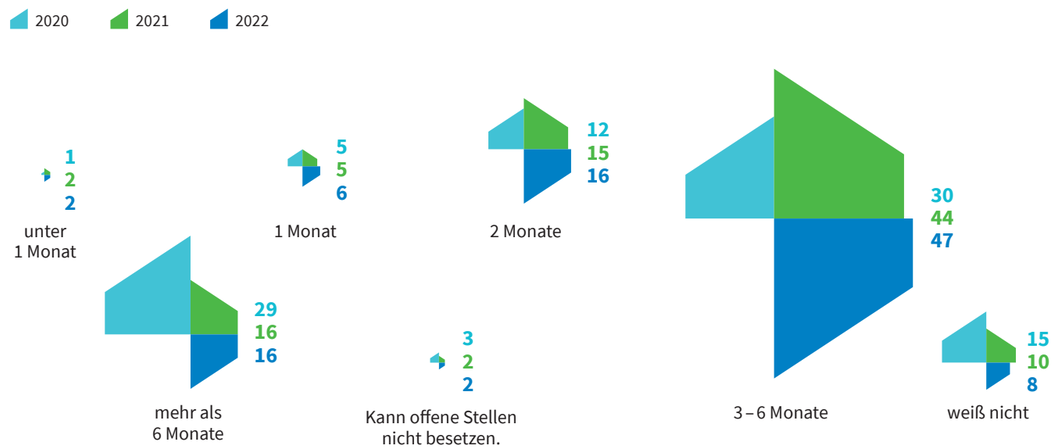


Quelle: (ISC)²

Keine Bewerberinnen und Bewerber

Zeit, um eine freie Cybersicherheits-Stelle im Unternehmen zu füllen; Cybersecurity-Fachleute (n=2 031); weltweit; in Prozent

Wie viel Zeit benötigt Ihre Organisation durchschnittlich, um eine Cybersicherheits-Stelle mit einer qualifizierten Kandidatin oder einem qualifizierten Kandidaten zu besetzen?



Quelle: ISACA

Grüner rechnen

Ein ideales Paar? Die Abwärme von Rechenzentren könnte in Zukunft Gewächshäuser und Indoorfarmen heizen. Erste Versuche gibt es etwa in Frankreich und Kanada.

Foto: AdobeStock

Server nachts herunterfahren, Grafikprozessoren einsetzen, Abwärme nutzen: Es gibt viele Möglichkeiten, dem wachsenden Ressourcenhunger von Rechenzentren etwas entgegenzuhalten. Der Wissenschaftler Ralph Hintemann weiß, welche schon funktionieren und wo Unternehmen mehr Druck auf die Anbieter ausüben könnten.

Text: Ulf Froitzheim

Rechenzentren gehören in Deutschland zu den Großverbrauchern von Strom. Laut Berechnungen des Wirtschaftswissenschaftlers Ralph Hintemann und seinem Team am Berliner Borderstep Institut bezogen 2021 alle Zentren zusammen 17 Terawattstunden elektrische Energie. So viel verbrauchen in etwa rund zehn Millionen Einwohner pro Jahr. Und der Stromhunger der immer leistungsfähigeren Systeme wächst kontinuierlich. Bis 2030 erwartet Borderstep einen Anstieg auf 28 Terawattstunden – eine Menge, die heute den jährlichen Bedarf aller Privathaushalte Nordrhein-Westfalens mit insgesamt knapp 18 Millionen Einwohnern decken würde.

Derzeit schlucken den größten Teil der Energie, nämlich 42 Prozent, die Server; mit den dazugehörigen Speichern sind es sogar 60 Prozent. Zur Stromrechnung trägt aber auch die Kühlung der elektronischen Komponenten massiv bei: 22 Prozent gehen allein dafür drauf, dass die Prozessoren und Memorys nicht buchstäblich durchschmoren.

Herr Hintemann, die Digitalisierung sorgt heute für viel Wertschöpfung, sie trägt aber zugleich dazu bei, was die Transformationsforscherin Maja Göpel „Schadschöpfung“ nennt. Der Stromverbrauch durch IT steigt stetig, so entstehen Kosten für Umwelt und Klima. Ist das den Verantwortlichen bewusst?

Ralph Hintemann: Sie stehen vor einem Zielkonflikt. Dass es da ein Problem gibt, sickert mehr und mehr durch. Aber unser aktuelles Wirtschaftssystem ist auf Konsum ausgerichtet und setzt die falschen Anreize. Deshalb haben auch viele digitale Lösungen zum Ziel, den Konsum anzuregen. Wenn ich auf einer Online-Plattform einkaufe, sagen mir die Algorithmen: Kauf dir dies noch, kauf dir das noch! Auch Tiktok und Meta wollen natürlich ihre Nutzer möglichst lange auf ihren Seiten halten. Diese ganzen Systeme tragen nicht gerade zu mehr Nachhaltigkeit bei. Das kann man aber den Unternehmen nicht unbedingt zum Vorwurf machen – unter den aktuellen Rahmenbedingungen handeln sie einfach rational.

Es gibt also ein strukturelles Nachhaltigkeitsproblem durch unsere Online-Nutzung?

Ja, genau. Wir haben beispielsweise bei der Corona-Pandemie gesehen, dass es durchaus geht, weniger zu reisen. Wir haben durch Videokonferenzen die Dienstreisen und vor allem die Inlandsflüge deutlich reduziert – und das hält noch an. Allerdings machen wir heute in Summe viel mehr Konferenzen.

Ihr Institut hat für den IT-Branchenverband Bitkom untersucht, wie es in Deutschlands Rechenzentren um die Nachhaltigkeit bestellt ist. Sie wollten zum Beispiel wissen, wie wichtig es den Befragten ist, die Abwärme der Server zu nutzen. Insgesamt gab es eine breite Zustimmung, auch wenn nicht alle der Meinung waren.

Dass die Nachhaltigkeit der Rechenzentren weiter erhöht werden soll, ist fast Konsens in der Branche. Allerdings gibt es einen Unterschied zwischen der Absicht und dem tatsächlichen Handeln. Nachhaltigkeit kann schwierig werden, wenn es das eigene Geschäft betrifft und man höhere Kosten hat. Aber das ist überall so, wir sehen das gerade bei den Heizungen. Sobald Nachhaltigkeit wehtun könnte, ist auf einmal die Geschwindigkeit zu hoch.

Wenn die Kosten durch höhere gesetzliche Anforderungen an die Nachhaltigkeit steigen, drohen manche Manager, ins Ausland zu gehen. Ist das ökologische Verantwortungsbewusstsein unterentwickelt?

Was wir brauchen, ist ein Zusammenspiel von unternehmerischem Verantwortungsbewusstsein und wirtschaftlichen Rahmenbedingungen, die Deutschland für Rechenzentren attraktiv machen. Wenn ich nur über die Grenze gehen muss, um meinen Dienst deutlich günstiger anbieten zu können, ist das sogar ›

Nachhaltiger Innovator
Der Maschinenbauer und promovierte Wirtschaftswissenschaftler Ralph Hintemann ist Gesellschafter und Senior Researcher am gemeinnützigen Borderstep Institut für Innovation und Nachhaltigkeit.
Sein besonderes Interesse gilt den Nachhaltigkeitspotenzialen der Digitalisierung.
Im Mittelpunkt seiner Forschung stehen Innovationsstrategien, neue Geschäftsmodelle für Nachhaltigkeitsinnovationen und ihre Erfolgsfaktoren. Zuvor arbeitete er viele Jahre für den Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V., kurz: BITKOM. Er lebt in Berlin und lehrt unter anderem an der Carl von Ossietzky Universität Oldenburg.

nachvollziehbar. Allerdings kann man auch erwarten, dass die Betreibenden von Rechenzentren begreifen, dass sie ihren Teil dazu beitragen müssen, eine nachhaltige Wirtschaft zu schaffen. Mit der Devise „Ich brauche nur Grünstrom, dann bin ich nachhaltig“ kommen wir nicht weiter.

Das kennt man auch aus anderen Zusammenhängen: Wasch mir den Pelz, aber mach mich nicht nass!

Pauschal kann man das nicht sagen. Der Entwurf des Energieeffizienzgesetzes (EnEfG) sieht die Pflicht vor, die Abwärme anzubieten. Das soll auch bei der Standortentscheidung eine Rolle spielen. Aus meiner Sicht ist das zwingend notwendig, wenn Rechenzentren zur Wärmewende beitragen sollen. In der Branche gehen die Meinungen noch auseinander. Einige sagen: „Wo es wirtschaftlich ist, gern, unsere Standorte möchten wir aber nicht danach auswählen.“ Andere wollen genau dahin gehen, wo sie Abnehmer für die Abwärme finden.

Was können denn IT-Anwender aus Industrie, in Banken oder bei Versicherungen zur Nachhaltigkeit beitragen, ohne ihr Geschäftsmodell zu beschädigen? Wie werden sie ihrer Verantwortung im Rahmen des Möglichen gerecht?

Für IT-Verantwortliche mittelständischer oder größerer Unternehmen sind zwei Nachhaltigkeitsthemen wesentlich: die Herstellung und Entsorgung der Geräte und ihr Stromverbrauch. Bei Rechenzentren ist der Verbrauch besonders relevant, schließlich laufen sie 365 Tage 24 Stunden durch.

Aber doch nicht die ganze Zeit auf dem gleichen Niveau, oder? Können sie nicht nach Bedarf heruntergeregelt werden?

Das geht. Bei einem typischen Mittelständler sind die Server nachts und am Wochenende oft nicht ausgelastet. Es wäre technisch möglich, viele dann auszuschalten, aber das wird noch nicht gern gemacht. Da könnte man eine Menge tun. Forschungsrechenzentren und IT-Dienstleister haben natürlich andere Lastkurven. Und Streamingdienste laufen gerade abends und am Wochenende.

Nicht benötigte Systeme außerhalb der Bürozeiten abzuschalten könnte zwei Fliegen mit einer Klappe schlagen: Kriminelle Hacker greifen gezielt dann an, wenn wenig Personal im Dienst ist. Sollte man nachts und am Wochenende vielleicht die eigene IT herunterfahren und nur die Website bei einem Hoster laufen lassen?

Ich bin kein Sicherheitsexperte, aber darüber nachdenken kann man bestimmt. Sicherheit und Nachhaltigkeit – das ist ein sehr ambivalentes Thema. Wenn ich alles verschlüssele und redundant mache, steigt mein Ressourcenbedarf. Andererseits kann ich Ressourcen sparen, wenn mein System so sicher ist, dass ich nicht allzu viele Kopien überall hinlegen muss.

Foto: © Christian Jungeblodt

Füreinander geschaffen? In Norwegen will eine Hummer-Zuchtstätte das auf 20 Grad erwärmte Meerwasser nutzen, mit dem ein benachbartes Rechenzentrum seine Server gekühlt hat.

Foto: AdobeStock

An welchen Stellschrauben kann man am leichtesten drehen, um energieeffizienter zu werden?

Im Rechenzentrum fängt das bei der Software an und geht weiter mit der Hardware, die dazu passen muss. Manche Anwendungen brauchen auf klassischen Prozessoren sehr viel Strom, arbeiten aber mit Unterstützung von Grafikprozessoren sehr effizient. Gerade auch im KI-Bereich ist spezifische Hardware ein ganz relevantes Thema.

Sie meinen Spezialchips für das Machine Learning. Als verbrauchsintensiv gelten auch Blockchains. Diese dezentralen, fälschungssicheren Datenbanken sollen unter anderem Nachweise von Lieferketten erleichtern. Sind herkömmliche Datenbanken nicht viel effizienter?

Das Problem ist das Prinzip „Proof of Work“ …

… also dass die Beteiligten auf ihren Geräten extrem komplexe Rechenaufgaben lösen müssen, um Manipulationen zu verhindern. Das hat dazu geführt, dass Bitcoin und ähnliche Fantasiewährungen praktisch nur noch von großen Playern in hoch spezialisierten Serverfarmen erzeugt werden, die in Billigstromländern stehen.

Da ist eine ganze Industrie entstanden, die nur davon lebt, unsinnig Energie zu verbrauchen. Das Blockchain-Projekt Ethereum hat immerhin gezeigt, dass man es anders machen kann. (*Anmerkung der Redaktion: Die Entwickler-Community ist auf das sogenannte Proof-of-stake-Verfahren umgestiegen, bei dem nicht mehr alle Teilnehmer ständig hohe Rechenleistung bereitstellen müssen, sondern nur noch ausgewählte Teilnehmer sporadisch.*) Ohne Proof of Work ist der Ressourcenverbrauch von Blockchain-Lösungen deutlich geringer. Trotzdem sollte man immer prüfen, ob sich der Einsatz überhaupt lohnt und ob es nicht eine ressourcensparende Alternative gibt.

Die Zeit der Universalrechner ist jedenfalls vorbei. Gilt das auch für Cloud-Anbieter, die Rechenleistung „as a service“ vermarkten? Kann man da schon die jeweils effizienteste Hardware buchen?

Beim Cloud-Anbieter bekomme ich typischerweise eher Standardprodukte. Aber es gibt immer mehr Möglichkeiten, Ressourcen innerhalb des Systems flexibel zuzuteilen.

Zum Beispiel auch Grafikprozessoren dazuschalten?

Ja. Wie man die Systeme künftig noch flexibler machen kann, ist bislang vor allem ein Forschungsthema. Im breiten Markt sind wir noch nicht so weit, dass man ganz nach Bedarf spezifische Hardware-Leistung für spezifische Anwendungen zubuchen könnte. 〉

Neues Bündnis: Im Südwesten Englands heizt Server-Abwärme ein kommunales Schwimmbad. Die Stadt spart mehrere Tausend Pfund Heizkosten.

Brauchen wir also künftig deutlich effizientere IT-Systeme?

Ja, die brauchen wir. Das sieht man gerade bei künstlicher Intelligenz. Bei einem System wie Chat GPT kann der Trainingsprozess enorm aufwendig sein.

Verschlingen solche Anwendungen auch dann noch viel Energie, wenn sie bereits trainiert sind?

Ja. Zum einen werden die Systeme ja laufend neu trainiert. So braucht auch jede Nutzung Energie. Die einzelne Anfrage mag nur wenig Energie benötigen. Wenn es aber eine Milliarde Menschen nutzen, kommt einiges zusammen. Bei diesen großen Sprachmodellen könnte die Nutzung mittlerweile schon der größere Ressourcenfresser sein. Zum Vergleich: Eine E-Mail verursacht nur etwa ein Gramm CO_2, aber wir schreiben in Deutschland am Tag mehr als zwei Milliarden E-Mails. Das sind täglich mehr als 2000 Tonnen CO_2.

Auch Kleinvieh macht Mist. Aber es ist doch ein großer Unterschied, ob ich eine kurze Textnachricht verschicke oder ein zig Megabyte großes PDF. Über Schulungen, wie man ressourceneffizient kommuniziert, könnten große Arbeitgeber ihre Ökobilanz verbessern, oder?

Einige Unternehmen machen das. Aber wenn der Mitarbeiter abends Videos streamt, gehen in einer Stunde drei Gigabyte übers Internet. Bis er bei der Arbeit auf dieses Volumen kommt, kann er viele E-Mails mit derart großen Anhängen schreiben. Dennoch sollte man darauf achten. Am besten wäre es, wenn das automatisch geschieht und er selbst gar nichts tun muss. Beim PDF-Export sollte man in den Standardeinstellungen eine mittlere Auflösung vorgeben. Das E-Mail-Programm könnte Nachrichten auf übergroße Attachments checken, bevor sie rausgehen. Oder die Videostream-Software passt die Auflösung automatisch an die Größe des Displays an.

Viele Menschen wissen nicht viel darüber, was ihre Technik kann und wie man damit umgeht.

Wir haben viel zu wenig Transparenz im Markt. Wo soll ich denn die Information bekommen, welcher Server oder PC wie nachhaltig ist, wie hoch der Ressourcenverbrauch bei seiner Herstellung war? Wo sind die Labels, die einem da helfen? Den Energy Star gibt es in Europa praktisch nicht mehr. Der Blaue Engel ist von der Hardware-Branche nie akzeptiert worden.

Helfen Neuerungen wie die ESG-Compliance (Environmental, Social, Governance) und das Lieferkettengesetz, eine Art Effizienzkultur zu schaffen?

Das Gesetz hat genau den Zweck, da Transparenz hineinzubekommen. Und Unternehmen können durchaus Marktdruck ausüben. Wenn ich als Unternehmen von meinem Cloud-Anbieter wissen möchte, wie viel Energie es verbraucht, was ich bei ihm mache, oder wie viel CO_2 es verursacht, ist die Chance groß, dass er mir das mitteilt. Bei IT-Hardware wissen aber nicht einmal die Hersteller, was in ihren Systemen alles drin ist.

Aus welchen Quellen erfahre ich als Unternehmer denn überhaupt etwas über die Ökobilanz meiner IT-Systeme?

Als Wissenschaftler kennen wir natürlich Studien, die sich damit beschäftigen. Für andere Nutzer ist es nicht einfach, an konkrete Informationen zu kommen. Generell verbrauchen Laptops und Smartphones sehr viel mehr Ressourcen in der Herstellung als im Betrieb. Deshalb ist es sinnvoll, sie lange zu nutzen. Ein Smartphone nach zwei Jahren auszutauschen ist ökologisch einfach nicht vertretbar – es sei denn, die alten Geräte werden weiterverkauft und genutzt. Bei Rechenzentren sieht es anders aus als bei Mobilgeräten, die wegen der Akkulaufzeit darauf getrimmt sind, möglichst wenig Strom zu verbrauchen.

Motto: Ist doch egal, bei uns kommt der Strom aus der Steckdose.

Bei Servern ist das Ziel hohe Leistung. Die Anwendungen erfordern immer mehr Leistung. Durch künstliche Intelligenz kriegen wir wahrscheinlich noch mal einen richtigen Boost bei den Hardware-Anforderungen. Die nächste Chip-Generation für KI-Systeme leistet über 600 Watt. Für einen einzelnen Chip! In einem Server stecken oft mehrere dieser Chips drin und in einem Rack mehrere Server.

Das heißt, da entsteht wiederum viel in Abwärme …

… die aber bislang kaum genutzt wird.

Da könnte bald das EnEfG Wirkung zeigen. Was bedeutet das für „On-Premise“, also hauseigene IT, und für externe wie Cloud oder Co-Location, bei der Dienstleister unter einem Dach mehrere kundeneigene Server betreiben?

Bei On-Premise gibt es meist genug Produktionsanlagen oder Büroräume als Abnehmer für die Wärme. Es gibt bereits jetzt einzelne Firmenstandorte, die gar keine zusätzliche Heizung mehr brauchen. Technisch ist das nicht sehr schwierig, man muss auch keine Fernwärmeleitung bauen. Die großen Cloud- und Co-Location-Anbieter haben typischerweise viel größere Wärmemengen. Sie brauchen einen sehr großen Abnehmer oder ein Fernwärmenetz in der Nähe.

Oder ein Gewächshaus.

Ja, daran wird zum Beispiel in Kanada gearbeitet. In Norddeutschland gibt es ein Rechenzentrum mit einer Algenfarm auf dem Dach. So etwas ist eine Alternative, wenn ich mein Rechenzentrum nicht in der Nähe einer Stadt bauen kann oder es wegen der Grundstückskosten nicht will.

Foto: AdobeStock

Die IT ist nur Dienstleister, nach dem Verursacherprinzip tragen auch Fachabteilungen wie Forschung & Entwicklung oder Marketing zur Schadschöpfung bei. Was können sie tun, um diese zu minimieren?

Da sind wir wieder beim Thema Transparenz. Wir müssten es schaffen, endlich einen Footprint für IT-Dienste zu ermitteln. Keiner weiß genau, was er braucht für das, was er da macht. Erst wenn ich das weiß, kann ich handeln. Dann kann ich auch entscheiden, was umweltfreundlicher ist – der Betrieb in der Cloud oder die eigene Lösung.

Sollte man nicht bei jedem IT-Projekt die Effizienz gleich mitdenken – also nicht nur dafür sorgen, dass eine bestimmte Funktionalität umgesetzt wird, sondern dass sie auch energieeffizient umgesetzt wird?

Ich würde sogar so weit gehen zu sagen: Ein Unternehmen sollte ein Digitalprojekt nur umsetzen, wenn es damit ganz klar seine Nachhaltigkeitsziele unterstützt. Und dabei sollten auch alle möglichen negativen Wirkungen beachtet werden. Das ist sicher nicht einfach – wie der Hype um die Sharing Economy gezeigt hat. Die Online-Plattform Airbnb galt mal als Nachhaltigkeitsprojekt. Oder Free Floating Carsharing: Bisher hat es nicht dazu geführt, dass weniger Autos auf den Straßen sind.

Unser System setzt einfach die falschen Anreize. Womit wir wieder am Anfang wären. Die Digitalisierung kann uns helfen, nachhaltiger zu werden – wir brauchen aber andere Anreize, damit das tatsächlich auch geschieht.

Das Potenzial von Abwärme

Erhitzen sich Server und andere Rechner auf mehr als 100 Grad, arbeiten sie nicht mehr zuverlässig. Frühere Großrechner wurden mit Leitungswasser gekühlt, das anschließend in die Kanalisation floss; die Abwärme blieb ungenutzt. Als sich Server auf Basis von PC-Prozessoren breitmachten, hielt Luftkühlung Einzug in die Data Centers – aber auch die warme Abluft wurde meist per Klimaanlage achtlos ins Freie entsorgt.

Seit einigen Jahren ist Wärmerückgewinnung im Kommen, begünstigt durch neue technische Entwicklungen. So hat eine Renaissance der Wasserkühlung begonnen: Die Prozessoren werden nun in geschlossenen Kreisläufen mit warmem Wasser von etwa 40 Grad gekühlt. Dadurch erreicht das Kühlwasser so hohe Temperaturen, dass sich die Abhitze sehr effizient per Wärmetauscher nutzen lässt. Das Energieeffizienzgesetz (EnEfG), über das der Bundestag berät, hat das Ziel, diese Wärmequelle systematisch anzuzapfen. Die geplanten Vorschriften betreffen insbesondere neue (Cloud-) Rechenzentren, wie sie im Rhein-Main-Gebiet sowie in und um Berlin entstehen. Der Jahresstromverbrauch eines solchen Standortes kann mehr als 100 000 Kilowattstunden beziehungsweise 100 Megawattstunden betragen.

WIRTSCHAFT

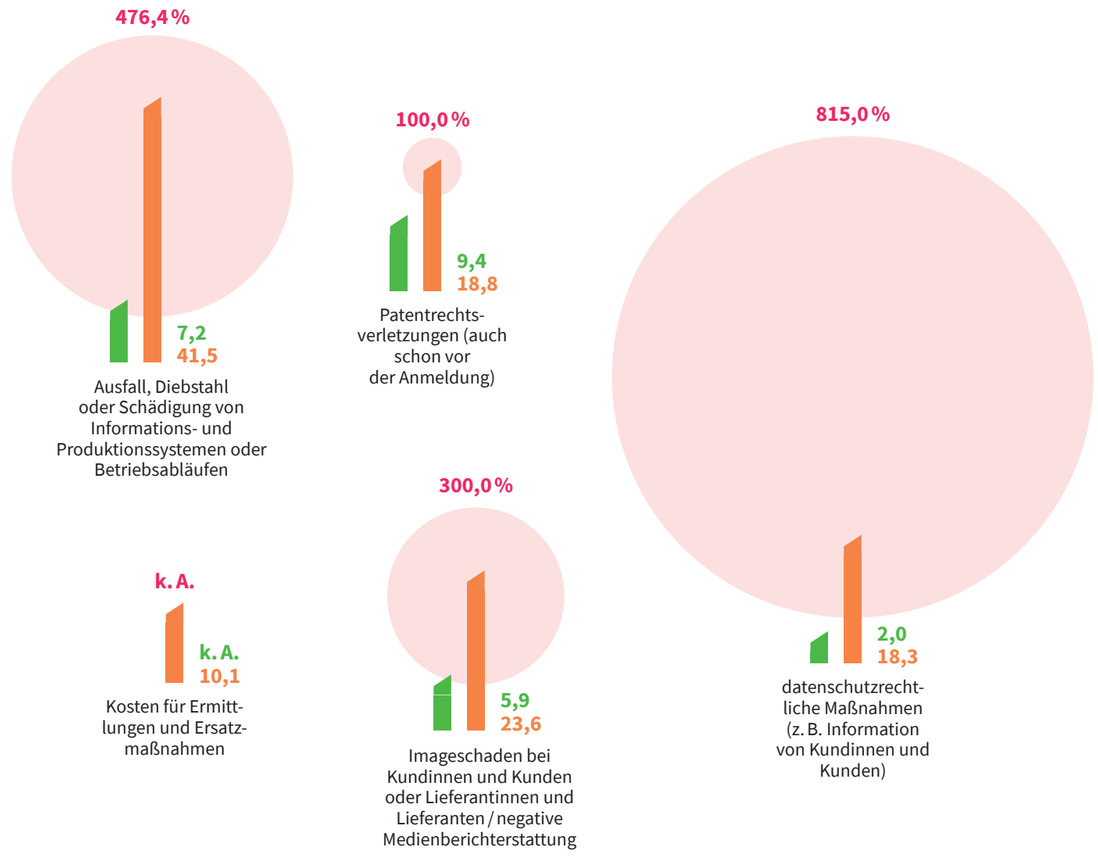
Wer ist im Unternehmen für Cybersecurity verantwortlich? Und wer kennt sich in diesem Feld tatsächlich aus? Wie ernst nehmen wir die Sicherheit unserer Infrastruktur wirklich? Und wie wollen wir uns konkret schützen? Was geben wir für mehr Sicherheit aus? Und wie viel investieren wir – technologisch, inhaltlich und personell?

Die Bedrohung steigt

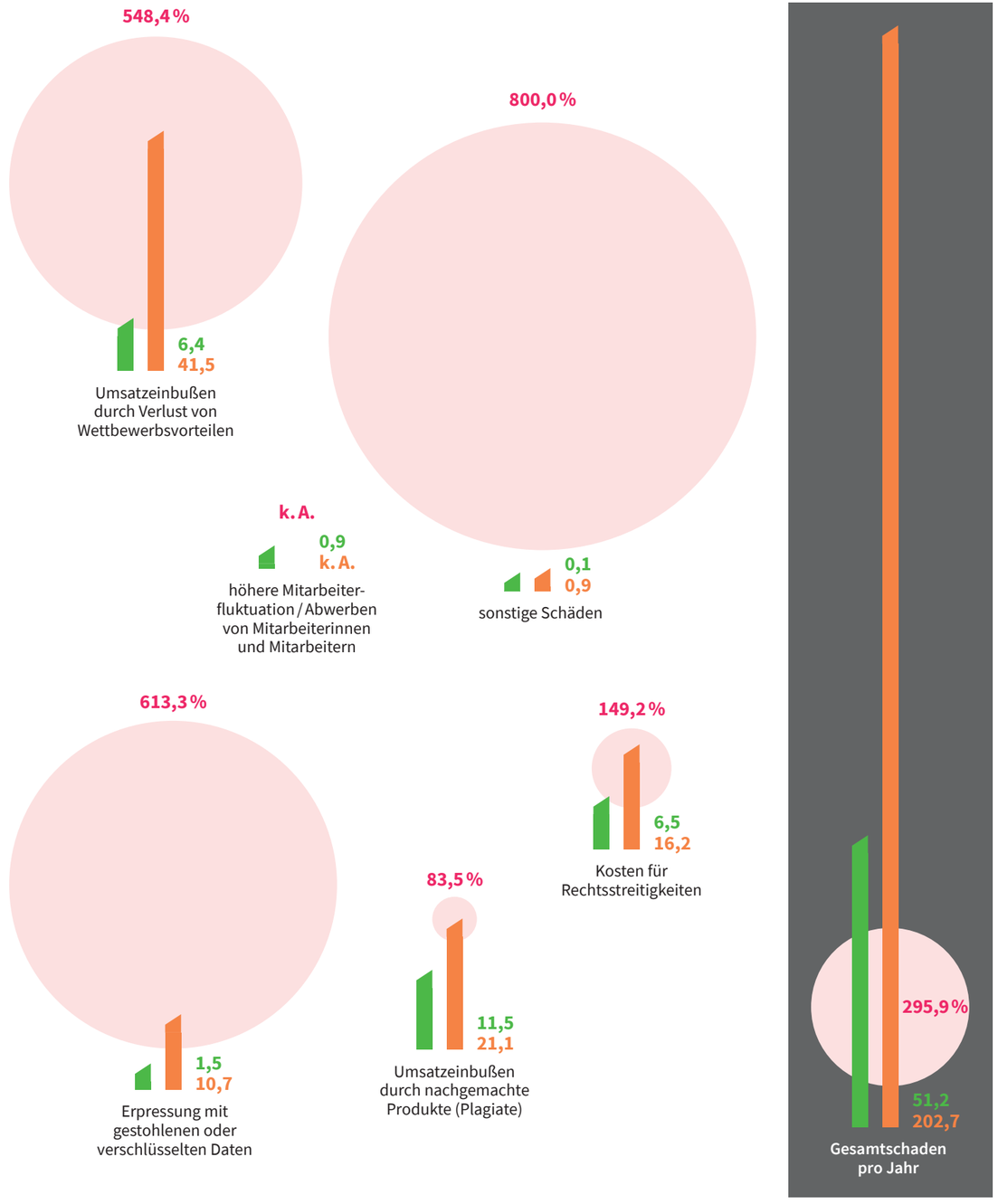
Schaden durch Cyberangriffe nach Delikttyp; Unternehmen, die in den vergangenen zwölf Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (2022: n=899; 2015: n=550); Deutschland; in Milliarden Euro

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

2015 2022 Veränderung 2015 – 2022



Quelle: Bitkom



Glossar der Cyberbegriffe auf Seite 100 – 103

Regelmäßig

Häufigkeit der Durchführung von Schwachstellen-Scans in Großunternehmen (mindestens 2 000 Mitarbeiterinnen und Mitarbeiter); IT-Verantwortliche aus (n=150); Deutschland; 2022; in Prozent

45 täglich

35 wöchentlich

21 monatlich oder ohne Routine

Quelle: techconsult

Anfällig

Herausforderungen im Schwachstellenmanagement in Großunternehmen (mindestens 2 000 Mitarbeiterinnen und Mitarbeiter); IT-Verantwortliche aus Deutschland (n=150); 2022; in Prozent

Mobile Endgeräte und Cloud-Anwendungen sind die größten Herausforderungen im Schwachstellenmanagement. 27

Alle möglichen Schwachstellen in der IT-Infrastruktur sind bekannt. 19

Quelle: techconsult

Mehrgleisig

Hauptverantwortung für Entscheidungen zu Architektur bzw. Produkten für Cyber-Security-Lösungen; Unternehmen ab 50 Mitarbeiterinnen und Mitarbeitern (n=204); Deutschland; 2022; in Prozent

Die Hauptverantwortung liegt …

42 beim Sicherheitsteam

37 sowohl beim Netzwerkteam als auch beim Sicherheitsteam

17 beim Netzwerkteam

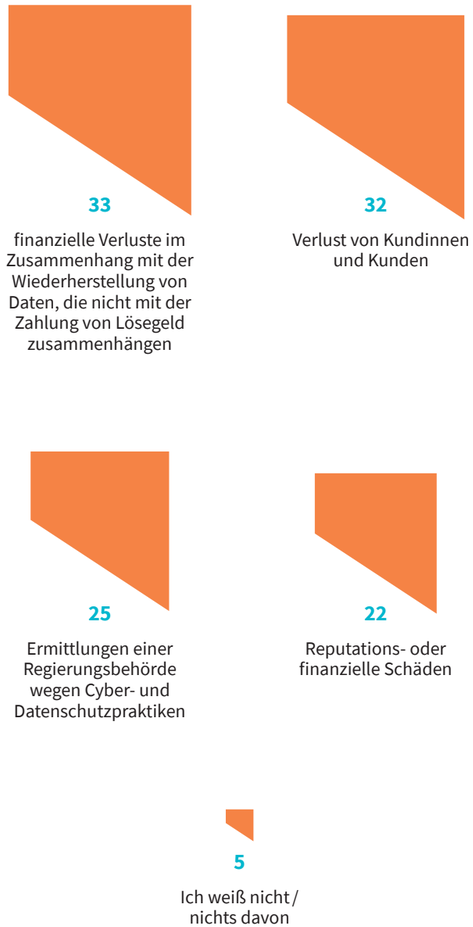
5 bei einem externen Dienstleister

Quellen: techconsult, SEP

Ohnmächtig

Folgen von Datenschutzverletzungen bzw. Datenschutzvorfällen; Chief Marketing Officer aus deutschen Unternehmen (n=63); 2022; in Prozent *

Welche der folgenden Situationen hat Ihre Organisation in den vergangenen drei Jahren aufgrund einer Datenschutzverletzung oder eines Datenschutzvorfalls erlebt?



33 finanzielle Verluste im Zusammenhang mit der Wiederherstellung von Daten, die nicht mit der Zahlung von Lösegeld zusammenhängen

32 Verlust von Kundinnen und Kunden

25 Ermittlungen einer Regierungsbehörde wegen Cyber- und Datenschutzpraktiken

22 Reputations- oder finanzielle Schäden

5 Ich weiß nicht / nichts davon

* Mehrfachnennungen möglich. Quelle: PricewaterhouseCoopers

Investiert

Top-Investitionsbereiche für Security Operations Services und -Maßnahmen; Unternehmen mit mind. 50 Mitarbeiterinnen und Mitarbeitern, die ihre Cyberverteidigung ändern (n=138); DACH-Region; 2022; in Prozent

26 Implementation Security Services

25 Cyber Recovery / Cybervault

22 Security-Schulungen und Awareness-Trainings

21 Notanlaufplan (Runbook)

19 Ransomware Assessments

18 Vulnerability Assessments (Schwachstellenanalysen)

18 Managed Detection & Response (MDR) Services

17 Consulting Security Services

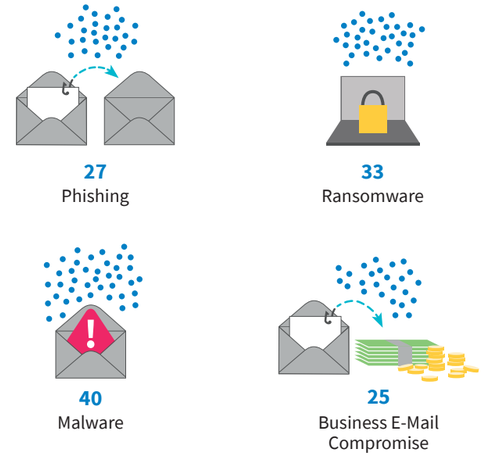
16 Penetration Testing („Pentesting“)

15 Tabletop Exercises (TTX / TTE)

Quelle: IDC

Informiert

Themenabdeckung in Security-Awareness-Trainings; berufstätige Erwachsene (n=4 000) und IT-Sicherheits-Expertinnen und -Experten (n=650) aus 15 Ländern, darunter Deutschland; 2022; in Prozent



27 Phishing

33 Ransomware

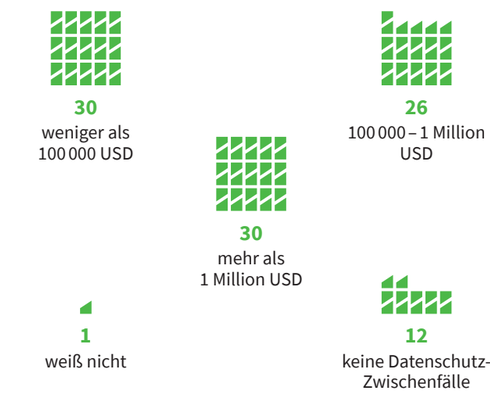
40 Malware

25 Business E-Mail Compromise

Quelle: Proofpoint

Repariert

Geschätzte Kosten der folgenschwersten Datenschutzverletzung in den vergangenen 3 Jahren; CISOs aus Unternehmen (n=76); Deutschland; 2022; in Prozent



30 weniger als 100 000 USD

30 mehr als 1 Million USD

26 100 000 – 1 Million USD

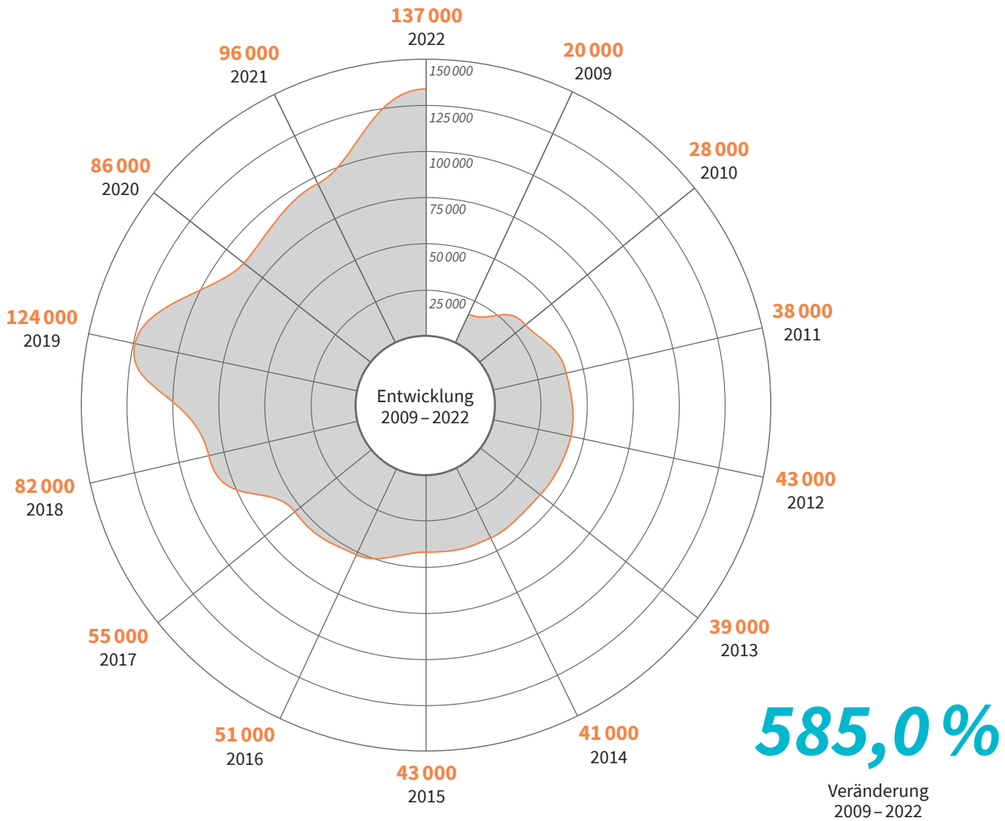
1 weiß nicht

12 keine Datenschutz-Zwischenfälle

Quelle: PricewaterhouseCoopers

Der Bedarf

Entwicklung des IT-Fachkräftebedarfs: Zahl der zu besetzenden IT-Stellen in der Gesamtwirtschaft; Deutschland; in Prozent

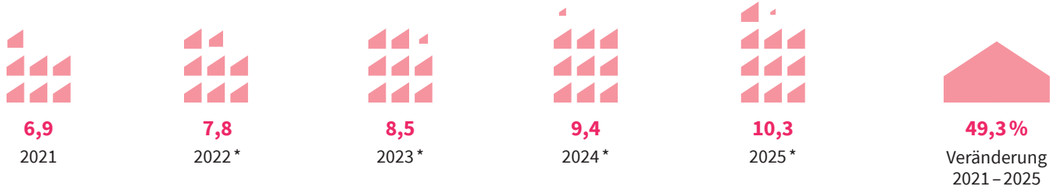


585,0 %
Veränderung
2009 – 2022

Quelle: Bitkom

Die Ausgaben

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

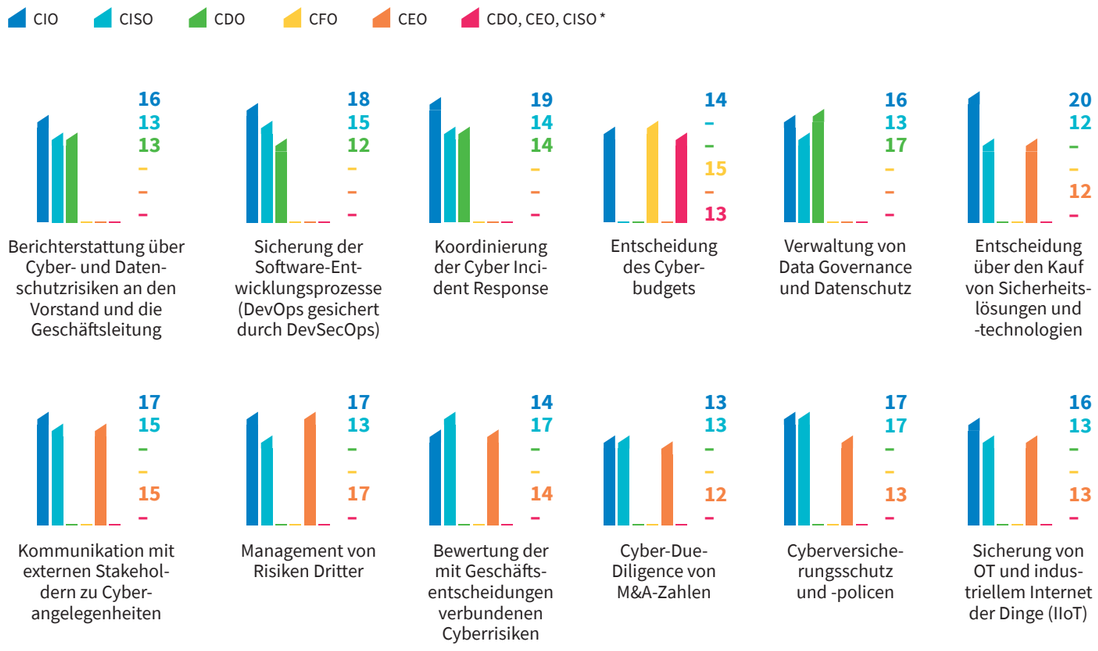


* Prognose. Quelle: Bitkom

Das C-Level

Verantwortung für Bereiche der Cybersicherheit im Unternehmen; Entscheiderinnen und Entscheider aus deutschen Unternehmen (n=242); 2022; Top-3-Werte des jeweiligen Bereichs in Prozent

Wer ist in Ihrer Organisation in erster Linie für jeden der folgenden Bereiche der Cybersicherheit verantwortlich?



* CIO: Chief Information Officer / CISO: Chief Information Security Officer / CDO: Chief Digital Officer (früher auch Chief Data Officer) / CFO: Chief Financial Officer / CEO: Chief Executive Officer. Quelle: PricewaterhouseCoopers

Die Politik

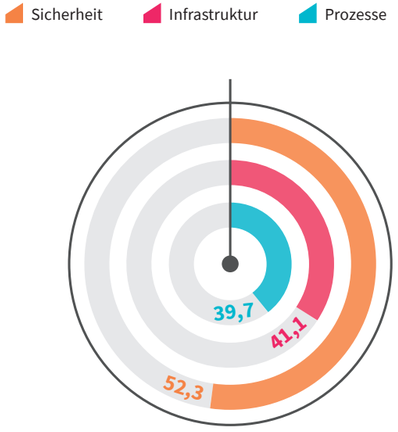
Bewertung von Aussagen zu politischen Debatten im Bereich Wirtschaftsschutz; Unternehmen in Deutschland mit mindestens 10 Mitarbeiterinnen und Mitarbeitern und einem Jahresumsatz von 1 Million Euro oder mehr (n=1 066); 2022; Prozentwerte für „Ich stimme voll und ganz zu“ und „Ich stimme eher zu“.

Quelle: Bitkom

Priorisiert

IT-Investments der kommenden drei Jahre; oberste (IT-)Verantwortliche von Unternehmen (n=323); DACH-Region; 2022; in Prozent *

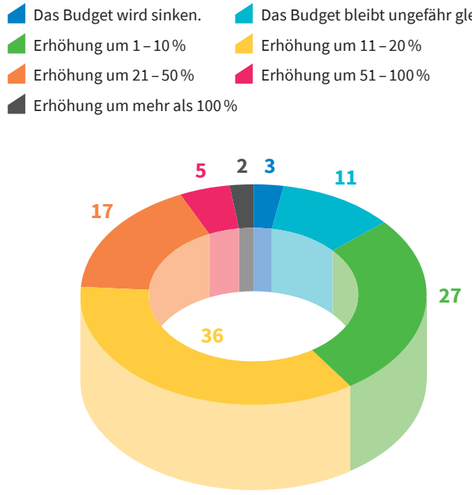
In welchen Bereichen wollen Sie in den kommenden drei Jahren substanzielle IT-Investments tätigen?



* Mehrfachnennungen möglich. Quellen: CIO, CSO, COMPUTERWOCHE

Budgetiert

Budget-Entwicklung für Cybersecurity in den kommenden zwei Jahren; Unternehmen ab 50 Mitarbeiterinnen und Mitarbeitern (n=196); Deutschland; 2022; in Prozent



Quelle: techconsult

Identifiziert

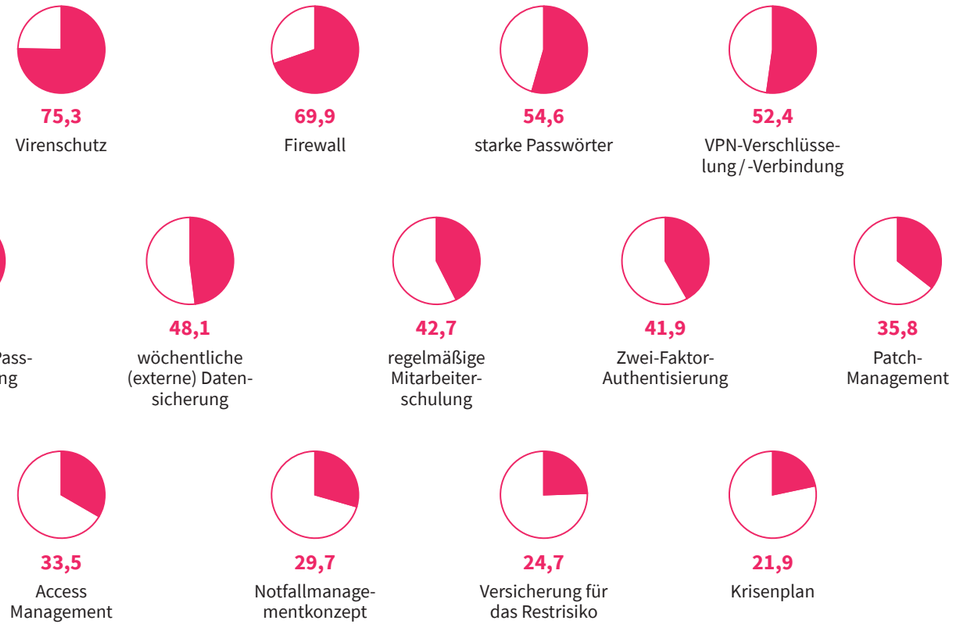
Themen zukünftiger IT-Security-Strategien; Unternehmen ab 50 Mitarbeiterinnen und Mitarbeitern (n=204); Deutschland; 2022; Prozentwerte für „sehr wichtig“ und „wichtig“

Identity & Access Management (IAM)	81
Datenschutz	77
Datenintegrität	75
sicherer Zugang zu Anwendungen in der (Public) Cloud	75
Endpunkt & Mobile Management	75
Netzwerkzugangskontrolle (NAC)	75
Datensicherheit / Disaster Recovery	75
Datenverschlüsselung	75
Data Loss Prevention (DLP)	74
Vereinfachung der Bereitstellung von sicheren Zugriffen	71
Einhaltung von Compliance-Vorgaben, DSGVO	69
Etablierung eines Zero-Trust-Sicherheitskonzeptes	68
Einführung einer Secure Access Service Edge (SASE) Architektur	68
Erweitern / Ersetzen bestehender Tools für den Fernzugriff	64

Quellen: techconsult, SEP

Realisiert

Umgesetzte Schutzmaßnahmen gegen Cyberrisiken; Vertreterinnen und Vertreter deutscher mittelständischer Unternehmen (n=511); Deutschland; 2022; in Prozent *



* Mehrfachnennungen möglich. Quelle: CyberDirekt

Implementiert

Maßnahmen zur Reduktion zukünftiger Cyberbedrohungen; Unternehmen ab 50 Mitarbeiterinnen und Mitarbeitern (n=204); Deutschland; 2022; in Prozent *

* Mehrfachnennungen möglich. Quellen: techconsult, SEP

Punktuell erwünscht

Gewünschte Unterstützung beim Thema IT-Sicherheit; Digitalisierungsumfrage in Unternehmen (n=4 000+); Deutschland; 2022; in Prozent *

40 rechtliche Hinweise

39 organisatorische Unterstützung / Prozessunterstützung

24 Infos zu technischer Prävention

18 Möglichkeit einer aktiven Teilnahme an einem Netzwerk zu mehr IT-Sicherheit

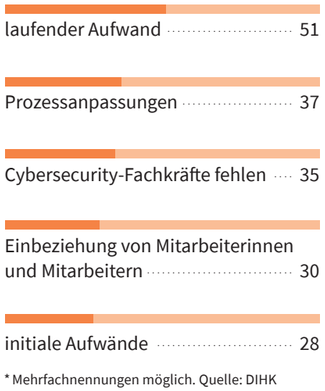
13 „Ich bin von Initiativen / Organisationen informiert, aber mir fehlt das umsetzbare Ergebnis."

25 „Mein Unternehmen benötigt keine Unterstützung."

* Mehrfachnennungen möglich. Quelle: DIHK

Gebremst?

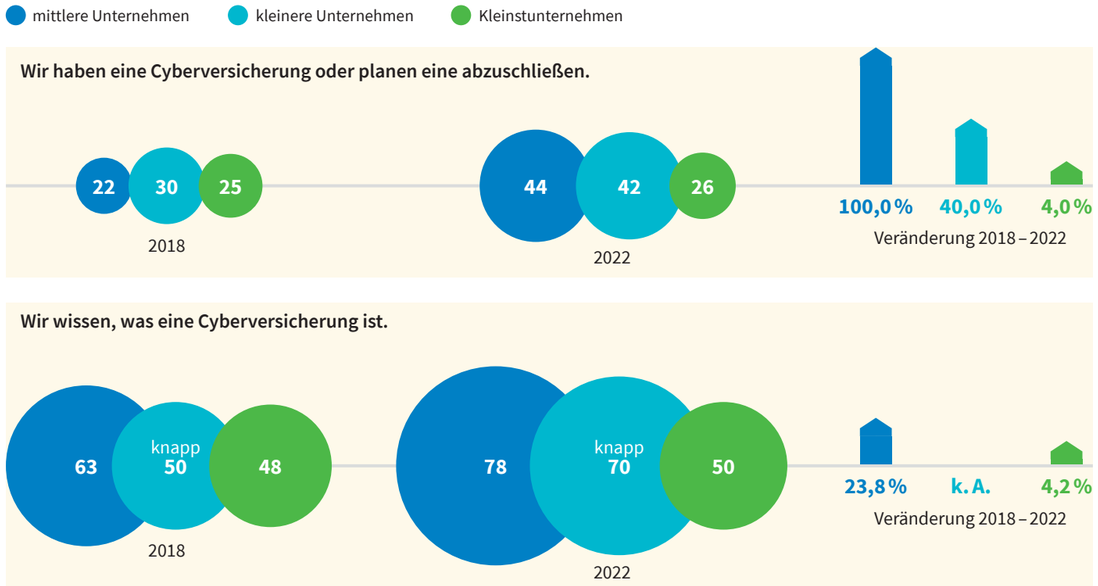
IT-Sicherheitsbremsen im Unternehmen; Digitalisierungsumfrage in Unternehmen (n=4 000+); Deutschland; 2022; in Prozent *



* Mehrfachnennungen möglich. Quelle: DIHK

Mäßig interessiert

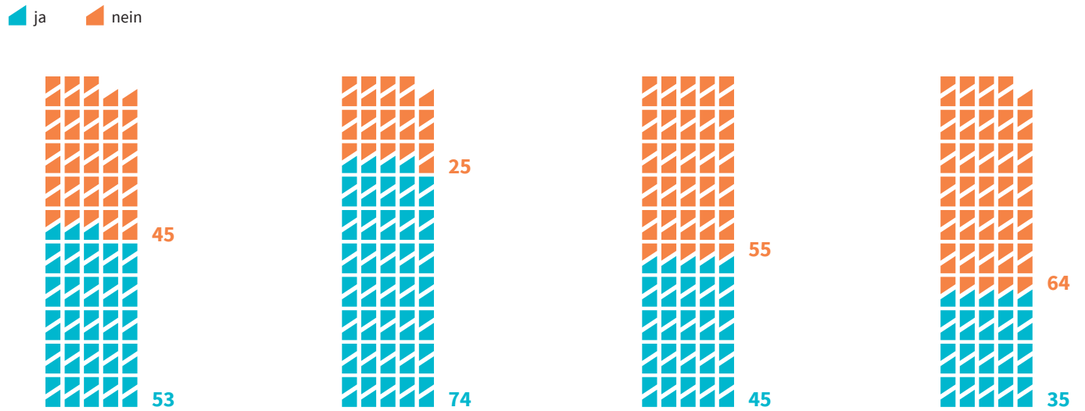
Interesse an Cyberversicherungen; Entscheiderinnen und Entscheider in kleinen und mittleren Unternehmen *; Deutschland; in Prozent



* Kleinstunternehmen: bis 9 Mitarbeiter, bis 2 Millionen Umsatz; kleine Unternehmen: 10–49 Mitarbeiter, 2–10 Millionen Euro Umsatz; mittlere Unternehmen: 50–249 Mitarbeiter, 10–50 Millionen Euro Umsatz. Quelle: GDV

Geschützt?

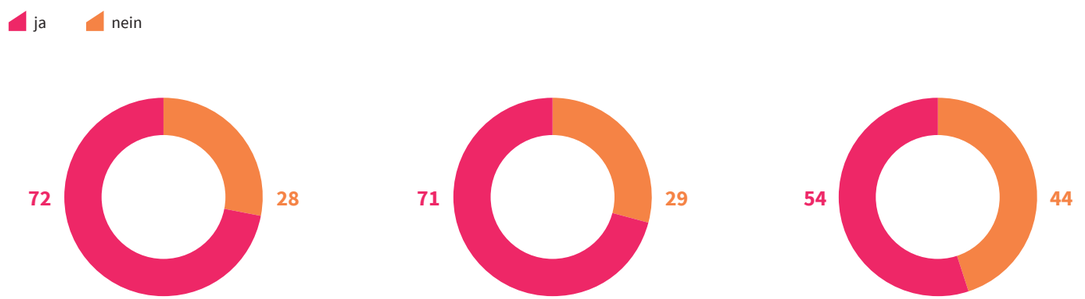
Wichtigkeit von Cybersicherheit in kleinen und mittleren Unternehmen; Entscheiderinnen und Entscheider in kleinen und mittleren Unternehmen (n=300); Deutschland; 2022; in Prozent



Quelle: GDV

Gesichert?

Datensicherung in Unternehmen; Entscheiderinnen und Entscheider in kleinen und mittleren Unternehmen (n=300); Deutschland; 2022; in Prozent



Quelle: GDV

Maßnahmen

Technische Maßnahmen / Lösungen für die Sicherstellung der Cybersecurity; Unternehmen ab 50 Mitarbeiterinnen und Mitarbeitern (n=204); Deutschland; 2022; in Prozent *

49 Antiviren-Lösungen und Malware-Erkennung	41 Paketfilter-/ Proxy-Firewall	38 Datensicherungs-, Backup- und Wiederherstellungslösungen	38 Verschlüsselung von Daten und Transportwegen	32 Nutzerprofile und Nutzer-/ Gruppenrichtlinien
31 Next Generation Firewall (NGF)	30 Multi-Factor Authentication	25 Threat Monitoring	24 Systemmonitoring, Logging und Reporting	23 Data Loss Prevention (DLP)
23 Verzeichnisdienste und Identitäts-management	20 Netzwerkzugangs-kontrolle (NAC)	18 Threat Analytics	18 Endpoint Security	18 Intrusion Detection & Prevention (IDS/ IPS)
18 (Distributed) Denial of Service Prevention (DoS/ DDoS)	18 automatisierte Schwachstellen-Scans	17 Security Information and Event Management (SIEM)	16 Zero Trust Network Access (ZTNA)	11 Unified Threat Management (UTM)

* Mehrfachnennungen möglich. Quelle: techconsult

Herausforderungen

Top-10-Security-Herausforderungen; Unternehmen mit mind. 50 Mitarbeiterinnen und Mitarbeitern (n=306); DACH-Region; 2022; in Prozent *

Sicherheitskomplexität	27
Datenschutz / Privacy	21
Cybersecurity-Personal- / Fachkräftemangel	19
Sicherheit von vernetzten Umgebungen	18
Integration und Rationalisierung	17
Phishing oder Advanced Persistent Threats (APT)	17
Ransomware-Attacken	15
unklare Prozesse im Disaster Recovery / bei Cyberattacke	14
konsistente Security-Maßnahmen lokal und in der Cloud	13
Budgetmangel für Security-Investitionen	13

* Maximal drei Antworten pro Studienteilnehmer. Quelle: IDC

Einschätzungen

Bewertung von Aussagen zur IT-Sicherheit; Logistikunternehmen ab 20 Mitarbeiterinnen und Mitarbeitern (n=404); Deutschland; 2022; Prozentwerte für „Trifft voll und ganz zu“ und „Trifft eher zu“

IT-Sicherheit ist in unserem Unternehmen auch auf Vorstands- bzw. Geschäftsführungsebene verankert.	88
Wir pflegen hohe IT-Sicherheitsstandards in unserem Unternehmen.	80
Wir schulen unsere Mitarbeiterinnen und Mitarbeiter regelmäßig zum Thema IT-Sicherheit.	69
Wir führen regelmäßige Sicherheits-Audits durch.	63
Vor dem Hintergrund des russischen Angriffs auf die Ukraine haben wir unsere Maßnahmen zur IT-Sicherheit verschärft.	51

Quelle: Bitkom

Verantwortungen

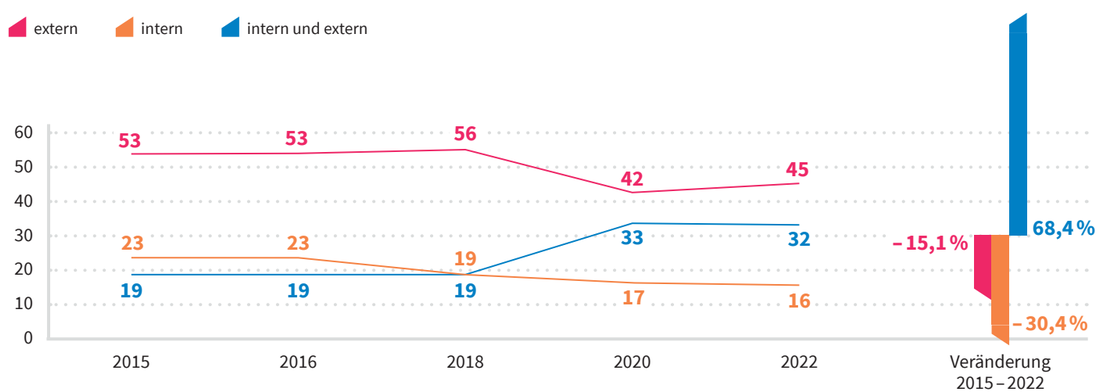
Anteil an Security-Entscheiderinnen und -Entscheidern nach Arbeitsposition; oberste (IT-)Verantwortliche von Unternehmen (n=323); DACH-Region; 2022; in Prozent

43 CIO / CDO / IT-Vorstände	41 CEO / Geschäfts-führung	36 IT-Leitung	32 CISO

Quellen: CIO, CSO und Computerwoche

Zuständigkeiten

Externe vs. interne Erledigung von IT-Aufgaben; Deutschland; in Prozent

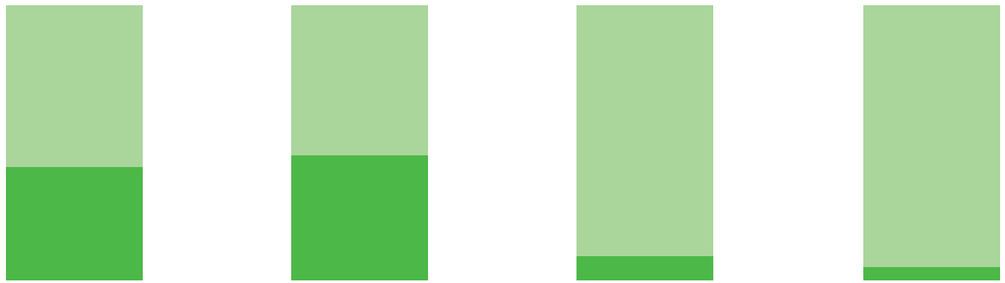


Quelle: Destatis

Cloud-Planungen?

Cloud-Investitionen in den nächsten 3 Jahren; oberste (IT-)Verantwortliche von Unternehmen (n=323); DACH-Region; 2022; in Prozent

Planen Sie in den nächsten drei Jahren in Cloud-Technologien und -Services zu investieren?

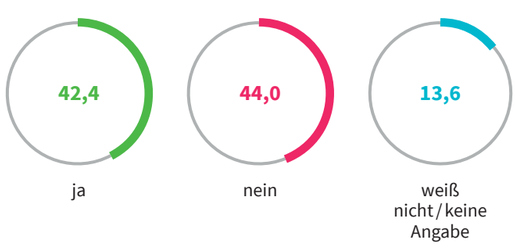


Quellen: CIO, CSO und Computerwoche

Cloud-Zielscheiben?

Cloud-Services als Ziel eines Cyberangriffs; oberste (IT-)Verantwortliche von Unternehmen (n=323); DACH-Region; 2022; in Prozent

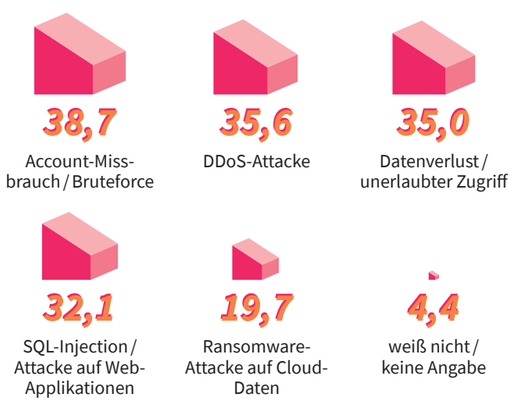
Waren die von Ihrem Unternehmen genutzten Cloud-Services schon einmal Ziel eines Cyberangriffs?



Quellen: CIO, CSO und Computerwoche

Cloud-Angriffe?

Art des Cyberangriffs auf genutzte Cloud-Services: Unternehmen, deren Cloud-Services schon einmal Ziel eines Cyberangriffs waren (n=137); DACH-Region; 2022; in Prozent *



* Mehrfachnennungen möglich. Quellen: CIO, CSO und Computerwoche

Was stimmt?

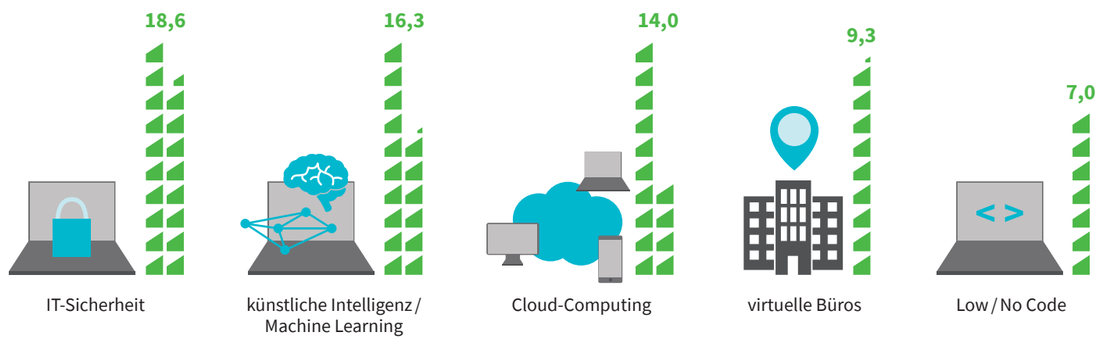
Stellenwert von Cybersicherheit; Unternehmen ab 50 Mitarbeiterinnen und Mitarbeiter (n=204); Deutschland; 2022; Prozentwerte für „Stimme zu“ und „Stimme voll zu“

Quellen: techconsult, SEP

Was ist in?

Top-5-Digital-Trends im Jahr 2023; mittelständische Unternehmen (n=34); Deutschland; 2022; in Prozent

Welcher Digital-Trend bestimmt das Jahr 2023?

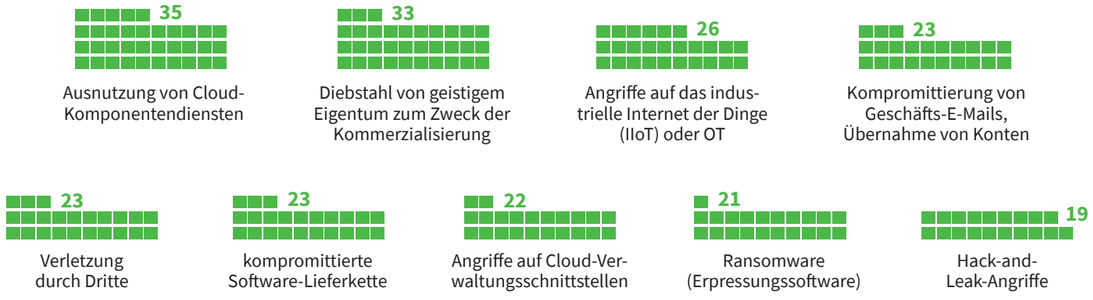


Quelle: bitmi

Damit rechnen wir

Erwartete Zunahme von Angriffsarten; Entscheiderinnen und Entscheider aus Unternehmen (n=242); Deutschland; 2022; in Prozent

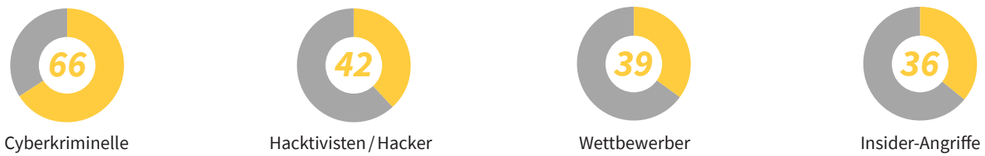
Angriffe, für die auf das eigene Unternehmen im Jahr 2023 im Vergleich zu 2022 eine deutliche Zunahme erwartet wird:



Quelle: PricewaterhouseCoopers

Das befürchten wir

Bedrohung durch Angriffsakteure; Führungskräfte aus dem Wirtschafts- und Technologie-Umfeld (n=231); Deutschland; 2022; in Prozent *



* Mehrfachnennungen möglich. Quelle: PricewaterhouseCoopers

Das registrieren wir

Zahl neuer Schadprogramm-Varianten *; Deutschland

	2020	2021	2022	Veränderung 2020 – 2022
pro Jahr	117,4 Mio.	144 Mio.	116,6 Mio.	– 0,7 %
pro Tag	322 000	394 000	320 000	– 0,6 %

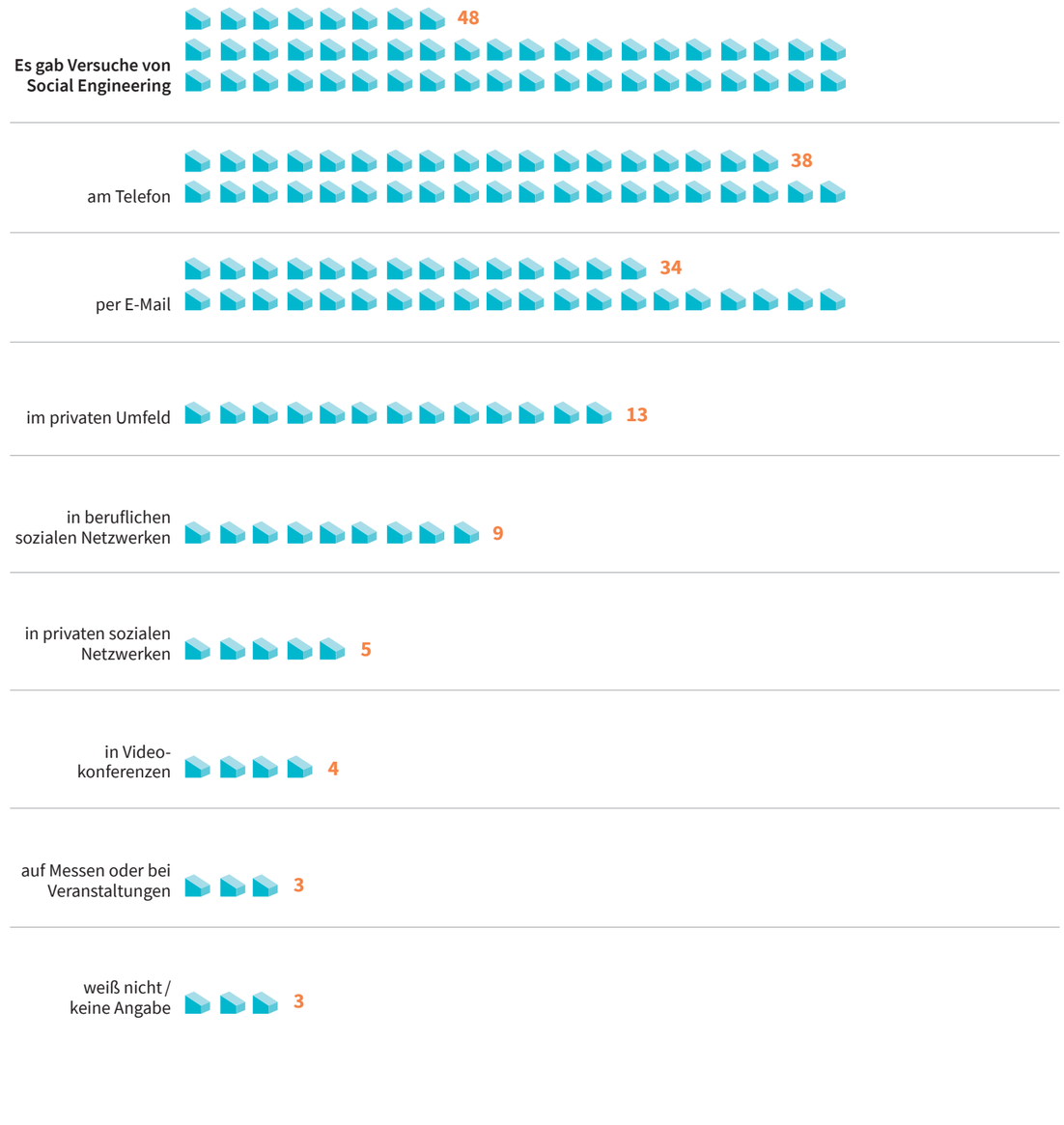
* Die Berichtszeiträume erstrecken sich vom 1. Juni des vorherigen Jahres bis zum 31. Mai des erwähnten Jahres. Quelle: BSI

Hinweis: Trotz der rückläufigen Zahlen ist es um die IT-Sicherheit in Deutschland schlecht bestellt. Denn Angreifer nutzen konsequent Sicherheitslücken aus, um Firmen zu kompromittieren. Auch unaufmerksame Mitarbeiterinnen und Mitarbeiter öffnen immer wieder Cyberkriminellen die Tür ins Netzwerk, wenn sie auf Phishing-Mails hereinfallen und Anhänge mit Schadcode öffnen oder Zugangsdaten auf gefälschten Webseiten preisgeben. Hier besteht bei vielen Unternehmen noch Nachholbedarf – sowohl bei technologischen Schutzmaßnahmen als auch beim Thema Security Awareness. Quelle: G DATA CyberDefense AG

Das erleben wir

Social Engineering als Cybercrime-Methode; Unternehmen (n=1 066; Deutschland; 2022; in Prozent *

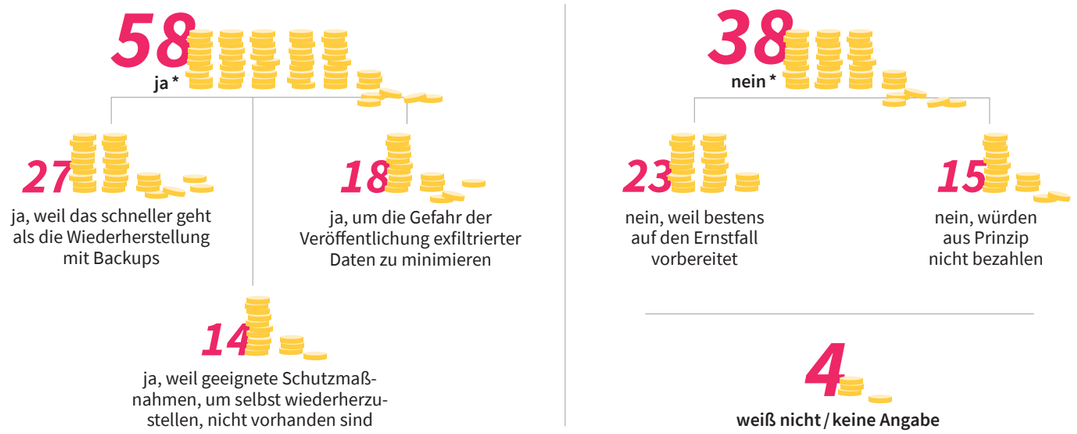
In welchen der folgenden Kontexte gab es innerhalb der vergangenen 12 Monate Versuche, Ihre Mitarbeiterinnen und Mitarbeiter mittels Social Engineering zu beeinflussen?



* Mehrfachnennungen möglich. Quelle: Bitkom

Erpressbar

Bereitschaft zur Bezahlung bei Ransomware-Attacken; Unternehmen mit mindestens 50 Mitarbeiterinnen und Mitarbeitern (n=306); DACH-Region; 2022; in Prozent

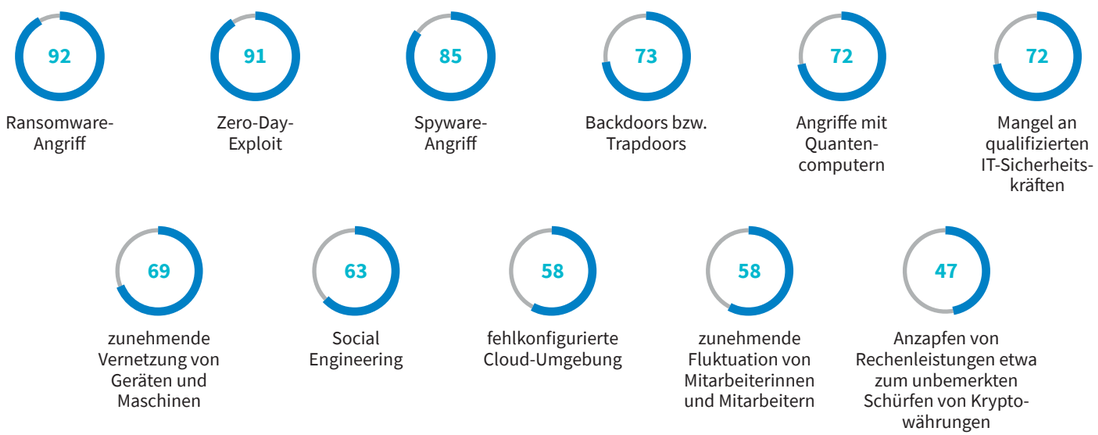


* Ja steht für die Bereitschaft zu bezahlen oder den Umstand, dass bereits bezahlt wurde. ** Nein steht für die Tatsache, dass entweder nicht bezahlt wurde oder man nicht bezahlen würde. Quelle: IDC

Absehbar

Zukünftige Bedrohungen für die IT-Sicherheit in Unternehmen; Führungskräfte, die für das Thema Wirtschaftsschutz verantwortlich sind (n=1 066); Deutschland; 2022; Prozentwerte für „sehr bedrohlich“ & „eher bedrohlich“.

Inwieweit betrachten Sie die folgenden Szenarien als zukünftige Bedrohung für die IT-Sicherheit Ihres Unternehmens?

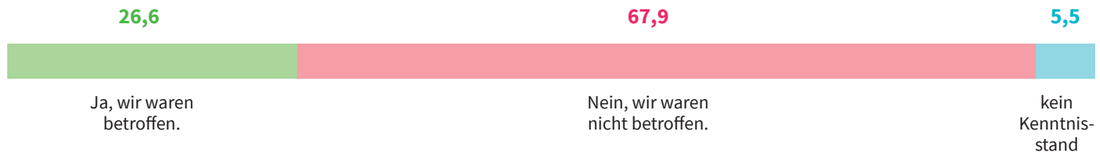


Quelle: Bitkom

Unwägbar

Erfolgreiche Cyberangriffe auf Unternehmen; Vertreterinnen und Vertreter mittelständischer Unternehmen aus den Branchen E-Commerce, Handel, Baugewerbe, Dienstleistungen und IT (n=511); Deutschland; 2021; in Prozent

Hat es in den vergangenen zwei Jahren erfolgreiche Cyberangriffe auf Ihr Unternehmen gegeben?

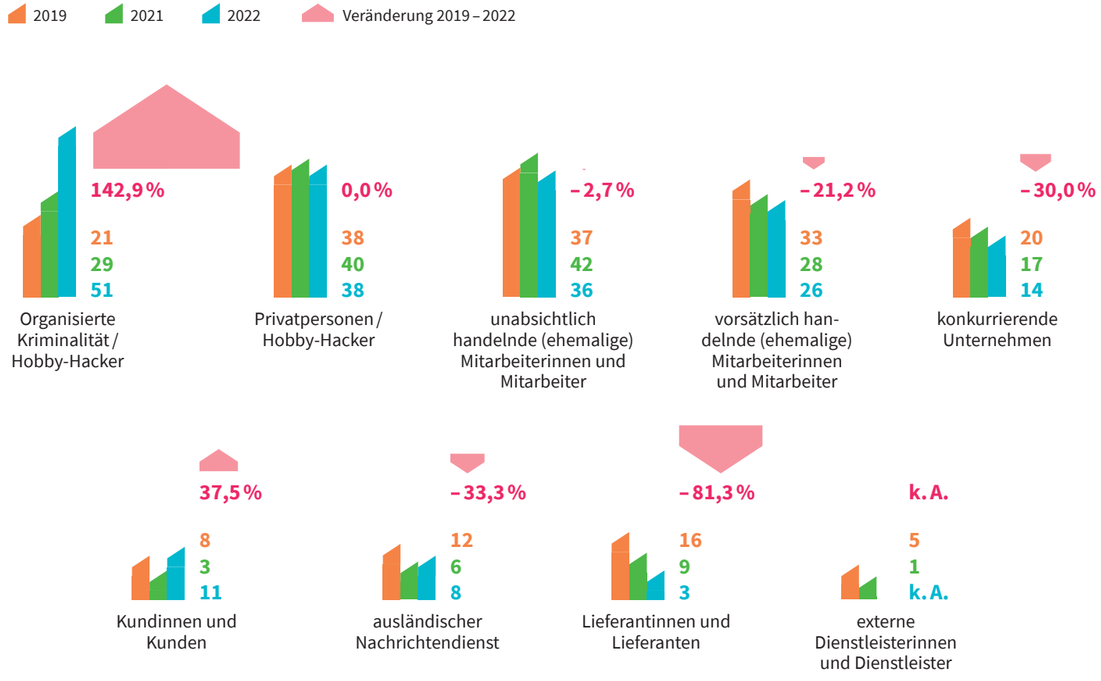


Quelle: CyberDirekt

Identifizierbar

IT-Angriffe auf Unternehmen nach Täterkreis; Unternehmen mit mindestens 10 Mitarbeiterinnen und Mitarbeitern und einem Jahresumsatz von 1 Million Euro oder mehr (n=1 066); Deutschland; in Prozent

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



Quelle: Bitkom

Und jetzt?

Foto: AdobeStock

Langfristig bietet künstliche Intelligenz viele Chancen für eine bessere Zukunft. Kurzfristig wird sie jedoch zum Problem für die Sicherheit elektronischer Systeme. Wie lösen wir es? Und wie kommen wir bis dahin klar?

Text: Peter Lau

Die Zukunft hat begonnen. Sie heißt künstliche Intelligenz (KI) und sorgt seit Monaten für optimistische, bizarre, beunruhigende, erstaunliche und vor allem spektakuläre Nachrichten. Die vielen neuen Möglichkeiten der Technologie sind noch lange nicht absehbar. Klar ist nur: Sie wird etliche gesellschaftliche Grundlagen verändern – wie wir arbeiten, lernen, uns organisieren, wie wir leben. Diese Veränderungen erleben wir schon sehr bald, zuallererst in der Wirtschaft, wo sich KI schon seit einiger Zeit rasend schnell verbreitet. Unternehmen nutzen selbstlernende Systeme in der Produktion, Verwaltung, Logistik, zur Planung, als persönliche Assistenz. Ein Ende der Entwicklung ist nicht vorhersehbar. Denn es gilt dieselbe Regel wie bei jeder erfolgreichen neuen Technologie: Ist sie endlich alltagsreif, investieren alle gleichzeitig und beschleunigen damit ihre Entwicklung enorm.

Was wie eine plötzliche Explosion der Möglichkeiten aussieht, ist tatsächlich das Ergebnis eines langen Prozesses. Schon 1950 entwickelte der britische Mathematiker Alan Turing in seinem Artikel „Computing Machinery and Intelligence“ die Idee eines universalen, intelligenten Computers. Nur sechs Jahre später wurde auf der Dartmouth-Konferenz, die von den damals wichtigsten IT-Pionieren organisiert worden war, das Forschungsgebiet KI definiert. Heute gelten neuronale Netze und Selbstverbesserung als revolutionär, tatsächlich standen sie schon damals auf dem Programm.

Die Technologie blieb jedoch lange weit hinter der Theorie zurück. Insbesondere Künstliche Neuronale Netzwerke (KNN), die von biologischen neuronalen Netzen wie dem Gehirn inspiriert sind, schienen lange nicht praktikabel. Erst in den Achtzigerjahren wurde die Grundlage für die gewaltigen ›

Fortschritte seit etwa 2010 geschaffen, die schließlich zum sogenannten Deep Learning führten: Maschinen lernen jenseits algorithmischer, regelbasierter Systeme selbstständig und können sich weiterentwickeln, was zu großen Durchbrüchen bei der maschinellen Übersetzung sowie bei Bild- und Spracherkennung geführt hat. Parallel entwickelte sich die generative KI, die auf der Basis von Wahrscheinlichkeiten selbstständig Bilder (Midjourney) oder Texte (ChatGPT) produziert.

Die Angst vor der neuen Intelligenz

Beide Modelle vervielfachten die Möglichkeiten künstlicher Intelligenz enorm, aber auch die Angst vor ihr. Viele Menschen sorgen sich wegen möglicher ökonomischer Probleme, etwa davor, ihren Arbeitsplatz zu verlieren. Andere haben Angst vor massenhaften Manipulationen per Deepfake. Einige fürchten gar eine „KI-Apokalypse".

Nick Bostrom, Philosoph und Gründer des Future of Humanity Institute an der University of Oxford, hat das Konzept des „existenziellen Risikos" von KI entwickelt: Ihr Tun könnte unbeabsichtigte Konsequenzen haben und die Menschheit bedrohen. Anfang 2023 thematisierte ein offener Brief in den USA diese Endzeittheorie. „Sollen wir es hinnehmen, dass ‚nicht-menschliche Intelligenzen' entstehen, die uns irgendwann überflüssig machen und ersetzen könnten?", hieß es in dem Schreiben, das unter anderen vom Hightech-Milliardär Elon Musk und Apple-Mitbegründer Steve Wozniak unterzeichnet wurde. Sie forderten, die Entwicklung von KI für eine kurze Zeit auszusetzen, um klare Regeln für den Umgang mit der Technologie zu erarbeiten.

Nach klaren Regeln fragen auch große Tech-Unternehmen und die Vorreiter in Sachen künstlicher Intelligenz: OpenAI, IBM, Microsoft, Google. Sam Altman, CEO von OpenAI, und der renommierte KI-Forscher Gary Marcus schlugen dem US-Kongress in einer Anhörung gar vor, eine Art internationale Behörde für künstliche Intelligenz – vergleichbar mit der International Atomic Energy Agency (IAEA) für Atomenergie oder dem CERN für Hochenergiephysik – zu gründen.

Die Frage ist also längst nicht mehr ob, sondern wie reguliert wird. Die USA setzten bislang auf eigene Maßnahmen der Entwickler und eher allgemeine Regeln wie den California Consumer Privacy Act und dessen Erweiterung, den California Privacy Rights Act („CPRA"), der die Daten der Verbraucherinnen und Verbraucher schützen soll, auch vor KI. Inzwischen will auch die US-Regierung konkretere Gesetze erarbeiten – und dabei mit der Europäische Union zusammenarbeiten.

Die EU ist nämlich einen Schritt weiter und hat einen Gesetzesentwurf vorgelegt, den EU AI Act. Kern der Vorlage ist eine Risikobewertung, auf deren Grundlage KI-Anwendungen erlaubt (minimales bis großes Risiko) oder verboten (unannehmbares Risiko) werden sollen. Eine Bedingung für alle Anwendungen: Transparenz. Den Nutzerinnen und Nutzern muss bewusst gemacht werden, dass sie eine KI nutzen.

Chancen auf eine gerechtere Welt

Wie die Regeln im Detail aussehen werden, ist noch nicht abzusehen. Auch nicht, ob und inwiefern sie die Wettbewerbsfähigkeit betroffener Unternehmen schmälern könnten. Klar ist: Langfristig kann KI nur durch internationale Abkommen reguliert werden. Schließlich wird auch in anderen Teilen der Welt die Technologie weiterentwickelt – vor allem in Asien.

Dort stehen den Bedenkenträgern aus der westlichen Welt Millionen, wenn nicht Milliarden Menschen wie Vijayalakshmi aus dem indischen Bangalore gegenüber. Sie verdient als Köchin 100 Dollar im Monat, spricht kein Englisch und nutzt nur die nötigsten Funktionen ihres Handys. Trotzdem hat sie kürzlich mit KI-Technologie experimentiert. Sie stellte einem Bot in ihrer Muttersprache Kannada Fragen zu Bildungsstipendien für ihren 15-jährigen Sohn, der Bot antwortete Augenblicke später mit einer menschlichen Stimme. Normalerweise hätte sie, um an diese Informationen zu kommen, Mittelsmänner teuer bezahlen müssen.

Die KI, die ihr geholfen hat, übersetzt mehrere der mehr als 100 lokalen Sprachen in Indien. Sie wurde von OpenNyAI entwickelt. Die indische NGO hat sich explizit der Förderung der Gerechtigkeit durch künstliche Intelligenz verschrieben – und liegt damit auf Regierungslinie. Während in den westlichen Industrieländern an Regulierungen gearbeitet wird, blickt man in Indien vor allem auf die Chancen: Künstliche Intelligenz gilt als ein Werkzeug, mit dem Sprachbarrieren abgebaut, mehr Bildung verbreitet und kulturelle Unterschiede überwunden werden können. Dazu passt, was Microsoft-CEO Natya Nadella – ein gebürtiger Inder – auf dem World Economic Forum 2023 sagte: „Wir warten immer noch darauf, dass in großen Teilen der Welt nach 250 Jahren die industrielle Revolution endlich ankommt." Er glaubt daran, dass KI diesen Nachholbedarf stillen könnte. Und steht mit diesem Glauben nicht allein.

Fast unbemerkt hat sich zwischen reichen und armen Ländern ein KI-Kulturkampf entwickelt: zwischen denjenigen, die viel zu verlieren haben – und den anderen. Es ist ein Disput, der vor allem in der Praxis, in Projekten und Anwendungen, ausgetragen wird. Denn im Gegensatz zu klassischen Produktionsmitteln ist KI eine niedrigschwellige Technologie: Existiert erst mal die Infrastruktur, braucht es vor allem Ideen. 〉

Foto: Start Digital

Foto: AdobeStock

Künstliche Intelligenz ist eine Technologie mit Schwächen. Doch im Moment ist es wie bei jeder neuen Technologie: Wir sehen anfangs nur die Möglichkeiten. Die Security ist immer die After-Show.

In ärmeren Ländern führte das zu sehr viel Aktivität in kurzer Zeit. Unternehmen und NGOs dort haben zahlreiche vorbildliche Projekte auf den Weg gebracht. Ein paar Beispiele:

Ushahidi (Kenia): Die Open-Source-Plattform sammelt Daten in Krisensituationen – und zwar nicht nur von Response-Teams, sondern auch von den Menschen vor Ort, etwa per SMS und aus sozialen Medien – und visualisiert sie. So bekommen die Einsatzteams mehr und schneller Informationen.

Wadhwani AI (Indien): Die in neun Sprachen erhältliche App hilft mit Bilderkennung, Datenanalyse und maschinellem Lernen beispielsweise Millionen kleinen Baumwollfarmern in Indien, Schädlingsbefall zu erkennen, zu interpretieren und den passenden Zeitpunkt für die Bekämpfung zu finden.

Farmerline (Ghana): Die Plattform nutzt KI, um Landwirten per Handy Informationen wie Wettervorhersagen, Marktpreise und Anbauwissen in lokalen Sprachen bereitzustellen. Insbesondere in Gebieten, in denen der Zugang zum Internet begrenzt und die Alphabetisierungsrate niedrig ist.

Selbstverständlich gibt es solche Entwicklungen auch in der westlichen Welt, zum Beispiel im Bildungsbereich: Beim Bildungsservice Cognii fördern virtuelle Assistenten Studentinnen und Studenten im direkten Austausch per Chatbot. Die nicht kommerzielle Online-Lernplattform Khan Academy macht Lerninhalte indi-vidualisiert zugänglich. Eine Revolution in der Bildung, deren Folgen kaum überschätzt werden können.

Vom extrem niedrigschwelligen Zugang profitieren aber auch Kriminelle. Cybercrime wie Sabotage, Erpressung oder Datendiebstahl waren früher aufwendige Verbrechen für sehr spezialisierte Gruppen. Mit der neuen Technologie werden sie für jeden durchführbar. Wer bislang dachte, sein Unternehmen sei zu klein, unwichtig oder unbekannt, um das Ziel von Cyberattacken zu werden, lebte schon immer gefährlich. Inzwischen ist es wie ein Spaziergang mitten auf der Autobahn. Nachts. Und nun? Was kann man tun?

Einige Antworten hat Marc Stoecklin, der in Zürich das Security Research Department von IBM Research Europe leitet. Er kennt die Gefahren von künstlicher Intelligenz sehr gut, aber auch die Lösungswege. Stoecklin ist nämlich für die Entwicklung künstlicher Intelligenz für Cybersecurity verantwortlich, insbesondere im Bereich automatisierter Sicherheitssysteme, deren Prinzip ist: erkennen, untersuchen, reagieren.

Herr Stoecklin, wir hören ständig, dass uns künstliche Intelligenz extrem voranbringen wird, aber zugleich hören wir, dass sie enorm gefährlich ist. In welchem Verhältnis stehen die Chancen und Gefahren wirklich?
Marc Stoecklin: Ich fürchte, es gibt darauf keine klare Antwort. Die Chancen sind tatsächlich sehr, sehr groß, um sehr viele gute Dinge zu tun. Doch künstliche Intelligenz ist auch eine Technologie mit Schwächen, die ausgetrickst oder für Böses genutzt werden kann. Das ist bei jeder Technologie so: Anfangs sehen wir vor allem die Möglichkeiten – die Security ist immer die After-Show.

Foto: AdobeStock

Nehmen Sie ein konkretes aktuelles Problem: Phishing. Mails, mit denen versucht wird, Daten wie etwa Passwörter abzugreifen, können heute mit KI-Technologie wahnsinnig präzise, persönlich, dynamisch und zugleich vollautomatisch generiert werden. Andererseits kann KI-Technologie Menschen auch dabei unterstützen, sich vor solchen Mails zu schützen. Das ist eine Art Duell, ein Rennen.

Und wie wird es enden?
Das ist nicht absehbar. Was auch schon in der Technologie begründet ist. Das lässt sich gut an Generative Adversarial Networks (GANs) zeigen, also Systemen, in denen zwei künstliche Intelligenzen unüberwacht voneinander lernen. Sie können zum Beispiel eine KI, die Deep Fakes generiert, mit einer anderen KI verbinden, die Deep Fakes erkennt. Beide KI werden durch das Feedback der jeweils anderen KI besser, sodass sich die beiden im Zusammenspiel mit der Zeit hochkochen. Und dabei ist nicht vorhersehbar, wohin das Ganze am Ende führt.

Wenn die Technologie eskaliert, wird der Mensch irgendwann nicht mehr mitkommen. Führt das zwangsläufig zu einem Technologie-Wettlauf?
Ich fürchte schon. Ich gebe Ihnen ein anderes Beispiel: Schularbeiten. Wie lange wird ein Mensch noch unterscheiden können, ob etwas von einem Kind oder einer Maschine geschrieben wurde? Da muss irgendwann Technologie her. Und es muss auch regulatorisch eingegriffen werden. Damit werden wir uns auseinandersetzen müssen.

Wo stehen wir zurzeit im Wettlauf zwischen KI, die uns hilft, und KI, die uns bedroht? Wer liegt vorn?
Es gibt gerade sehr viel spannende universitäre Forschung, aber auch sehr gute Deep Fakes – Sie kennen sicherlich den Papst im Balenciaga-Outfit. Grundsätzlich ist es so, dass diejenigen, die solche Fälschungen erschaffen, gedanklich immer einen Schritt voraus sind.

Sie arbeiten an Detektionssystemen, die Fälschungen automatisch erkennen – wie gut sind die heute?
Die Trefferquote ist sehr gut, die Herausforderung ist die Fehlalarmquote. Der Empfänger sollte nicht mit zu vielen Fehlern überlastet werden, weil er dann das Tool nicht mehr nutzt und es irrelevant wird. Die Frage ist: Wie schaffe ich ein System, das den Benutzer nicht ermüdet?

Die Frage ist auch: Wie schnell wird es so etwas geben?
Momentan ist die Entwicklung sehr schnell, das geht alles ruckzuck. Aber irgendwann wird es zu einem Gleichstand kommen, das ist wie bei jedem Wettrüsten. Es kommt zu einer Plattform-Immunisierung, die die Arbeit für beide Seiten schwierig macht, bis eine neue Technologie kommt – das ist dann der nächste Schauplatz. 〉

Foto: flickr

Der Sicherheitsentwickler
Marc Stoecklin leitet das Security Research Department von IBM Research Europe in Zürich. Er ist seit 2006 für IBM tätig, war im IBM T. J. Watson Research Center und im Industry & Cloud Solutions Department tätig, hat IBMs COVID-19 Technology Taskforce geleitet und beschäftigt sich heute mit dem Einsatz von KI für Cybersecurity.

Der Sicherheitsbewerter
Matthias Neu ist Referent im Referat „Bewertungsverfahren für eID-Technologien in der Digitalisierung“ im Bundesamt für Sicherheit in der Informationstechnik.

Für Marc Stoecklin, den Entwickler künstlicher Intelligenz, führt der eskalierende Wettlauf von hilfreichen und bedrohlichen KI-Systemen also zwangsläufig zu immer neuen Gefahren und Schutzmaßnahmen – und somit Produkten.

Matthias Neu hat eine andere Sicht. Der Spezialist für Deep Fakes beim Bundesamt für Sicherheit in der Informationstechnik (BSI) richtet seinen Blick vor allem auf die Menschen und erklärt, warum:

„Es gibt bei Deep Fakes drei große Bereiche: Audio Deep Fakes, Video und Bild Deep Fakes sowie textbasierte Fakes. Der Begriff entstand vor fünf, sechs Jahren. Damals funktionierten die Fälschungen mehr schlecht als recht, doch seitdem gab es eine enorme Entwicklung sowohl in der Qualität der Fälschungen als auch in der Zugänglichkeit der nötigen Werkzeuge.

Seit Anfang 2023 existiert zum Beispiel ein cloud-basierter Dienst, mit dem auch Laien sehr einfach Text in Sprache verwandeln können – mit jeder beliebigen Stimme. Früher wurden etwa 20 Stunden Audiomaterial von der Zielperson benötigt, um eine Fälschung zu erstellen. Bei dem neuen Dienst lädt man eine Minute Audiomaterial der Person hoch, zahlt ein paar Euro und kann danach jeden Text mit deren Stimme beziehungsweise einer sehr ähnlichen Stimme sprechen lassen.

Das gibt es mittlerweile auch als Voice Conversion, bei der Texte nicht geschrieben, sondern gesprochen werden. Sie sprechen live, und Ihre Stimme wird mit einer winzigen Verzögerung in eine andere Stimme konvertiert. Für dieses Verfahren werden aktuell noch mehr Expertise und Ressourcen benötigt, aber es ist nur eine Frage der Zeit, bis das als Dienst angeboten wird. Das wird für Angriffe auf Unternehmen und Organisationen in Zukunft auf jeden Fall relevant werden.

Verhindern lassen sich solche Fälschungen nicht – die Systeme gibt es nun mal. Schutz bietet vor allem die Sensibilisierung der Mitarbeiterinnen und Mitarbeiter. Die müssen wissen, dass die Technik existiert und dass deshalb bei einem Anruf die Stimme einer Person als Authentizitätsmerkmal nicht mehr ausreicht. Schon gar nicht, wenn es um wichtige Entscheidungen wie etwa eine Geldtransaktion geht. Die Unternehmen müssen einen Prozess gestalten, der sicherstellt, dass dafür ein Anruf nicht genügt. Es könnte zum Beispiel die Regel geben, dass die Person außerdem eine signierte E-Mail schicken muss. Oder dass jemand die Person unter der Nummer zurückrufen muss, die auch sonst im Alltag genutzt wird.

Die Bedrohungsszenarien von Videofakes sehen anders aus. Es ist beispielsweise vorstellbar, dass jemand einer Videokonferenz mit dem Gesicht einer bekannten Person beitritt, mit deren Stimme spricht und dann sensible Informationen mithört. Es könnten auch gefälschte kompromittierende Bilder der Chefin veröffentlicht werden, etwa vor dem Börsengang. So etwas kann sehr großen Schaden anrichten. Und auch das lässt sich nicht verhindern.

Aber es gibt die Möglichkeit, präventiv zu arbeiten: also vorher ankündigen, was vom Unternehmen ins Internet gestellt wird, und alles Offizielle grundsätzlich kryptografisch signieren, sodass es nachverfolgt werden kann. Damit ist zumindest klar, was wirklich aus dem Unternehmen kommt und was nicht den offiziellen Prozess durchlaufen hat.

Foto: AdobeStock

Gefälschte königliche Laune

Und dann sind da auch noch die Textgeneratoren, Large Language Models wie ChatGPT, die für große Phishing-Angriffe genutzt werden können, um beispielsweise an Passwörter zu kommen. Damit lassen sich Nachrichten in Massen verschicken, die sehr stark personalisiert werden können, wenn man ihnen zum Beispiel die Social-Media-Profile der Zielpersonen als Zusatzinformationen gibt. E-Mails, die so erstellt werden, klingen sehr echt.

Phishing gibt es schon lange, aber inzwischen ist der Aufwand für Angreifer sehr niedrig, zumal nicht nur die E-Mails automatisiert werden können, sondern die Modelle auch interaktiv agieren: Wenn eine Person zurückschreibt, bekommt sie automatisch eine Reaktion. So lassen sich große, qualitativ hochwertige Angriffe ausführen, bei denen Hunderte Mitarbeiterinnen und Mitarbeiter angeschrieben werden können. Das lässt sich nicht verhindern. Auch dafür müssen Unternehmen ihre Beschäftigten sensibilisieren und neue Prozesse installieren. In Zukunft wären automatisierte Detektionsverfahren ideal, wahrscheinlich auf der Basis künstlicher Intelligenz, mit denen sich klassifizieren ließe: Ist das Material echt oder nicht? Daran wird aktuell geforscht. Zum Glück, weil solche Angriffe künftig sicher noch besser und leichter möglich werden.

Aber die Sensibilisierung ist ebenso wichtig, vor allem wenn wir über Desinformation sprechen. Es ist essenziell, zu verstehen, dass ein Foto oder ein Film kein Beweis dafür ist, dass etwas wirklich so geschehen ist, wie es aussieht. Wir müssen als Gesellschaft lernen, Bilder zu hinterfragen, denn es gibt noch keine zuverlässigen technischen Möglichkeiten, sich vor solchen Fakes zu schützen.“

Das alles ist nur der Anfang. Künstliche Intelligenz wird in den kommenden Jahren immer besser und billiger werden – und damit zumindest kurzfristig gefährlicher. Sie hat damit aber auch das Potenzial, die Welt deutlich zu verbessern. Welche Seite am Ende die Oberhand haben wird, ist nicht absehbar. Nur eines ist sicher: Die Zukunft war schon lange nicht mehr so offen wie heute.

Foto: Start Digital

WIR

Woher rührt unsere Unbekümmertheit? Warum sorgen wir in der digitalen Welt nicht für ausreichend Schutz? Sind wir uns der Gefahren im Netz zu wenig bewusst? Mangelt es uns an Informationen? An Sorgfalt? An den finanziellen Mitteln? Wo machen wir es den Angreifern zu leicht? Und warum nehmen wir uns nicht selbst in die Pflicht?

Mehr Information, mehr Aufklärung, mehr Hilfestellung

Verbesserung von Sicherheitswissen / -kompetenz; Verbraucherinnen und Verbraucher über 16 Jahre (n=2 000+); Deutschland; 2022; Prozentwerte für „trifft voll und ganz zu“ und „trifft eher zu“.

63,5

Die Informationen darüber, wie man sich im Internet besser schützen kann, müssten verständlicher sein.

59,6

Es müsste mehr Aufklärungsangebote in beruflicher oder schulischer Aus- und Weiterbildung geben.

62,6

Die Informationen darüber, wie man sich im Internet besser schützen kann, müssten stärker gebündelt werden (z. B. auf einer zentralen Website).

59,2

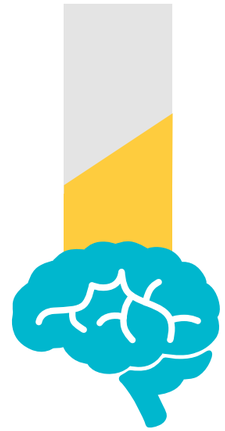
Ich wünsche mir im Internet mehr Informationen zu möglichen Risiken.

44,6

Die Informationen darüber, wie man sich im Internet schützen kann, müssten unterhaltsamer gestaltet werden (Quiz, lustige Videoclips etc.).

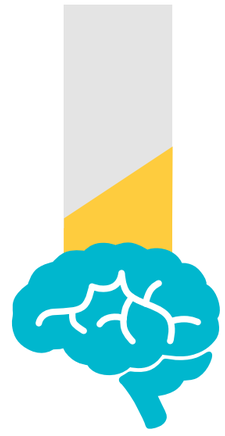
52,2

Ich möchte außerhalb des Internets (Fernsehen, Radio etc.) über digitale Sicherheit aufgeklärt werden.



56,2

Es müsste mehr professionelle Ansprechpartner geben, die persönliche Hilfestellung bieten.



43,4

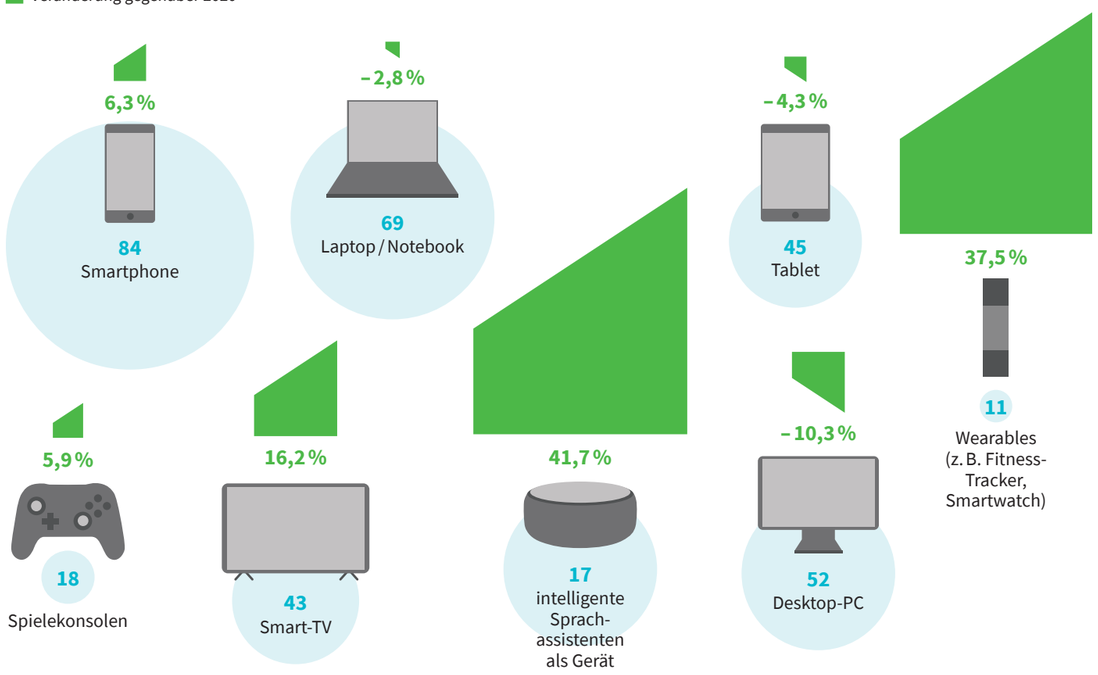
Es müsste mehr Informationsveranstaltungen und Workshops in meiner Nähe zu dem Thema geben.

Quelle: DsiN

Glossar der Cyberbegriffe auf Seite 100 – 103

In Gebrauch

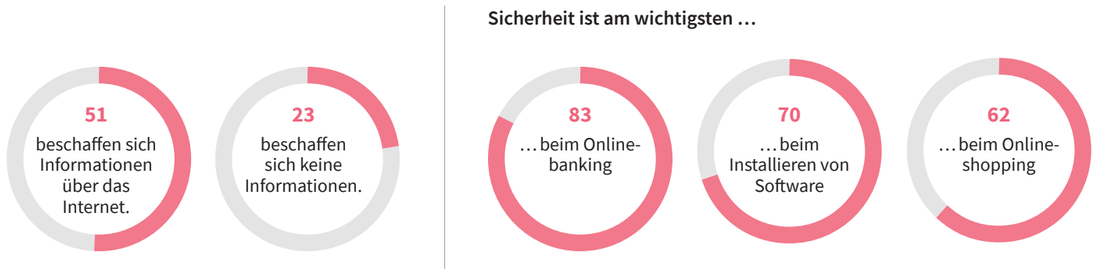
Verwendung von Geräten zur Internetnutzung; Bürgerinnen und Bürger (n=3 050); Deutschland; 2022 ; in Prozent



Quelle: Postbank

Im Fokus

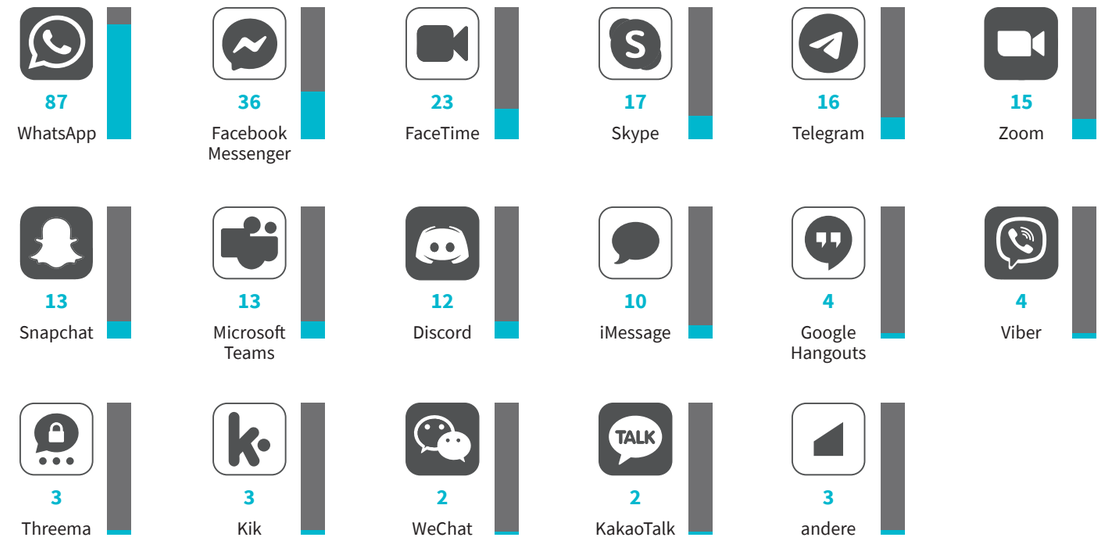
Eigenständige Informationsbeschaffung zur Internetsicherheit; Deutschland; 2022; in Prozent



Quelle: BSI

Im Gespräch

Nutzungsanteile von Online-Kommunikationsdiensten; Bürgerinnen und Bürger (n=36 171); Deutschland; 2022; in Prozent

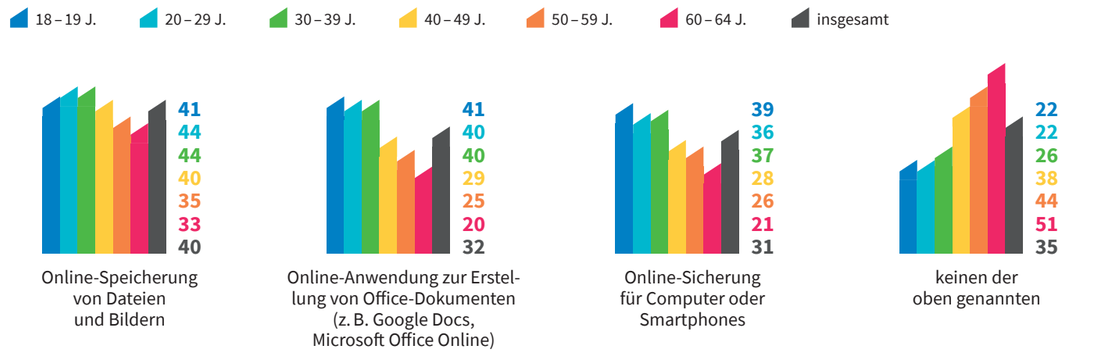


Quelle: Statista Global Consumer Survey

In der Cloud

Nutzung von Cloud nach Altersgruppen; Bürgerinnen und Bürger (n=36 171); Deutschland; 2022; in Prozent

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



Quelle: Statista Global Consumer Survey

Windows-Versionen

Marktanteile der verschiedenen Windows-Versionen; Deutschland; 2022 ; in Prozent

79,97 Windows 10

10,91 Windows 11

5,43 Windows 7

2,69 Windows 8.1

0,44 Windows 8

0,29 Windows XP

0,25 andere

Support-Ende für …

8. April 2014 Windows XP

10. April 2012 Windows Vista

14. Januar 2020 Windows 7

12. Januar 2016 Windows 8

10. Januar 2023 Windows 8.1

rund 9 %

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; 2022 ; in Prozent

76,14 macOS Catalina

17,52 macOS Mojave

3,13 macOS High Sierra

1,03 macOS Sierra

0,86 OS X El Capitan

0,47 OS X Mavericks

* Apple meldet Big Sur 11 fälschlicherweise als Catalin 10.15. Wir können die Nutzung von Big Sur 11 oder Catalina 10.15 nicht korrekt anzeigen, bis Apple dies behebt. Quelle: Statcounter

iOS-Versionen

Marktanteile der verschiedenen iOS-Versionen (Mobile & Tablet); Deutschland; 2023; in Prozent

34,77 iOS 16.1

23,97 iOS 16.2

13,91 iOS 16.0

9,72 iOS 15.6

4,71 iOS 15.7

2,17 iOS 16.3

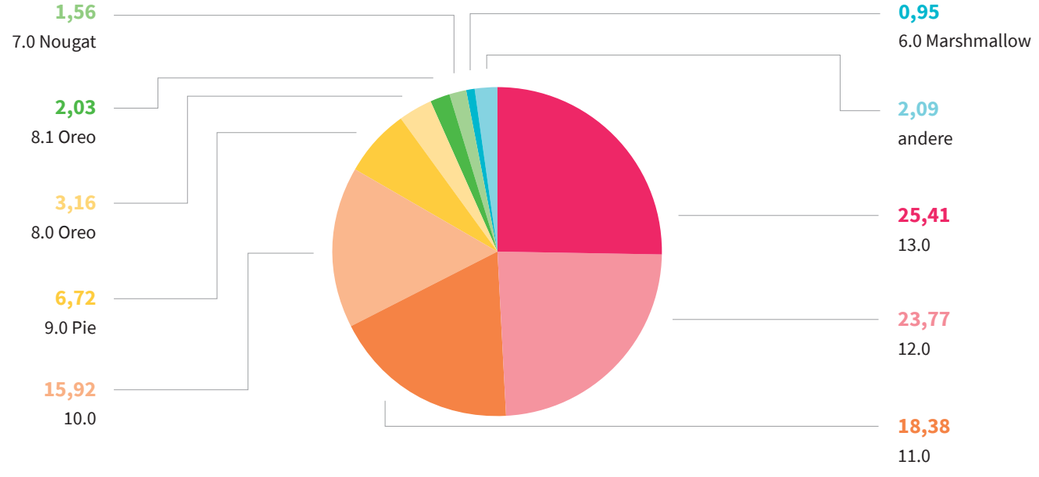
2,13 iOS 15.5

8,62 andere

Quelle: Statcounter

Android-Versionen

Marktanteile der verschiedenen Android-Versionen (Mobile & Tablet); Deutschland; 2023 ; in Prozent



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

Quelle: Statcounter

Aggressionen und Abwehrreaktionen

Schad-Apps für Geräte und entdeckte Bedrohungen

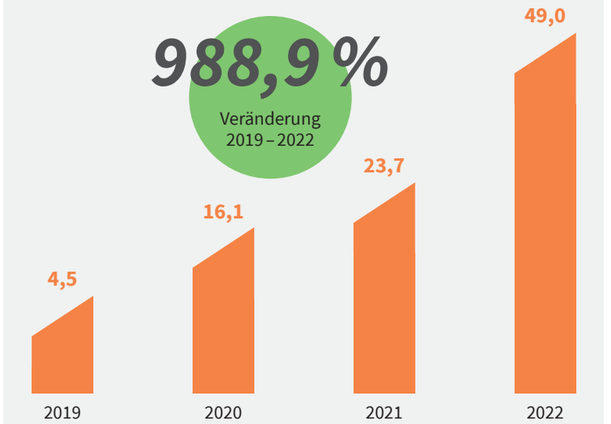
Zahl der Schad-Apps für Android-Geräte, weltweit, 2022:

mehr als 1 Million

Zahl neuer schadhafter Android-Apps pro Minute, weltweit, 2022:

2 bis 3

Zahl der durch G DATA entdeckten Cyberattacken in Deutschland, Österreich und der Schweiz, in Millionen



Zahl der durch G DATA 2022 entdeckten Cyberattacken in Deutschland, Österreich und der Schweiz, in Millionen

49 000 000
gesamt

135 000
pro Tag

> 93
pro Minute

Quelle: G DATA CyberDefense AG

Tätergruppe

Kriminalitätsstatistik zu Cybercrime *; Deutschland

Cybercrime in 2021	Cybercrime in 2022			
146 363	**176,0**	**14 780**	**29 855**	**29,3**
136 865	**162,4**	**13 780**	**28 875**	**29,2**
erfasste Fälle	Fälle pro 100 000 Einwohner	Versuche	Tatverdächtige	Aufklärungsquote in %

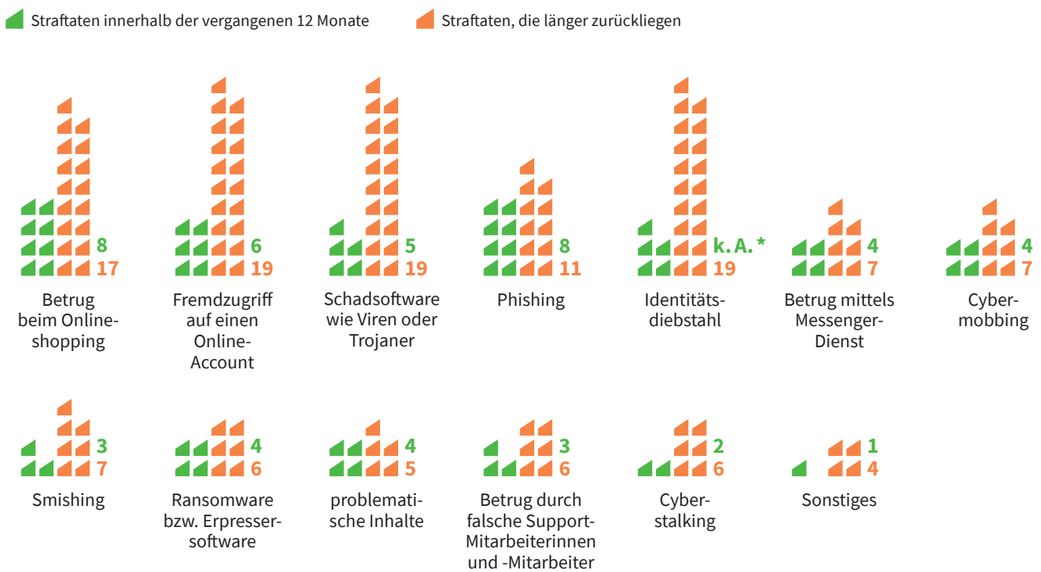
* Cybercrime ist ein sogenannter Summenschlüssel („897 000 Cybercrime“). Folgende Schlüssel sind hier enthalten:
543 000 Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung §§ 269, 270 StGB
674 200 Datenveränderung, Computersabotage §§ 303a, 303b StGB
678 000 Ausspähen, 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.
Quelle: Bundeskriminalamt

Opfer

Opfer von Internetkriminalität nach Art der Straftaten; Befragte, die Opfer von Internetkriminalität geworden sind (n=583) / die innerhalb der vergangenen 12 Monate Opfer von Internetkriminalität geworden sind (n=223); Deutschland; 2022; in Prozent

29 % sind bereits einmal Opfer von Kriminalität im Internet geworden

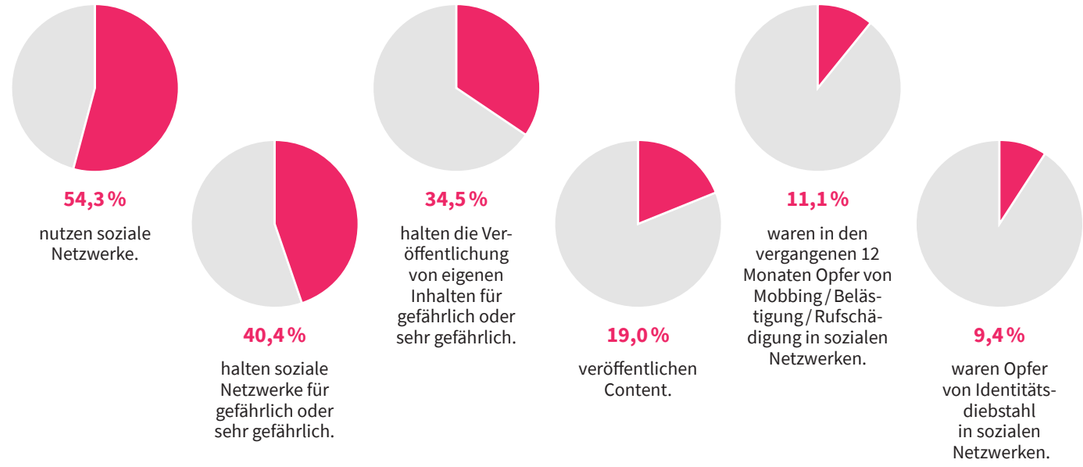
Um welche Art von Straftat handelte es sich, als Sie ein Opfer von Internetkriminalität geworden sind?



* Zahlen zu den vergangenen 12 Monaten liegen nicht vor. Quelle: BSI / ProPK

Einschätzungen und Vorfälle

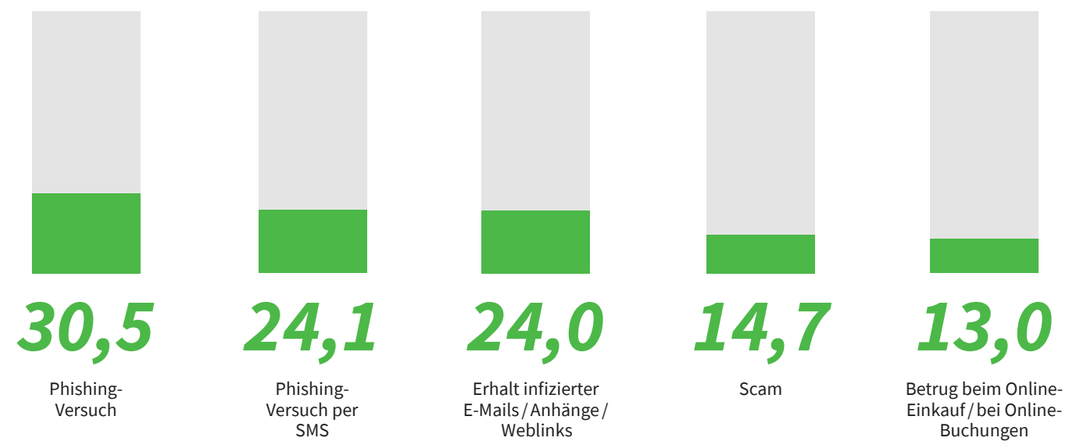
Gefahren und Vorkommnisse bei der Nutzung sozialer Medien; Verbraucherinnen und Verbraucher über 16 Jahre (n=2 000+); Deutschland; 2022



Quelle: DsiN

Attacken und Versuche

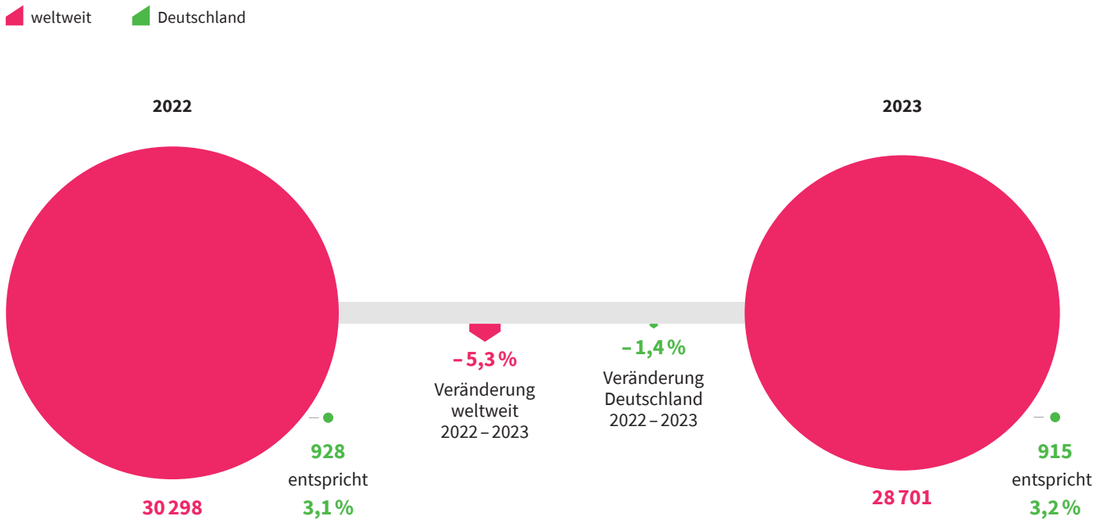
Die häufigsten IT-Sicherheitsvorfälle; Verbraucherinnen und Verbraucher über 16 Jahre (n=2 000+); Deutschland; 2022; in Prozent



Quelle: DsiN

Verwundbar

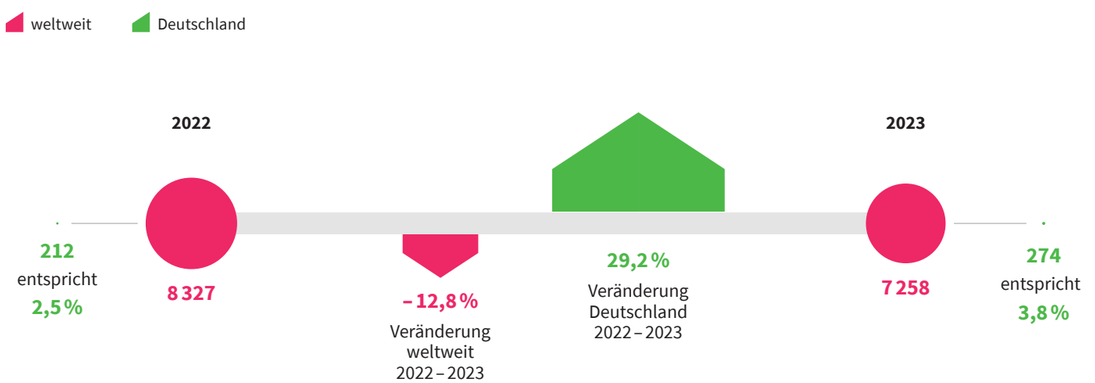
Zahl der über Shodan* auffindbaren „verletzlichen“ Systeme mit default password; weltweit / Deutschland; Zahl / in Prozent



* 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. Quelle: Shodan.io

Verletzbar

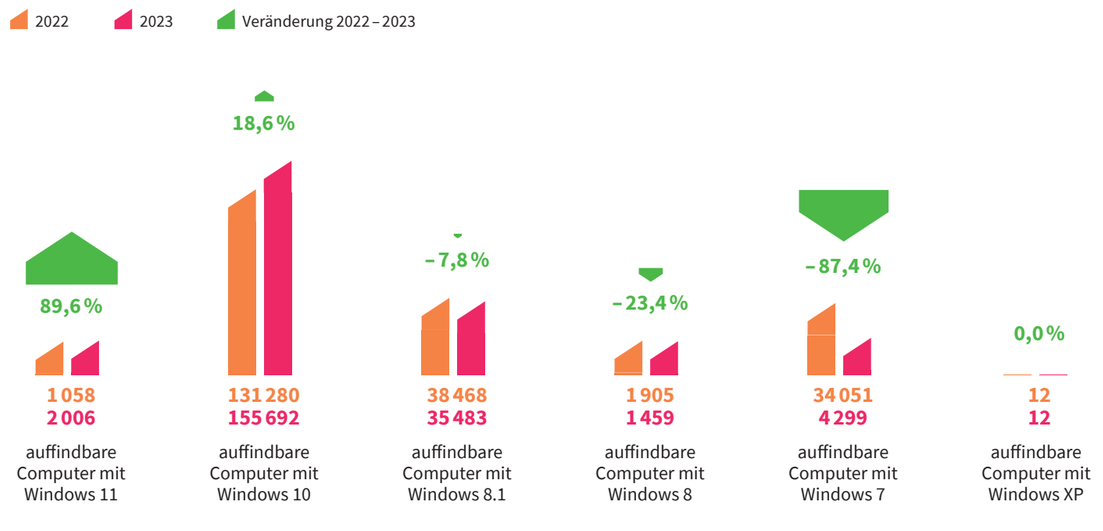
Zahl der über Shodan auffindbaren „verletzlichen“ Webcams; weltweit / Deutschland; Zahl / in Prozent



Quelle: Shodan.io

Auffindbar

Zahl der über Shodan über das Internet auffindbaren „verletzlichen“ Systeme nach Windows-Betriebssystemen; Deutschland; Zahl / in Prozent

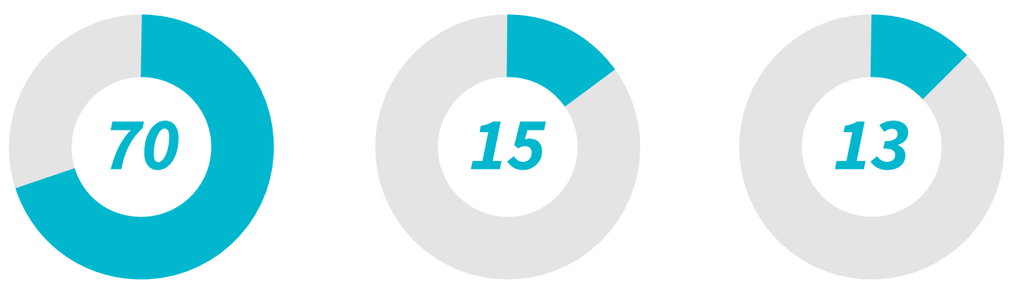


Quelle: Shodan.io

Sonderbar

Zuständigkeitsgefühl im Internet; Personen ab 16 Jahren, die das Internet nutzen (n=1 014); Deutschland; 2022; in Prozent

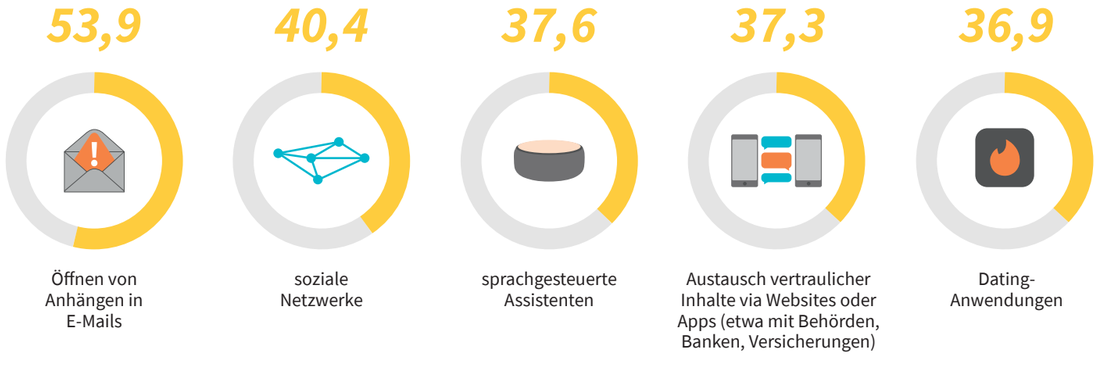
Wer ist verantwortlich für den Schutz im Internet?



* Unternehmen wie z. B. Internet-Anbieter oder die Hersteller von Hard- und Software. Quelle: Bitkom

Fühlbar

Aktivitäten im Internet, bei denen sich Nutzerinnen und Nutzer am unsichersten fühlen; Verbraucherinnen und Verbraucher über 16 Jahre (n=2 000+); Deutschland; 2022; in Prozent



Quelle: DsiN

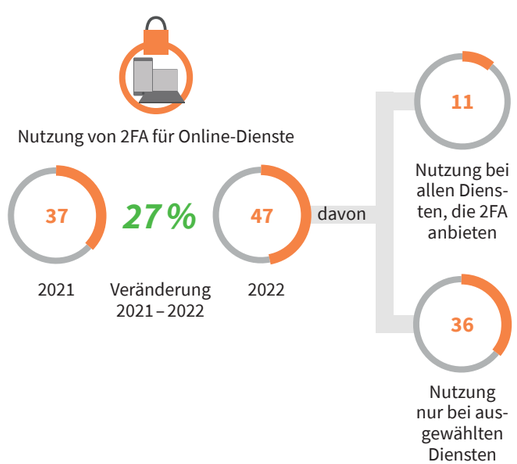
Absehbar

Nutzung von Zwei-Faktor-Authentifizierung (2FA) abseits vom Onlinebanking; Personen ab 18 Jahren, die das Internet nutzen (n=1 000); Deutschland; 2022; in Prozent

Quelle: Bilendi via Statista

Verbesserbar

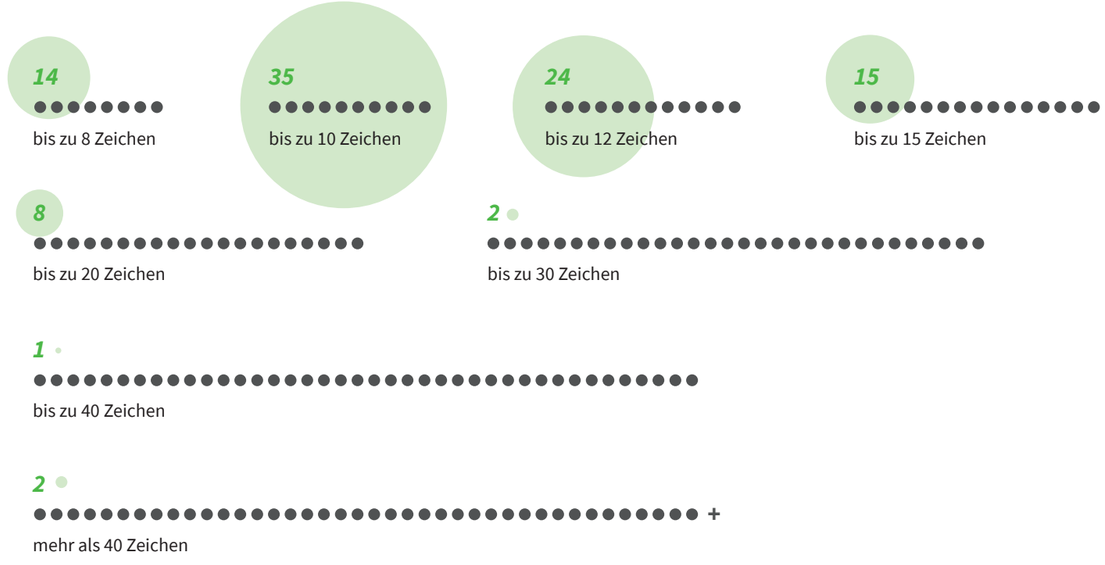
Nutzung von Zwei-Faktor-Authentifizierung (2FA) bei ausgewählten Seiten; Personen ab 16 Jahren, die das Internet nutzen (n=1 014); Deutschland; 2022; in Prozent



Quelle: Bitkom

Dehnbar

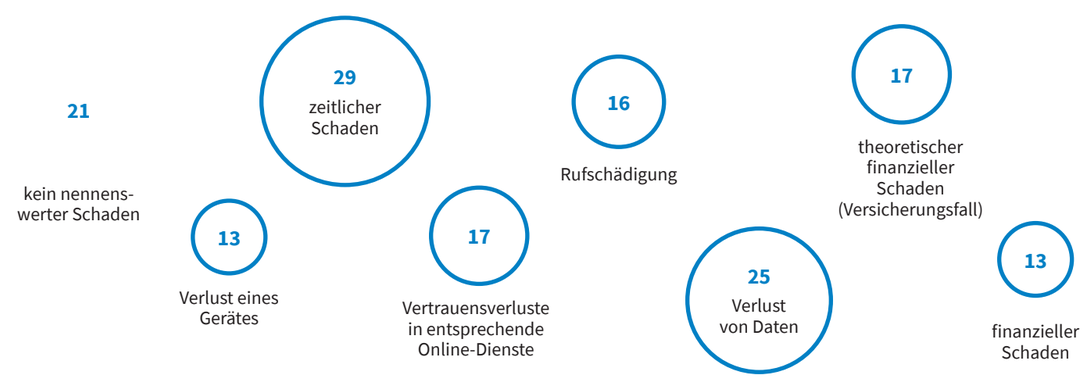
Länge der am häufigsten verwendeten Passwörter; Deutschland; 2022; in Prozent



Quelle: Web.de

Angreifbar

Schäden bei Opfern von Cyberkriminalität; Befragte, die bereits Opfer von Internetkriminalität geworden sind (n=583); Deutschland; 2022; in Prozent *



* Mehrfachnennungen möglich. Quelle: BSI

Sorglos

Eigeninitiative bei Updates; deutschsprachige Bevölkerung im Alter von 16 bis 69 Jahren, die in einem Privathaushalt lebt und über einen Internetzugang verfügt (n=2 000); Deutschland; 2022; in Prozent

34

Nutzung des Angebots der Hersteller, Updates automatisch einzuspielen

30

manuelle Installation von Updates

27

Nutzung von veralteten Programmen, für die keine Updates und Patches mehr bereitgestellt werden

bei mobilen Geräten:

31

Aktualisierung von Apps oder Betriebssystem ausschließlich, wenn neue Funktionen angekündigt werden

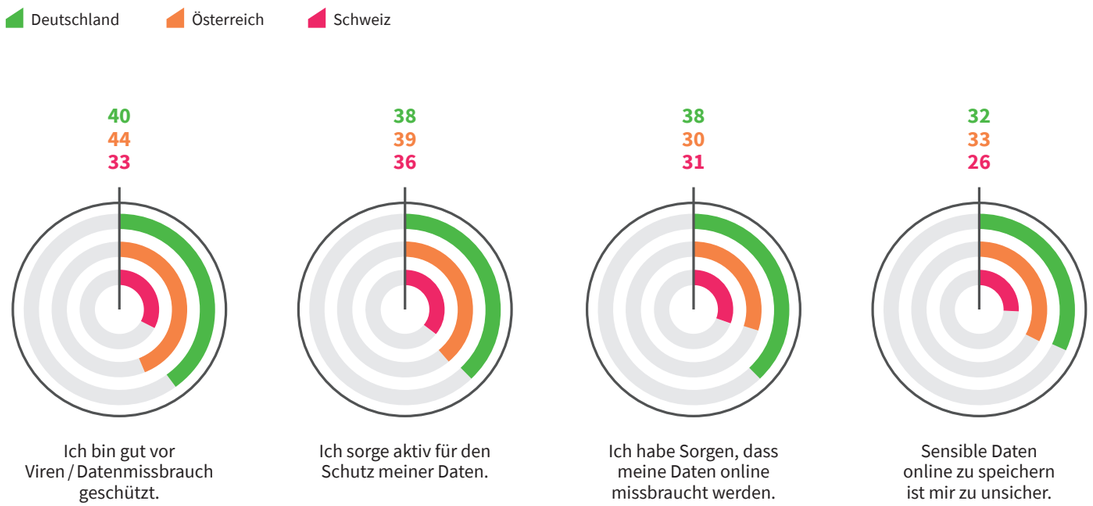
8

keine Durchführung von Aktualisierungen

Quelle: BSI

Schutzlos

Sorgen vor Datenmissbrauch; Befragte im Alter von 18 – 64 Jahren (n=2 000 – 6 000 pro Land); DACH-Region; 2022; Zustimmung zu den Aussagen in Prozent *



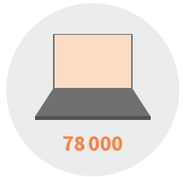
* Mehrfachnennungen möglich. Quelle: BSI

Gnadenlos

Cybercrime in Regierungsnetzen; Deutschland; 1. Juni 2021 bis 31. Mai 2022; Zahl / in Prozent

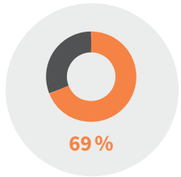
34 000

Zahl der Mails mit Schadprogrammen, die durchschnittlich monatlich in deutschen Regierungsnetzen abgefangen wurden



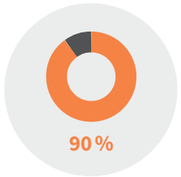
78 000

Zahl neuer Websites, die wegen enthaltener Schadprogramme für den Zugriff aus den Regierungsnetzen gesperrt wurden



69 %

Anteil aller Spam-Mails, die Cyberangriffe wie z. B. Phishing-Mails und Mail-Erpressung waren



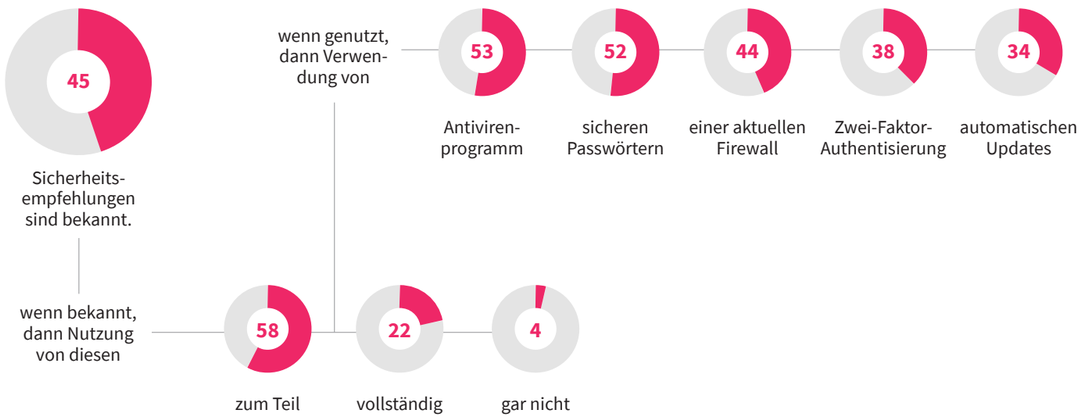
90 %

Anteil des Mail-Betrugs, bei dem es sich um Finance-Phishing handelte

Quelle: BSI

Folgenlos

Umsetzung von bekannten Sicherheitsempfehlungen im Internet; deutschsprachige Bevölkerung im Alter von 16 bis 69 Jahren, die in einem Privathaushalt lebt und über einen Internetzugang verfügt (n=2 000); Deutschland; 2022; in Prozent



Quelle: BSI

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: Eine Backdoor ist ein üblicherweise durch Viren, Würmer oder Trojaner installiertes Programm, das Dritten unbefugten Zugang (Hintertür) 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.

Bug: Mit Bug wird ein Fehler in Programmen bezeichnet.

Computer-Virus: Ein Computer-Virus ist eine nicht selbstständige Programmroutine, die sich selbst reproduziert und dadurch von den Anwenderinnen und Anwerndern nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. Zusätzlich können programmierte Schadensfunktionen des Virus vorhanden sein.

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 digitalen (E-Mail) Übertragung unterschieden. Das kann beispielsweise eine Kollegin oder ein Kollege sein, 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.

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 Hard- 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, Benutzerrechte ausgeweitet oder 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, wie z. B. Benutzername und Passwort. Verschafft sich ein unberechtigter Dritter Zugang zu solchen Daten, so wird von einem Identitätsdiebstahl gesprochen.

Information Stealer: Ein Info Stealer (Information Stealer) ist ein Schadprogramm, das darauf spezialisiert ist, bestimmte Arten von persönlichen Daten, beispielsweise Login-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 (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 Computer-Viren, 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 im 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, 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.

Netzwerkzugangskontrolle: Network Access Control 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 (engl. Flicken): Kleines Programm, das Fehler in Anwendungsprogrammen oder Betriebssystemen behebt.

Penetrationstest: Mit einem Penetrationstest kann herausgefunden werden, ob die Sicherheit innerhalb einer kritischen Umgebungen gewährleistet ist. In beliebigen Systemen und Applikationen, wie z. B. Webseiten oder Warenwirtschaftssysteme, 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 die normale Firewall 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 er 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-Anwendung 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 sicheres 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 (englisch „vulnerability“): 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): Die Abkürzung SIEM steht für Security Information and Event Management. 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-Systeme 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 Zahlungsterminals. Mit den ausgelesenen Daten werden Karten-Kopien 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: Spoofing (von to spoof, zu Deutsch: manipulieren, vortäuschen) 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 der Angreiferinnen odert 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.

Threat Monitoring: Cyber 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): VPN 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. Der Begriff 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, LSI Bayern, Microsoft, NIST, Proofpoint, Rapid7, RiskXchange, Security Insider, TechTarget, Wiener Börse

QUELLENVERZEICHNIS

(ISC)²
Allianz
Bildendi
Bitkom e. V.
bitmi
Blackfog
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Bundeskriminalamt
CIO
Computerwoche
CSO
CVE
CyberDirekt
CyberEdge
Deutschland sicher im Netz (DsiN)
DIHK
Domo
DSGVO-Portal
Europäische Kommission
Foundry
G DATA CyberDefense AG
Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GdV)
HPI
Hiscox
IBM
IDC
ISACA
Mimecast
Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK)
Postbank
Precedence Research
PricewaterhouseCoopers
Proofpoint
SEP
Shodan.io
Statcounter
Statista
Transforma Insights
techconsult
Web.de

IMPRESSUM

Herausgeber: G DATA CyberDefense AG • G DATA Campus • Königsallee 178, 44799 Bochum,
vertreten durch die Vorstände Kai Figge, Frank Heisler, Andreas Lüning
G DATA-Projektteam: Vera Haake, Dr. Daniela Kalkühler, 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, Peter Lau, Kathrin Lilienthal
Autoren: Ulf J. Froitzheim, Christoph Koch
Marktforschung, Recherche, Daten und Quellen:
Cindy Karwowski, Robin Rehfeldt, Tobias Steddin, Daniel Tippel, Katrin Von Soosten

brand eins G DATA statista