2022/2023

CYBERSICHERHEIT IN ZAHLEN

Lernen. Wissen. Handeln.

Liebe Leserinnen und Leser,

zum Unternehmertum gehörte schon immer Mut. Mut, kalkulierte Risiken einzugehen. Mut, auch in schwierigen Zeiten Verantwortung zu übernehmen und Entscheidungen zu treffen. Und Mut, sich als Unternehmen immer wieder neu zu erfinden.

Auch die Beschäftigung mit dem Thema IT-Sicherheit erfordert einigen Mut: Für viele Unternehmerinnen und Unternehmer zählt das Thema nicht zu den Prioritäten. Über viele Jahre war Cybersicherheit, wenn überhaupt, vor allem ein Thema für die IT-Abteilung, mit dem das Management sich höchstens punktuell beschäftigen wollte. Die Zunahme erfolgreicher Angriffe in den vergangenen Jahren zeigt klar: Das ist eine Fehleinschätzung.

Um Ihnen zu helfen, sich mit dem Thema Cybersicherheit vertraut zu machen, haben wir mit unseren Partnern brand eins und Statista wie schon im vergangenen Jahr die wichtigsten Erkenntnisse rund um das Thema Cybersicherheit zusammengetragen. Information als Mutspender.

Im Zentrum des Magazins: eine exklusiv für unser Heft durchgeführte Umfrage. Sie widmet sich in diesem Jahr neben der gefühlten und wahrgenommenen Bedrohungslage auch intensiv den Bedürfnissen von Fachkräften und Mitarbeitenden im Bereich Cybersicherheit.

Denn wer sein eigenes Unternehmen beim Thema Cybersicherheit nachhaltig gut aufstellen will, muss die Menschen ernst nehmen – und einen Kulturwandel herbeiführen. IT-Sicherheit mag mit der Technik beginnen. Aber dort ist lange noch nicht Schluss. Gerade Führungskräfte müssen eine gute Fehlerkultur vorleben und Mitarbeitende ermutigen, auch Fehler einzugestehen. Nur so kann Security Awareness auf Dauer wachsen.

Für Unternehmerinnen und Unternehmer ebenfalls essenziell: das richtige Personal finden, um die Verteidigung hochzufahren. Insbesondere im Bereich Cybersicherheit gibt es einen enormen Wettbewerb um Fachkräfte. Auch darum wird es in diesem Magazin gehen – mit einem Blick in die Aus- und Weiterbildung von Fachpersonal und Einblicke in den Arbeitsalltag von Praktikerinnen und Praktikern in der Cybersecurity.

Wir laden Sie herzlich ein, tief einzutauchen in die Welt der Zahlen, Daten und Fakten. Und wir freuen uns, wenn wir über die anstehenden Herausforderungen ins Gespräch kommen.

Mit herzlichem Gruß,

Ihr Andreas Lüning
Vorstand und Mitgründer G DATA CyberDefense

Wehrt euch!

Wir hätten das ganze Heft mit der Beschreibung von Schadensvorfällen und Angriffen füllen können. Inzwischen vergeht kein Tag ohne Cyberattacke auf kritische Infrastrukturen, Unternehmen und öffentliche Organisationen. Ransomware-Angriffe belegen dabei einen unrühmlichen Spitzenplatz, und Deutschland zählt zu den fünf Ländern weltweit, die am häufigsten als Ziel auserkoren werden. Auch im Privaten sind wir mittlerweile unentwegt Cybercrime-Bedrohungen ausgesetzt – und doch nutzen hierzulande erst 37 Prozent der Menschen zumindest für einige ihrer Online-Dienste eine Zwei-Faktor-Authentifizierung. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im vergangenen Jahr 144 Millionen neue Schadprogramm-Varianten in Deutschland gezählt – 394 000 pro Tag. Unser Schaden durch Ransomware wurde 2021 auf 24,3 Milliarden Euro beziffert.

Wir sind verwundbar geworden. Und wir könnten deutlich mehr dagegen tun. Laut einer Untersuchung von KPMG ist Sparsamkeit derzeit unser größtes Problem. Mehr als 43 Prozent der Unternehmen hierzulande beklagen ein limitiertes Budget für Sicherheitsmaßnahmen – Hauptgrund für erfolgreiche Cyberattacken. Auch eine verteilte Datenhaltung und damit mangelnde Kontrolle werden oft genannt (38,5 Prozent). Platz drei der begünstigenden Faktoren für Cyberkriminalität belegt mit 35 Prozent der Klassiker: unzureichend geschultes Personal.

Dass es sich lohnt, in Weiterbildung zu investieren, und selbst Profis noch jede Menge lernen können, hat unser Autor Ulf Froitzheim in Darmstadt erfahren. In der Cyber Range des Fraunhofer-Instituts für Sichere Informationstechnologie (SIT) kommen selbst ausgebuffte Sicherheitsleute regelmäßig ins Schwitzen. Das Darmstädter Trainingszentrum simuliert lebensecht tückische Hackerangriffe, die sich nur in Teamarbeit stoppen lassen (*Seite 78*). Christoph Koch war in Pennsylvania unterwegs, um herauszufinden, wie sich Cybersecurity lehren lässt. Dort, an der Elite-Universität Carnegie-Mellon, hat die Professorin Dena Haritos Tsamitis in den vergangenen 20 Jahren aus dem Information Networking Institute (INI) eine der angesehensten Ausbildungsstätten der Welt gemacht (*Seite 50*). In Wolfsburg hat Andreas Molitor erfahren, wie viel Zeit und Geld ein global agierender Konzern investiert, um sich gegen Cyberangriffe zu schützen. Michael Kramm, der Chief Information Security Officer der Volkswagen AG, nennt seinen Alltag einen nicht enden wollenden Wettlauf mit kriminellen Hackern (*Seite 24*).

Wenn dann doch passiert, was nicht passieren soll, und ein Ransomware-Angriff das gesamte System lahmlegt, wünscht man sich jemanden wie Kira Groß-Bölting, eine Art Seelsorgerin für digitale Notfälle. Sie ist bei G DATA die erste Ansprechpartnerin für gehackte Firmen. Was das im Alltag bedeutet und was im Ernstfall zu tun ist, haben wir ab *Seite 54* für Sie aufgeschrieben.

Es ist leider so: Totale IT-Sicherheit wird es nie geben. Wir müssen lernen, uns zu verteidigen und für den Notfall zu wappnen. Und wir sollten den Angreifern nicht mehr Angriffsflächen bieten als unbedingt nötig.

Susanne Risch
Chefredakteurin

Inhalt

Gut gewappnet?

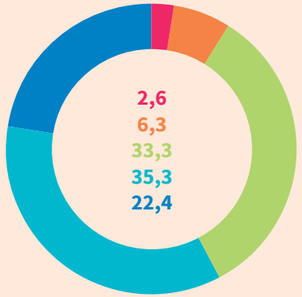
Mehr als 5000 Beschäftigte in Deutschland zwischen 16 und 70 Jahren aus Firmen aller Branchen und Größen gaben im März und April 2022 Auskunft über ihr Wissen, ihre Einschätzungen und Erfahrungen im Umgang mit IT. Die repräsentative Umfrage zeigt ein Stimmungsbild der gefühlten Sicherheit der Menschen in ihrem Berufsalltag.

Prüfen, regeln, ahnden, reden

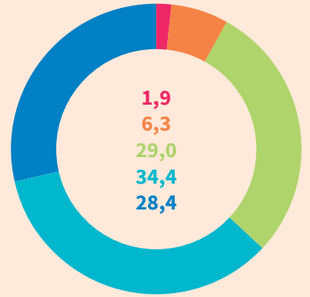
Einschätzung von Aussagen rund um IT-Sicherheit; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2022; in Prozent
1 = ich stimme überhaupt nicht zu, 5 = ich stimme voll und ganz zu, mit den Zahlen dazwischen kann die Meinung abgestuft werden.

1 = stimme überhaupt nicht zu · 2 · 3 · 4 · 5 = stimme voll und ganz zu

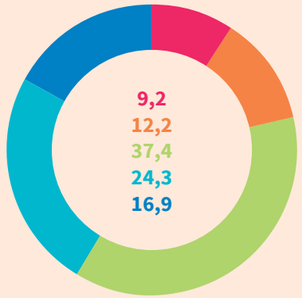
Gesetzliche Regeln im Bereich IT-Sicherheit finde ich sinnvoll, und ich halte mich daran, auch wenn die Umsetzung manchmal sehr komplex ist.



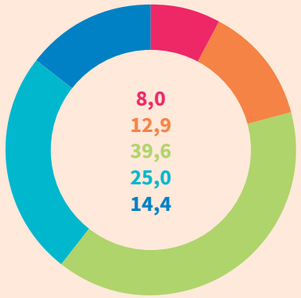
Beim Thema IT-Sicherheit gehe ich kein Risiko ein.



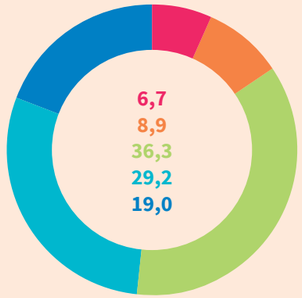
Unternehmen sollten unangekündigte Wissensüberprüfungen zum Thema IT-Sicherheit bei ihren Mitarbeitenden vornehmen.



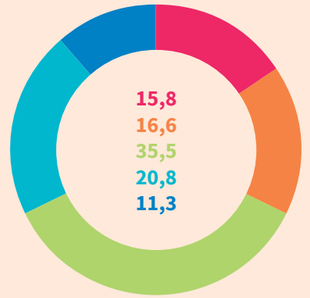
Unternehmen sollten höhere Bußgelder bezahlen, wenn es aufgrund von nicht beachteten Vorgaben / Richtlinien zu Sicherheitsvorfällen kommt.



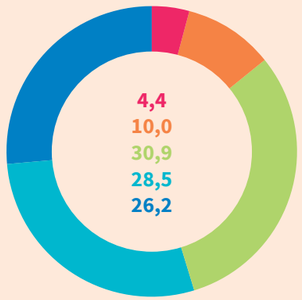
Ich weise meine Vorgesetzten und Kolleginnen und Kollegen auf Fehlverhalten im Bereich IT-Sicherheit hin, auch wenn das nicht gern gehört wird.



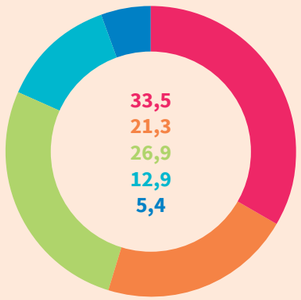
Ich bringe aktiv Vorschläge ein, um die IT-Sicherheit in meinem Unternehmen zu verbessern.



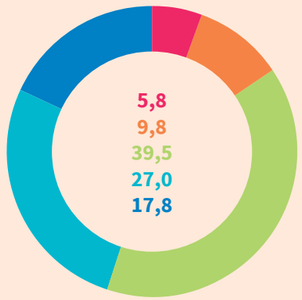
IT-Sicherheitsregeln erschweren meine Arbeit nicht.



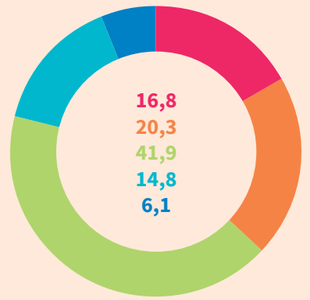
Mein Unternehmen nimmt das Thema IT-Sicherheit auf die leichte Schulter.



In einem Unternehmen mit zu lockerem Umgang beim Thema IT-Sicherheit möchte ich nicht arbeiten.



In einem Unternehmen mit zu vielen Regeln und Vorschriften zur IT-Sicherheit möchte ich nicht arbeiten.



Quelle: Statista im Auftrag von G DATA

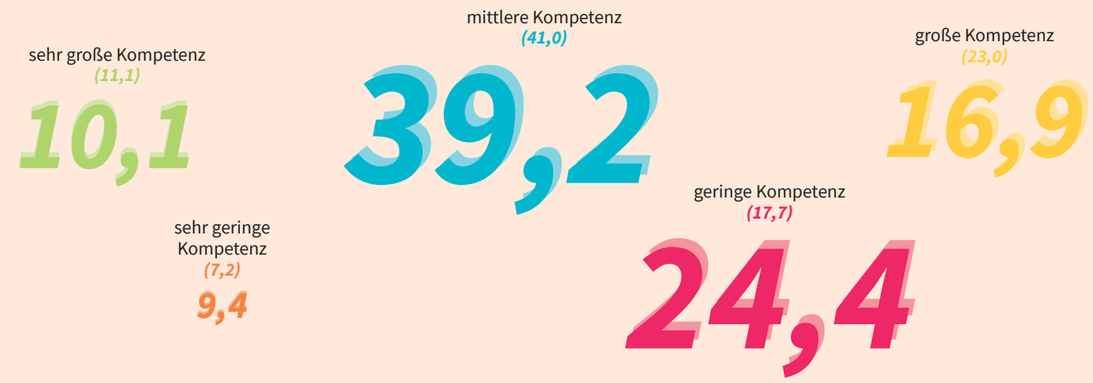
Cyberbegriffe-Übersicht im Glossar auf Seite 100 – 103.

Wie kompetent sind wir beim Thema IT-Sicherheit?

Einschätzung der persönlichen Kompetenz zum Thema IT-Sicherheit; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2022; in Prozent

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

(in Klammern der Wert aus dem Vorjahr)



nach Geschlecht

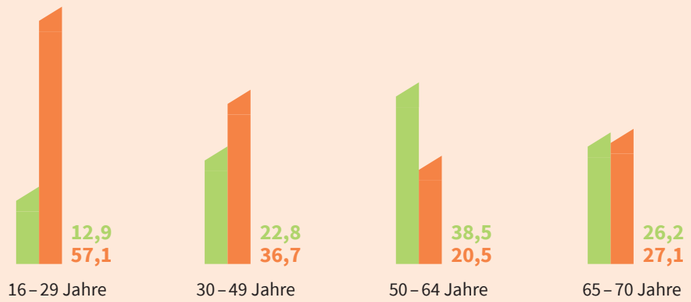
20,9

Anteil der **männlichen** Befragten, die ihre persönliche Kompetenz als (sehr) groß einschätzen

34,0

Anteil der **weiblichen** Befragten, die ihre persönliche Kompetenz als (sehr) groß einschätzen

nach Alter



nach Abteilungen

	sehr große Kompetenz	große Kompetenz	mittlere Kompetenz	geringe Kompetenz	sehr geringe Kompetenz
IT und EDV	26,5	46,2	25,0	2,1	0,2
Personal und Recruiting	14,5	29,8	40,2	10,4	5,2
Geschäftsleitung	13,7	27,5	44,2	11,3	3,3
Buchhaltung und Finanzen	11,0	27,3	37,6	18,7	5,3
Rechtsabteilung	8,1	32,4	39,0	14,0	6,6
Forschung und Entwicklung	8,0	42,8	39,0	8,6	1,6
Produktion und Fertigung	8,0	22,6	40,0	19,2	10,2
Marketing und Vertrieb	7,9	26,1	44,3	15,4	6,3
andere Abteilungen	3,5	14,0	40,9	23,6	18,1

Quelle: Statista im Auftrag von G DATA

nach Branchen

Mittelwert: 5 = sehr große Kompetenz // 4 = große Kompetenz // 3 = mittlere Kompetenz // 2 = geringe Kompetenz // 1 = sehr geringe Kompetenz

nach Unternehmensgröße

	unter 50 Beschäftigte	50 bis 999 Beschäftigte	1 000 Beschäftigte und mehr
(sehr) große Kompetenz	22,8	42,6	33,5
(sehr) geringe Kompetenz	36,6	21,4	23,4

nach Homeoffice-Möglichkeit

	komplette Arbeitswoche im Homeoffice	einige Arbeitstage pro Woche im Homeoffice	keine Homeoffice-Möglichkeit
(sehr) große Kompetenz	42,7	52,6	16,3
(sehr) geringe Kompetenz	14,8	10,3	44,0

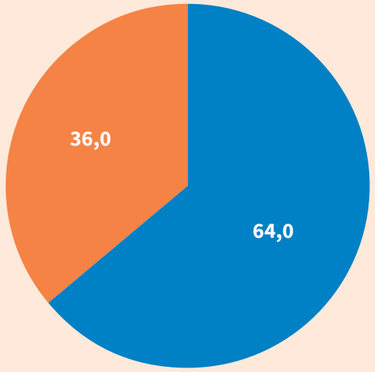
Quelle: Statista im Auftrag von G DATA

Sind genügend Fachleute im Haus?

Vorhandensein von IT-Abteilung bzw. IT-Verantwortlichen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland *; 2022; in Prozent

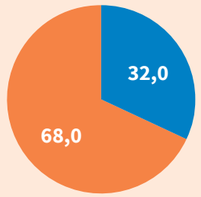
nein ja

Befragte insgesamt

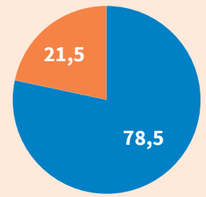


Deutschland

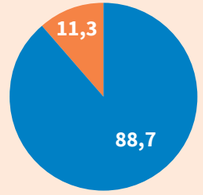
nach Unternehmensgröße



unter 50 Beschäftigte



50 bis 999 Beschäftigte



1 000 Beschäftigte und mehr

nach Branchen

	ja	nein
Telekommunikation und Informationsdienstleistungen	89,9	10,1
Finanz- und Versicherungsdienstleistungen	86,3	13,7
öffentlicher Dienst	85,6	14,4
Maschinenbau, Kraftwagen- und sonstiger Fahrzeugbau	85,3	14,7
Herstellung von Chemie- und Pharma-Erzeugnissen	85,0	15,0
Energie- und Wasserversorgung, Abwasser- und Abfallentsorgung	78,6	21,4
Herstellung von Textilien, Bekleidung und Schuhen	76,6	23,4
Herstellung / Verarbeitung von Papier, Pappe, Glas, Keramik, Metalle, Holz-, Flecht-, Gummi-, Kunststoffwaren, Möbeln	76,0	24,0
Verkehr und Logistik	66,4	33,6
Herstellung von Lebensmitteln, Genuss- und Futtermitteln	66,3	33,7
Groß- und Einzelhandel (inkl. Kfz-Handel)	65,1	34,9
Gesundheit und Soziales	59,6	40,4
andere Branche	54,3	45,7
Erziehung und Bildung	53,2	46,8
Dienstleistungen (Personal, Callcenter, Sicherheit)	50,8	49,2
freiberufliche, wissenschaftliche und technische Dienstleistungen (Beratung, Wirtschaftsprüfung, Forschung / Entwicklung, Ingenieurbüros etc.)	49,7	50,3
Grundstücks- und Wohnungswesen	49,0	51,0
Bau	43,7	56,3
Kunst, Freizeit, Sport und Erholung	43,7	56,3
Beherbergung und Gastronomie	35,8	64,2

* Befragte, die nicht in der IT / EDV arbeiten. Quelle: Statista im Auftrag von G DATA

Wie steht es um die Ausstattung im IT-Bereich?

Einschätzung der Ausstattung des IT-Bereichs; Arbeitnehmerinnen und Arbeitnehmer in Deutschland *; 2022; in Prozent

Befragte insgesamt

sehr gut	36,3
gut	52,6
weder noch	9,3
schlecht	1,7
sehr schlecht	0,1

nach persönlicher Kompetenz der Befragten im Bereich IT-Sicherheit

	(sehr) geringe Kompetenz	mittlere Kompetenz	(sehr) große Kompetenz
(sehr) gut	61,1	80,2	93,4
(sehr) schlecht	11,1	3,0	1,0

* Befragte, die in der IT / EDV oder in der Geschäftsleitung arbeiten und deren Unternehmen eine eigene IT-Abteilung bzw. Verantwortliche für den IT-Bereich hat. Quelle: Statista im Auftrag von G DATA

Wie steht es um die Kompetenz der IT-Abteilung?

Kompetenz der IT-Abteilung bzw. des IT-Verantwortlichen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland *; 2022; in Prozent

28,2 sehr große Kompetenz

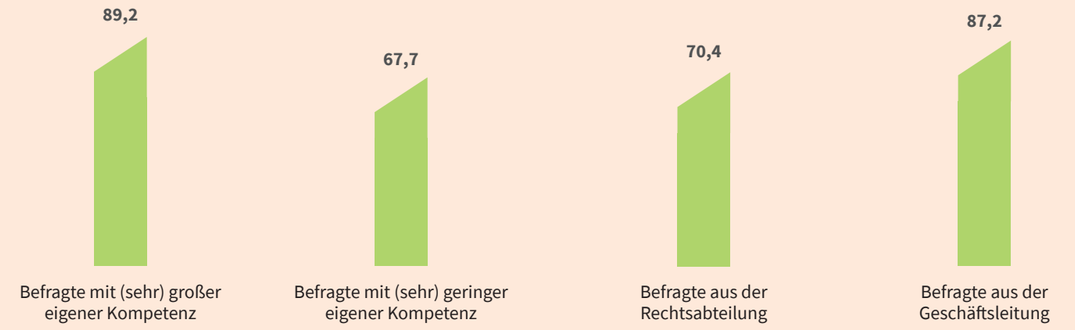
50,2 große Kompetenz

19,1 mittlere Kompetenz

0,6 sehr geringe Kompetenz

1,9 geringe Kompetenz

Anteil der Befragten, die der IT-Abteilung bzw. dem IT-Verantwortlichen (sehr) große Kompetenz bescheinigen:



* Befragte, die in der IT / EDV arbeiten oder deren Unternehmen eine eigene IT-Abteilung bzw. Verantwortliche für den IT-Bereich hat. Quelle: Statista im Auftrag von G DATA

Wo wird nach Experten für den IT-Bereich gesucht?

Häufigste Bewerbungskanäle im IT-Bereich nach Unternehmensgröße; Arbeitnehmerinnen und Arbeitnehmer in Deutschland *; 2022; in Prozent

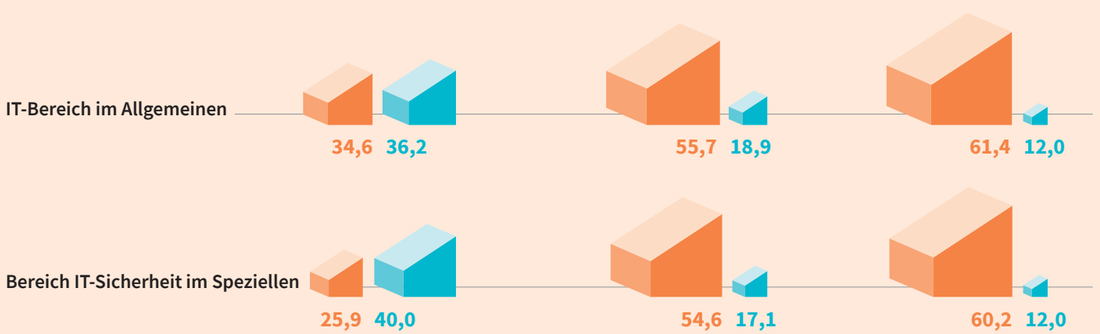
	unter 50 Beschäftigte	50 bis 999 Beschäftigte	1 000 Beschäftigte und mehr
Karriereseite des Unternehmens	33,3	41,8	65,0
Jobbörsen (z. B. Stepstone)	26,2	49,7	43,3
Weiterempfehlung durch eigene Mitarbeitende	31,0	32,7	38,3
Social Media	38,1	29,1	18,3
Jobmessen	21,4	22,4	23,3
Headhunter	14,3	21,2	20,0
keiner der genannten Kanäle	9,5	3,6	1,7
Sonstige	0,0	1,2	5,0

* Nur Befragte, die im Personal / Recruiting arbeiten und deren Unternehmen eine eigene IT-Abteilung bzw. Verantwortliche für den IT-Bereich hat; Mehrfachauswahl möglich. Quelle: Statista im Auftrag von G DATA

Wie dringend werden IT-Fachleute gebraucht?

Mitarbeitersuche für den IT-Bereich nach Unternehmensgröße; Arbeitnehmerinnen und Arbeitnehmer in Deutschland *; 2022; in Prozent

(sehr) dringend — (überhaupt) nicht dringend / gar nicht



* Befragte, die in der IT oder im Personalbereich/ Recruiting bzw. in der Geschäftsleitung arbeiten und deren Unternehmen eine eigene IT-Abteilung bzw. Veranwortliche für den IT-Bereich hat. Quelle: Statista im Auftrag von G DATA

Wer kümmert sich um die notwendige Expertise?

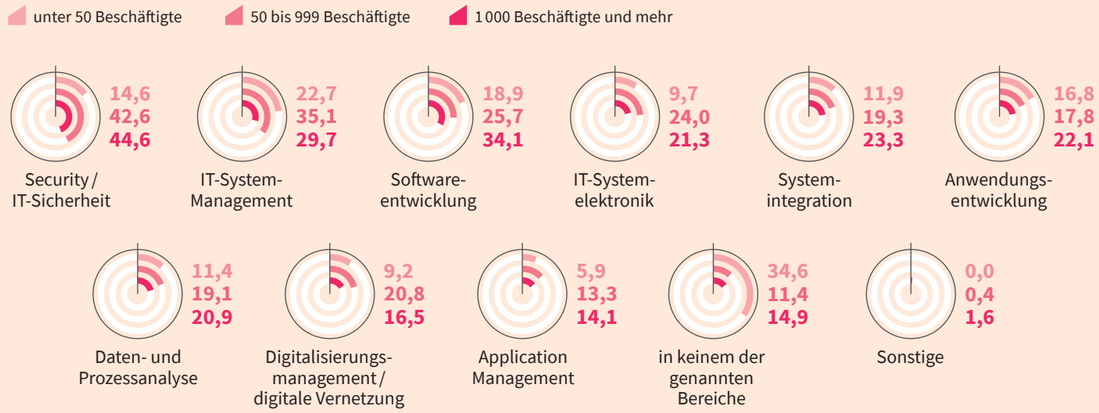
Zuständigkeit für Aus- / Weiterbildung der Mitarbeitenden im Bereich IT-Sicherheit; Arbeitnehmerinnen und Arbeitnehmer in Deutschland *; 2022; in Prozent

Wir bilden überwiegend selbst aus / weiter (unternehmensintern)	47,3
überwiegend über externe Dienstleister	27,9
unternehmensintern und über externe Dienstleister gleichermaßen	24,8

* Befragte, die in der IT oder im Personalbereich / Recruiting bzw. in der Geschäftsleitung arbeiten und deren Unternehmen eine eigene IT-Abteilung bzw. Veranwortliche für den IT-Bereich hat. Quelle: Statista im Auftrag von G DATA

Wo ist der Bedarf an IT-Fachleuten am größten?

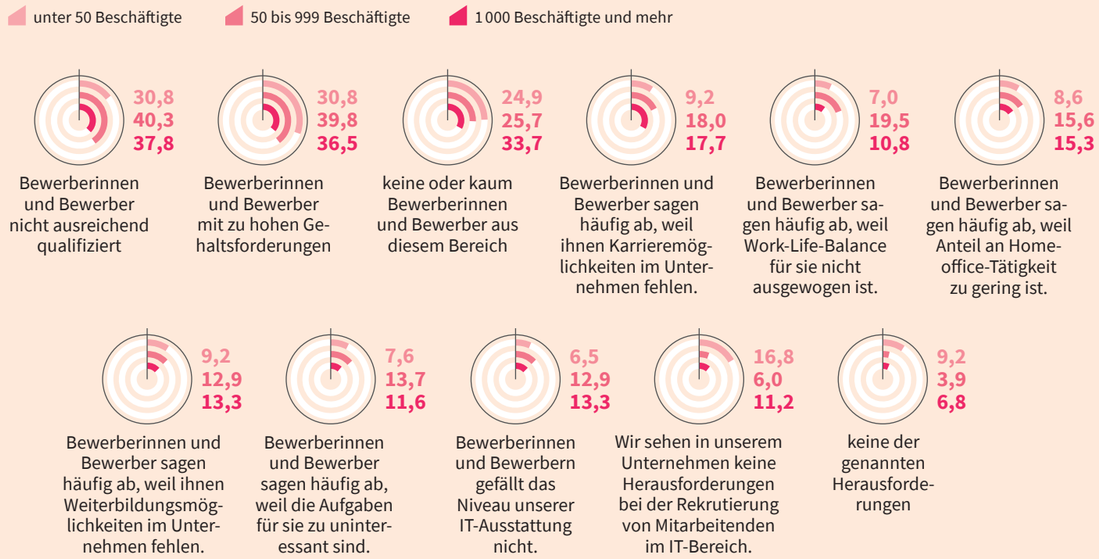
IT-Bereiche mit dringendem Mitarbeiterbedarf nach Unternehmensgröße; Arbeitnehmerinnen und Arbeitnehmer in Deutschland *; 2022; in Prozent



* Befragte, die in der IT oder im Personalbereich / Recruiting bzw. in der Geschäftsleitung arbeiten und deren Unternehmen eine eigene IT-Abteilung bzw. Veranwortliche für den IT-Bereich hat. Mehrfachauswahl möglich. Quelle: Statista im Auftrag von G DATA

Woran hapert es für die IT im Recruiting?

Herausforderung bei der Rekrutierung von Mitarbeitenden im IT-Bereich nach Unternehmensgröße; Arbeitnehmerinnen und Arbeitnehmer in Deutschland *; 2022; in Prozent



* Befragte, die in der IT oder im Personalbereich / Recruiting bzw. in der Geschäftsleitung arbeiten und deren Unternehmen eine eigene IT-Abteilung bzw. Veranwortliche für den IT-Bereich hat. Mehrfachauswahl möglich. Quelle: Statista im Auftrag von G DATA

Privat eher sparsam

Investitionen in die IT-Sicherheit privater Geräte im Jahr 2022 gegenüber 2021; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2022; in Prozent

erhöhen | gleich bleiben | verringern

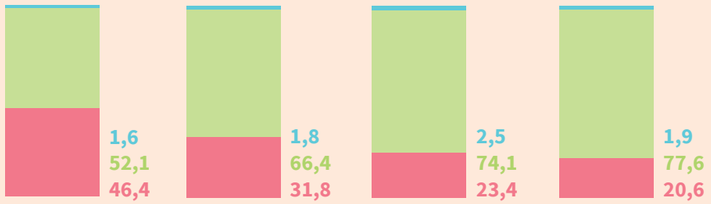
Was schätzen Sie, wie werden sich Ihre Investitionen in die IT-Sicherheit Ihrer privaten internetfähigen Geräte (z. B. Laptop, Smartphone, Tablet) im Jahr 2022 gegenüber 2021 verändern?

30,8 erhöhen

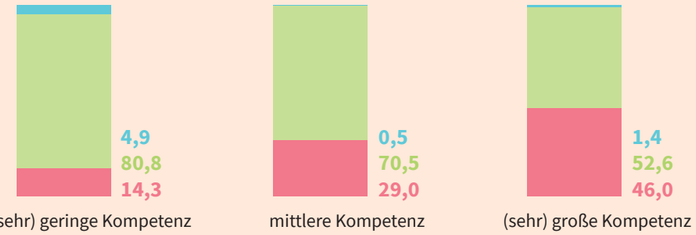
67,2 gleich bleiben

2,0 verringern

nach Alter



nach persönlicher Kompetenz im Bereich IT-Sicherheit



Quelle: Statista im Auftrag von G DATA

Arbeitnehmerinnen und Arbeitnehmer, deren Investitionen in die IT-Sicherheit privater Geräte sich erhöhen nach Homeoffice-Möglichkeit

Arbeitnehmerinnen und Arbeitnehmer …	
… mit kompletter Arbeitswoche im Homeoffice	29,5
… mit einigen Arbeitstagen pro Woche im Homeoffice	44,9
… ohne Homeoffice-Möglichkeit	20,1

Quelle: Statista im Auftrag von G DATA

Arbeitnehmerinnen und Arbeitnehmer, deren Investitionen sich erhöhen nach Branchen

Herstellung von Textilien, Bekleidung und Schuhen	50,0
Telekommunikation und Informationsdienstleistungen	42,9
Maschinenbau, Kraftwagen- und sonstiger Fahrzeugbau	38,6
Herstellung / Verarbeitung von Papier, Pappe, Glas, Keramik, Metalle, Holz-, Flecht-, Gummi-, Kunststoffwaren, Möbeln	35,5
Dienstleistungen (Personal, Callcenter, Sicherheit)	32,8
Groß- und Einzelhandel (inkl. Kfz-Handel)	31,4
Kunst, Freizeit, Sport und Erholung	29,3
Bau	28,8
Verkehr und Logistik	27,7
öffentlicher Dienst	26,2
Erziehung und Bildung	25,0
Gesundheit und Soziales	24,8
Beherbergung und Gastronomie	24,5

Quelle: Statista im Auftrag von G DATA

Unternehmerisch eher durchwachsen

Investitionen in die IT-Sicherheit des Unternehmens im Jahr 2022 gegenüber 2021; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2022; in Prozent *

erhöhen | gleich bleiben | verringern

Was schätzen Sie, wie werden sich die Investitionen in die IT-Sicherheit Ihres Unternehmens im Jahr 2022 gegenüber 2021 verändern?

44,7 erhöhen

53,8 gleich bleiben

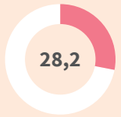
1,5 verringern

nach persönlicher Kompetenz im Bereich IT-Sicherheit

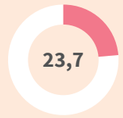
	(sehr) geringe Kompetenz	mittlere Kompetenz	(sehr) große Kompetenz
erhöhen	16,9	32,1	55,1
gleich bleiben	76,9	66,6	44,0
verringern	6,2	1,4	0,9

Anteil der Arbeitnehmerinnen und Arbeitnehmer, die schätzen, dass sich die Investitionen ihres Unternehmens in IT-Sicherheit im Jahr 2022 gegenüber 2021 erhöhen:

52,8 aus der Branche Finanz- und Versicherungsdienstleistungen



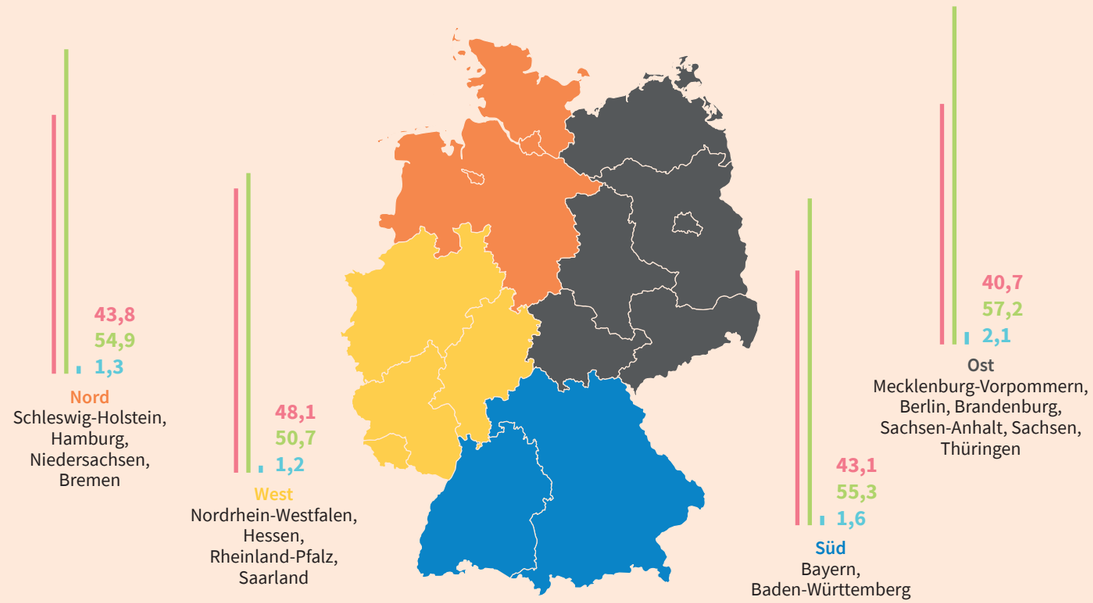
28,2 aus der Branche freiberufliche, wissenschaftliche und technische Dienstleistungen



23,7 aus Unternehmen mit weniger als 50 Beschäftigten

56,5 aus Unternehmen mit 1 000 Beschäftigten und mehr

nach Regionen



* Befragte, die in der IT / EDV oder in der Geschäftsleitung arbeiten. Quelle: Statista im Auftrag von G DATA

Gut geschützt?

Schutzgefühl durch IT-Sicherheitsmaßnahmen im privaten und beruflichen Umfeld; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2022; in Prozent

(sehr) schlecht, privat | (sehr) gut, privat | (sehr) schlecht, beruflich | (sehr) gut, beruflich

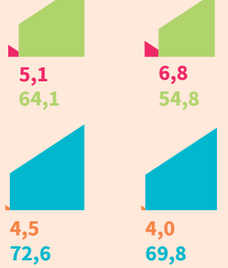
im privaten Umfeld

sehr schlecht	1,2
schlecht	4,7
weder noch	34,3
gut	39,3
sehr gut	20,5
(sehr) schlecht	*5,9*
(sehr) gut	*59,8*

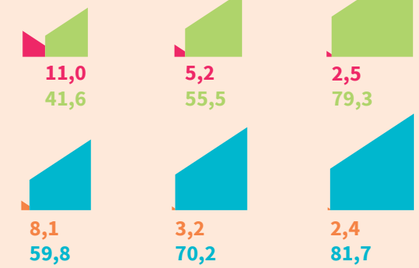
im beruflichen Umfeld

sehr schlecht	1,4
schlecht	2,9
weder noch	24,5
gut	38,8
sehr gut	32,5
(sehr) schlecht	*4,3*
(sehr) gut	*71,3*

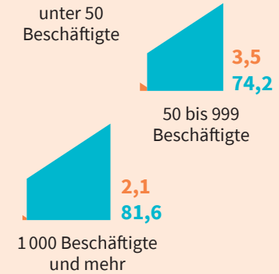
nach Geschlecht



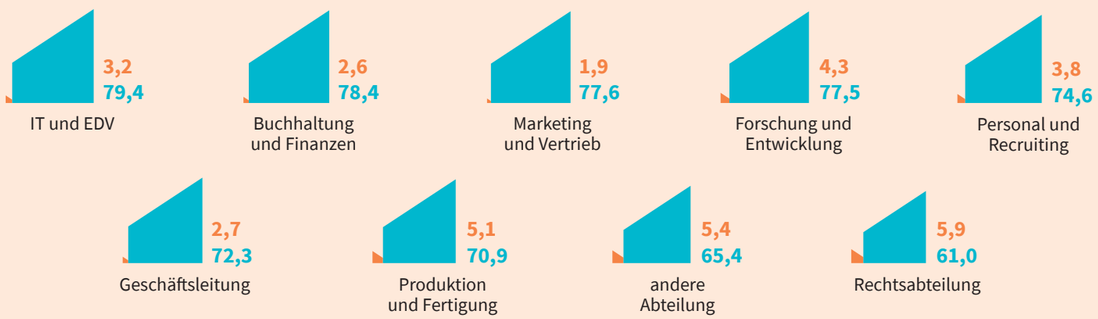
nach persönlicher Kompetenz im Bereich IT-Sicherheit



im beruflichen Umfeld nach Unternehmensgröße



im beruflichen Umfeld nach Abteilung



Quelle: Statista im Auftrag von G DATA

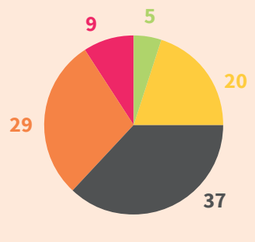
Persönlich gefährdet?

Risikoeinschätzung zum Thema Cyberkriminalität im privaten und beruflichen Umfeld; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2022; in Prozent

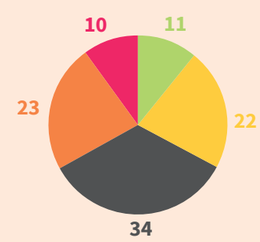
Wie hoch schätzen Sie das Risiko ein, dass Sie Opfer von Cyberkriminalität oder Datenklau werden (z. B. Identitätsdiebstahl, Diebstahl von Kreditkartendaten oder Unternehmensdaten, Internetbetrug, Cybererpressung, Cyberspionage)?

sehr gering | gering | weder noch | hoch | sehr hoch

im privaten Umfeld



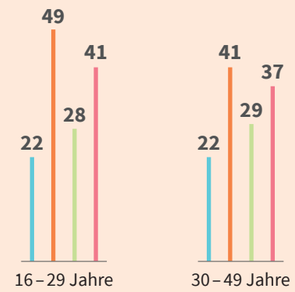
im beruflichen Umfeld



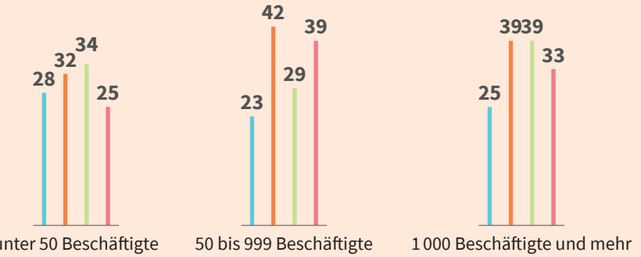
Quelle: Statista im Auftrag von G DATA

(sehr) gering, privat | (sehr) hoch, privat | (sehr) gering, beruflich | (sehr) hoch, beruflich

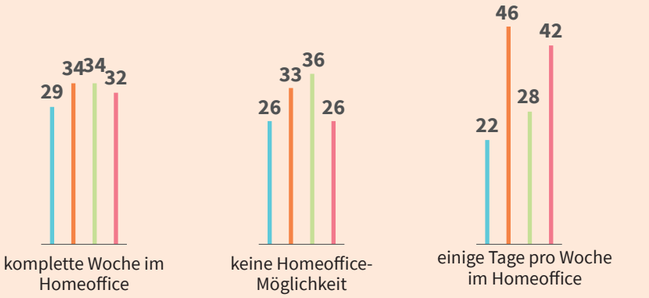
nach Alter



nach Unternehmensgröße



nach Homeoffice-Möglichkeit



Quelle: Statista im Auftrag von G DATA

Definierte Prozesse für den Ernstfall?

Bekanntheit von definierten Prozessen bei IT-Sicherheitsvorfällen nach Unternehmensgröße; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2022; in Prozent

Sind Ihnen in Ihrem Unternehmen definierte Prozesse bekannt, wie Sie im Falle eines IT-Sicherheitsvorfalls vorzugehen haben?

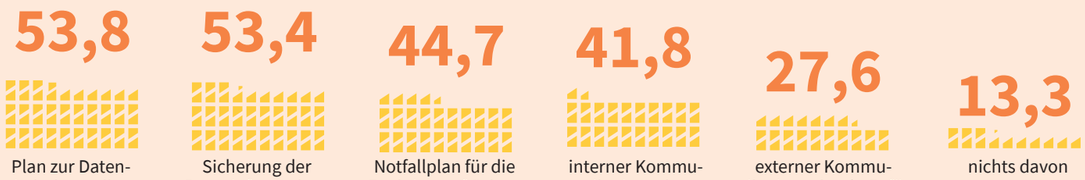
	Deutschland	unter 50 Beschäftigte	50 bis 999 Beschäftigte	1 000 Beschäftigte und mehr
ja	50,9	32,5	58,7	63,9
nein	49,1	67,5	41,3	36,1

Quelle: Statista im Auftrag von G DATA

Maßnahmenplan für den Schadensfall?

Verfahren oder Maßnahmen bei einem IT-Sicherheitsvorfall; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2022; in Prozent *

Welche Verfahren oder Maßnahmen gibt es in Ihrem Unternehmen im Falle eines IT-Sicherheitsvorfalls?



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

Einfluss von gesetzlichen Vorgaben?

Einfluss von regulatorischen Vorgaben durch die Politik nach Unternehmensgröße; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2022; in Prozent *

Wie bewerten Sie den Einfluss von regulatorischen Vorgaben durch die Politik (z. B. DSGVO, IT-Sicherheitsgesetz) für Ihr Unternehmen?

	unter 50 Beschäftigte	50 bis 999 Beschäftigte	1 000 Beschäftigte und mehr
Sie haben in meinem Unternehmen Handlungsbedarfe offengelegt.	13,2	25,6	18,3
Sie haben mir geholfen, Investitionen in IT-Sicherheit intern umzusetzen / zu rechtfertigen.	8,2	18,7	14,1
Sie wirken sich störend auf unser Geschäft aus, da die individuellen Voraussetzungen unserer Branche nicht berücksichtigt wurden.	12,3	15,9	11,1
Sie betreffen uns in der Praxis nicht, weil Branchen-Vorgaben ohnehin strenger sind.	7,9	12,6	11,4
Sie betreffen uns nicht, da wir sie bereits übererfüllen.	10,8	9,5	12,9
Das kann ich nicht beurteilen.	51,6	30,3	40,3

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

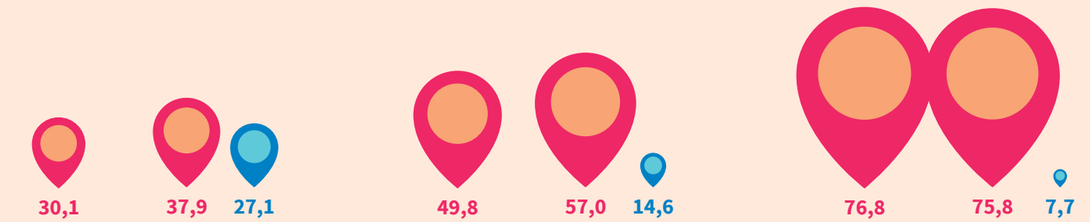
Standort-Relevanz des IT-Dienstleisters?

Relevanz des Standortes eines IT-Sicherheitsanbieters; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2022; in Prozent

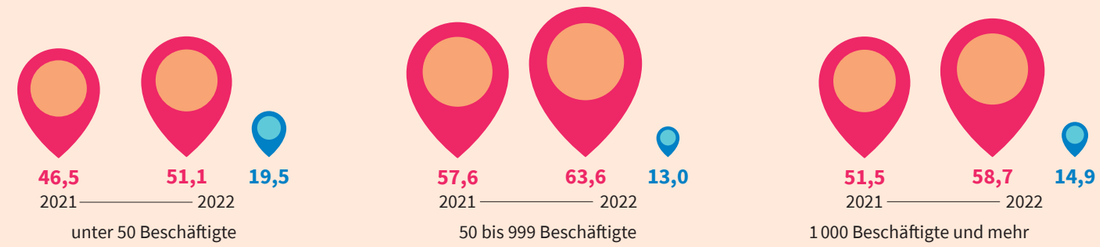
Wie wichtig ist es Ihnen, wo ein Anbieter von IT-Sicherheitslösungen seinen Standort hat?

Vergleich zum Vorjahr:
Anteil der Befragten, denen 2021 wichtig war, wo ein Anbieter seinen Standort hat, in Prozent: **52,2**

nach persönlicher Kompetenz



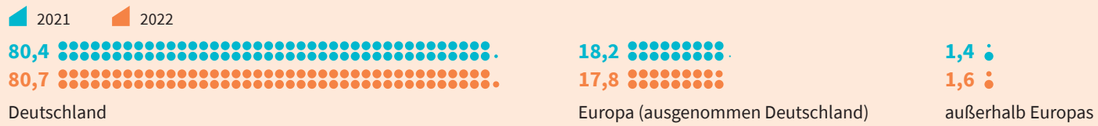
nach Unternehmensgröße



Quelle: Statista im Auftrag von G DATA

Heimatliebe

Bevorzugter Standort eines IT-Sicherheitsanbieters; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2022; in Prozent *



* Befragte, denen der Standort eines Anbieters für IT-Sicherheitslösungen (sehr) wichtig ist. Quelle: Statista im Auftrag von G DATA

Wen informieren im Schadensfall?

Meldung eines IT-Sicherheitsvorfalls nach Unternehmensgröße; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2022; in Prozent *

An welche der genannten Instanzen hat Ihr Unternehmen schon einmal einen IT-Sicherheitsvorfall gemeldet?

	Deutschland	unter 50 Beschäftigte	50 bis 999 Beschäftigte	1 000 Beschäftigte und mehr
BSI (Bundesamt für Sicherheit in der Informationstechnik)	**18,6**	5,7	25,6	25,9
BfDI (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit)	**16,7**	6,0	25,8	16,1
jeweilige Landesdatenschutzbehörde	**16,4**	7,6	22,5	18,7
andere zuständige Stelle	**7,5**	5,4	7,6	10,9
an keine der genannten Instanzen	**38,1**	61,4	27,2	21,8
Das kann ich nicht beurteilen.	**18,9**	17,7	15,1	28,5

* Befragte, die in der IT / EDV oder in der Geschäftsleitung arbeiten. Mehrfachnennung möglich. Quelle: Statista im Auftrag von G DATA

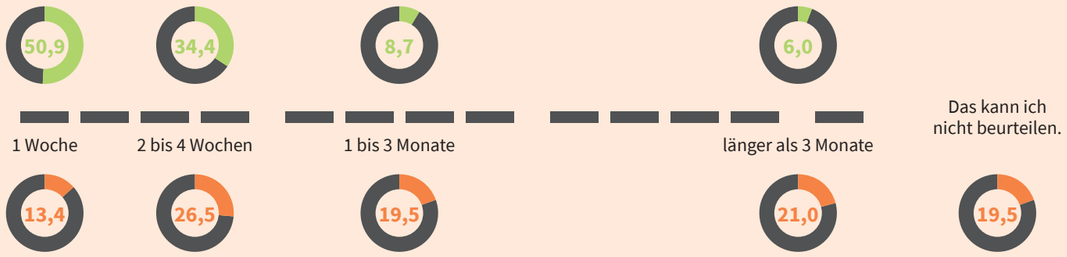
Unbemerkt und unbesorgt?

Geschätzte Dauer zwischen Hackerangriff und Auswirkungen; durchschnittliche Aufbewahrungsdauer von Log-Dateien; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2022; in Prozent

Zwischen einem Hackerangriff und den spürbaren Auswirkungen vergeht einige Zeit. Was glauben Sie, wie lange ein Hackerangriff in Unternehmen im Durchschnitt unbemerkt bleibt?

Wie lange hält Ihr Unternehmen Log-Dateien (Protokoll-Datei mit Informationen zu aufgetretenen Ereignissen) im Durchschnitt vor?

1 Woche



* Quelle: Statista im Auftrag von G DATA

Unsicherer geworden?

Veränderung der Wahrnehmung von IT-Sicherheit seit dem Ukraine-Krieg; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2022; in Prozent

Derzeit herrscht Krieg in der Ukraine. Wie hat sich Ihre Wahrnehmung bezüglich IT-Sicherheit seit dieser Zeit verändert?

37,2
höhere Wahrnehmung für das Thema

57,8
Wahrnehmung ist gleich geblieben.

5,0
geringere Wahrnehmung für das Thema

* Quelle: Statista im Auftrag von G DATA

Gut informiert?

Kommunikation von IT-Sicherheitslücken mit bundesweitem Ausmaß; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2022; in Prozent

Finden Sie, dass IT-Sicherheitslücken mit bundesweitem Ausmaß (z. B. Log4Shell) genügend in der Öffentlichkeit kommuniziert werden?

51,4
nein, zu wenig

17,5
nein, viel zu wenig

15,8
ja

15,2
Ich habe noch nie von solchen IT-Sicherheitslücken gehört.

Quelle: Statista im Auftrag von G DATA

Persönlich interessiert?

Interesse an IT-Sicherheitslücken mit bundesweitem Ausmaß; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2022; in Prozent

Wie sehr interessieren Sie sich bzw. würden Sie sich für IT-Sicherheitslücken mit bundesweitem Ausmaß (z. B. Log4Shell) und deren Folgen interessieren?

sehr interessiert	17,2
interessiert	46,4
weder noch	23,2
wenig interessiert	7,4
überhaupt nicht interessiert	5,9

(sehr) interessiert — wenig / überhaupt nicht interessiert

nach Geschlecht

männlich: 68,5 / 10,0

weiblich: 57,9 / 17,0

nach Alter

16 – 29 Jahre: 67,1 / 10,3

30 – 49 Jahre: 64,4 / 12,0

50 – 64 Jahre: 60,6 / 15,9

65 – 70 Jahre: 69,2 / 15,9

nach persönlicher Kompetenz im Bereich IT-Sicherheit

(sehr) geringe Kompetenz: 39,4 / 28,5

mittlere Kompetenz: 64,4 / 10,3

(sehr) große Kompetenz: 82,0 / 4,4

Quelle: Statista im Auftrag von G DATA

Eher differenziert?

Informationsquellen für IT-Sicherheitslücken mit bundesweitem Ausmaß; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2022; in Prozent *

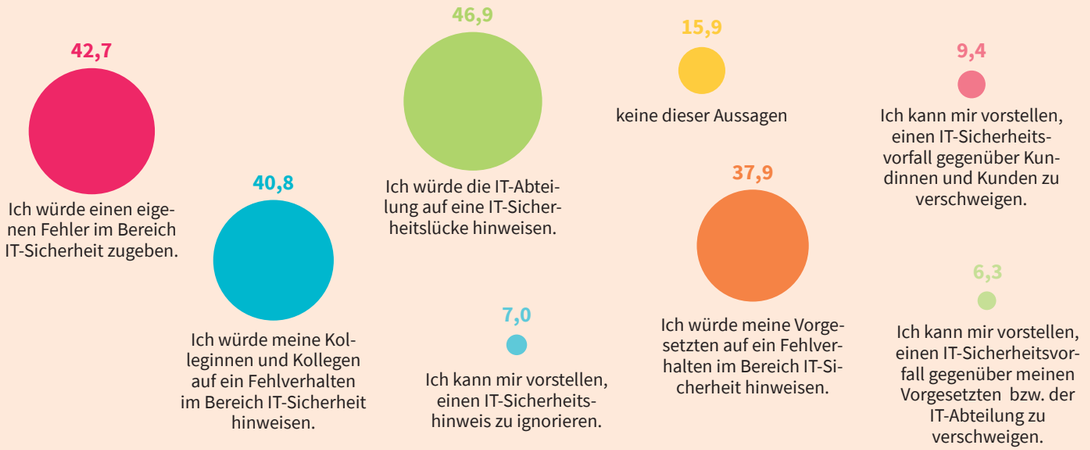
Wer liefert Ihnen verlässliche Informationen zu IT-Sicherheitslücken mit bundesweitem Ausmaß?

Beauftragter IT-Sicherheitsdienstleister	25,6
BSI (Bundesamt für Sicherheit in der Informationstechnik)	24,8
Beauftragter IT-Dienstleister	24,0
Fachmedien (z. B. Heise)	23,5
Verbände (z. B. Bundesverband für IT-Sicherheit, IHK)	16,9
Geräte-Hersteller	13,2
Berater	13,0
keine der genannten Quellen	21,6

* Befragte, die schon mal von IT-Sicherheitslücken mit bundesweitem Ausmaß gehört haben. Mehrfachauswahl möglich. Quelle: Statista im Auftrag von G DATA

Offen und ehrlich?

Zutreffende Aussagen rund um IT-Sicherheit; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2022; in Prozent *



nach Abteilung

Ich würde einen eigenen Fehler im Bereich IT-Sicherheit zugeben.

Forschung und Entwicklung	51,3
IT und EDV	50,9
Geschäftsleitung	48,6
Marketing und Vertrieb	46,6
Personal und Recruiting	45,7
andere Abteilung	39,8
Buchhaltung und Finanzen	39,8
Produktion und Fertigung	38,6
Rechtsabteilung	34,6

Ich würde die IT-Abteilung auf eine IT-Sicherheitslücke hinweisen.

Forschung und Entwicklung	62,0
IT und EDV	57,8
Marketing und Vertrieb	53,4
Produktion und Fertigung	46,6
Buchhaltung und Finanzen	46,5
Geschäftsleitung	45,1
Personal und Recruiting	44,2
andere Abteilung	42,4
Rechtsabteilung	41,9

Ich würde meine Kolleginnen und Kollegen auf ein Fehlverhalten im Bereich IT-Sicherheit hinweisen.

IT und EDV	52,5
Forschung und Entwicklung	51,3
Marketing und Vertrieb	43,1
Produktion und Fertigung	39,9
Buchhaltung und Finanzen	39,8
Rechtsabteilung	39,7
Geschäftsleitung	39,6
Personal und Recruiting	39,0
andere Abteilung	37,1

Ich würde meine Vorgesetzten auf ein Fehlverhalten im Bereich IT-Sicherheit hinweisen.

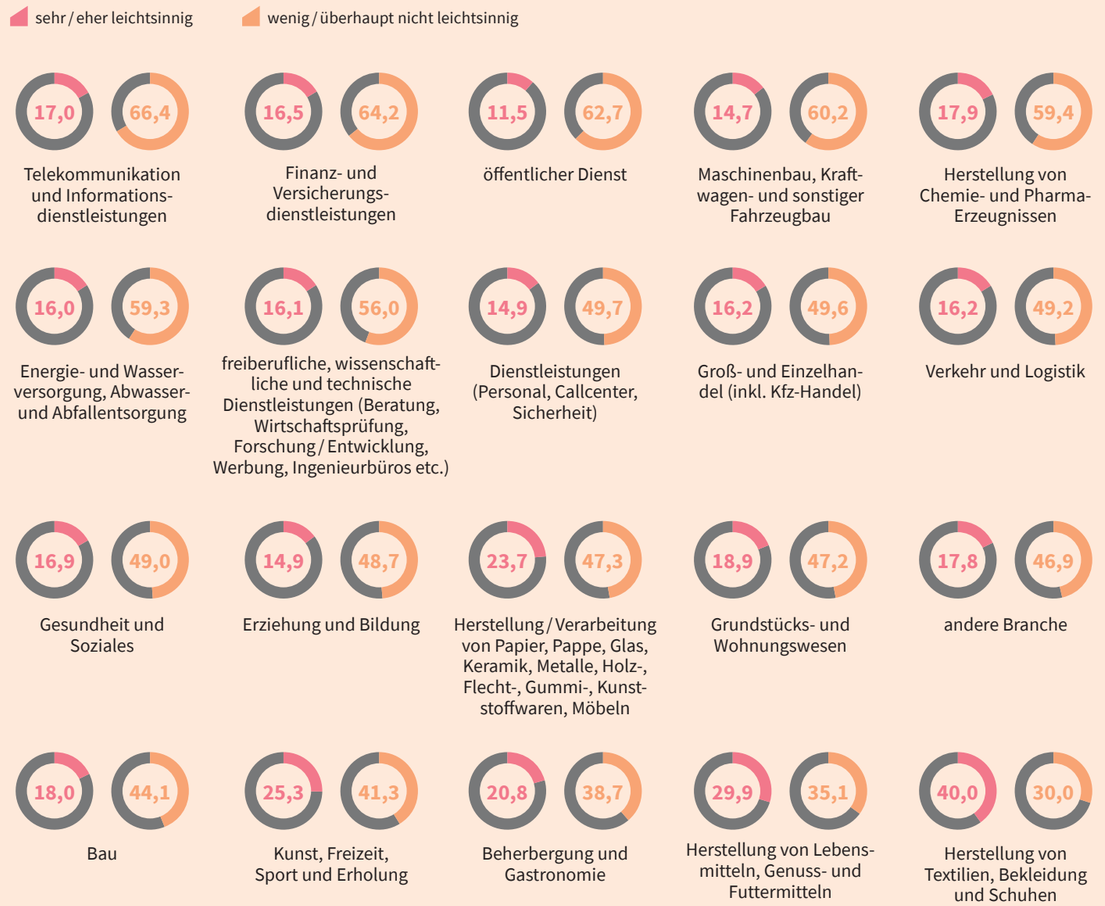
Forschung und Entwicklung	44,9
IT und EDV	43,9
Marketing und Vertrieb	42,4
Geschäftsleitung	38,7
Buchhaltung und Finanzen	37,9
Produktion und Fertigung	37,8
andere Abteilung	35,4
Rechtsabteilung	34,6
Personal und Recruiting	34,1

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

Vorsichtig oder leichtsinnig?

Einschätzung des Leichtsinns des Unternehmens beim Thema IT-Sicherheit; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2022; in Prozent

nach Branchen

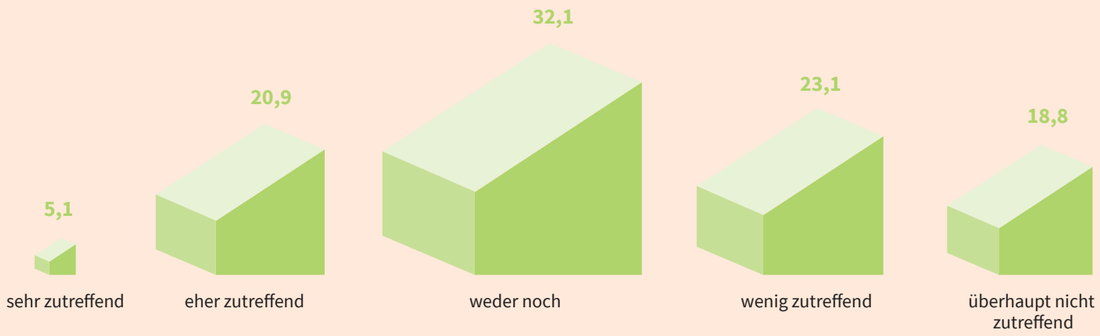


Quelle: Statista im Auftrag von G DATA

Augen zu und durch?

Zutreffen des Spruchs „Augen zu und durch“; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2022; in Prozent

Augen zu und durch – wie sehr trifft dieser Spruch auf die IT-Sicherheits- und -Schutzmaßnahmen in Ihrem privaten Umfeld zu?

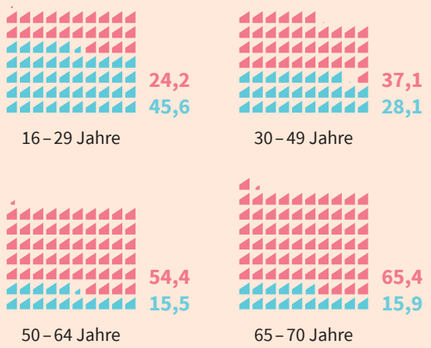


sehr / eher zutreffend

wenig / überhaupt nicht zutreffend

nach Kompetenz im Bereich IT-Sicherheit

nach Alter



sehr / eher zutreffend ist die Aussage für …

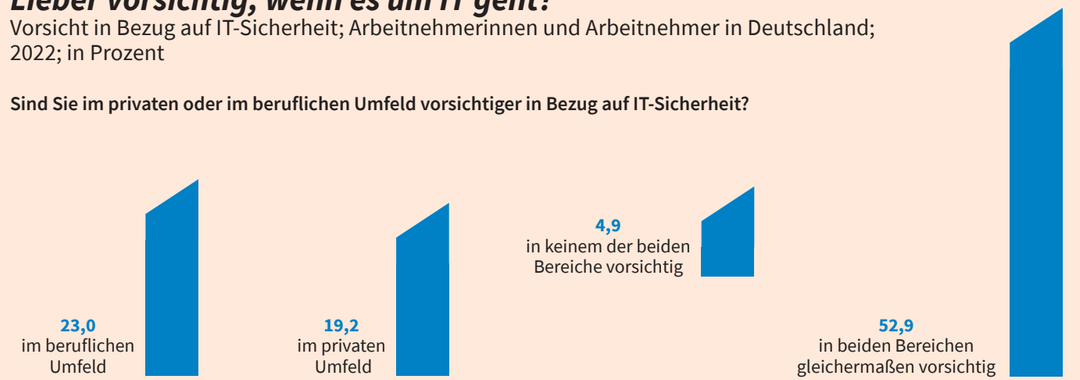
Befragte aus Marketing und Vertrieb	24,5
Befragte aus der Rechtsabteilung	37,5
Befragte, die einige Tage pro Woche im Homeoffice arbeiten	33,9
Befragte, die keine Homeoffice-Möglichkeit haben	20,5
Befragte aus der Branche Herstellung von Textilien, Bekleidung und Schuhen	54,3
Befragte aus der Branche Verkehr und Logistik	18,1

Quelle: Statista im Auftrag von G DATA

Lieber vorsichtig, wenn es um IT geht?

Vorsicht in Bezug auf IT-Sicherheit; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2022; in Prozent

Sind Sie im privaten oder im beruflichen Umfeld vorsichtiger in Bezug auf IT-Sicherheit?



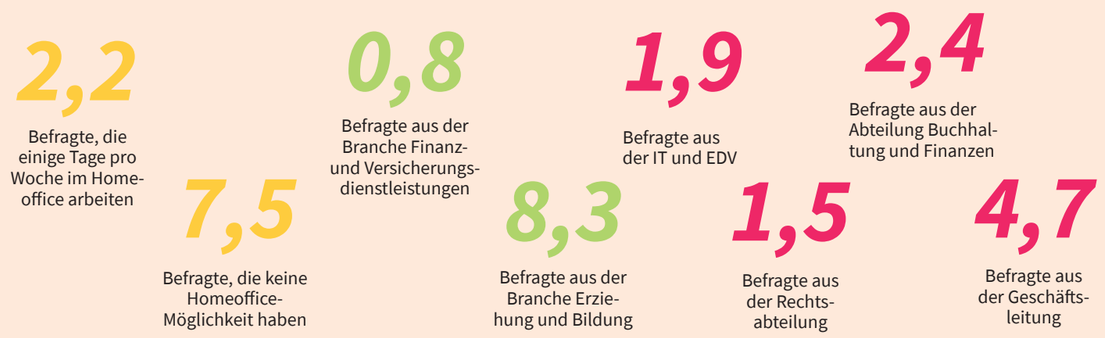
nach Alter

	16 – 29 Jahre	30 – 49 Jahre	50 – 64 Jahre	65 – 70 Jahre
im beruflichen Umfeld	39,1	25,6	13,8	7,5
im privaten Umfeld	22,9	18,1	18,9	20,6
in keinem der beiden Bereiche vorsichtig	4,7	4,9	5,2	3,7
in beiden Bereichen gleichermaßen vorsichtig	33,4	51,4	62,1	68,2

nach persönlicher Kompetenz im Bereich IT-Sicherheit

	(sehr) geringe Kompetenz	mittlere Kompetenz	(sehr) große Kompetenz
im beruflichen Umfeld	15,6	22,6	29,5
im privaten Umfeld	24,1	17,2	17,6
in keinem der beiden Bereiche vorsichtig	10,3	3,2	2,6
in beiden Bereichen gleichermaßen vorsichtig	50,0	57,1	50,3

in keinem der beiden Bereiche vorsichtig sind …



Quelle: Statista im Auftrag von G DATA

„Der Gegner wird keine Ruhe geben.“

Michael Kramm, verantwortlich für IT-Sicherheit beim Volkswagen-Konzern, über den nie endenden Wettlauf mit kriminellen Hackern

Text: Andreas Molitor

Michael Kramm, 52 Jahre, Diplom-Volkswirt, arbeitet seit 1997 bei Volkswagen. Im Laufe der Jahre bekleidete er verschiedene Leitungspositionen bei Fahrzeug-, Fabrik- und IT-Projekten im In- und Ausland, unter anderem in Mexiko, Brasilien und Argentinien sowie im Stammwerk Wolfsburg. Vor anderthalb Jahren übernahm er die Leitung der konzernweiten IT-Sicherheit.

• An das vorige Weihnachtsfest denkt Michael Kramm nur ungern zurück. „Wir hatten eine Verwundbarkeit, die uns sieben Wochen auf Trab gehalten hat“, erinnert er sich. „An den Weihnachtstagen und auch Silvester und Neujahr war ich mehr im Büro als zu Hause.“ Ein Cyberangriff auf die IT-Sicherheitsarchitektur des größten Autoherstellers Europas hielt Kramm und sein Team in Atem. Was genau passiert war und an welcher Stelle die Attacke erfolgte, darf Kramm natürlich nicht verraten. Für den Chief Information Security Officer der Volkswagen AG ist Verschwiegenheit oberstes Gebot – ein Grund, warum sein Profil beim Business-Netzwerk LinkedIn so denkbar dürftig ausfällt.

Der Angriff versetzte seine Mannschaft in einen Notfallmodus, fast wie bei einer Naturkatastrophe. Alarmierungsketten wurden in Gang gesetzt, Expertenteams in kontinuierliche Wechselschichten eingeteilt, Notfallhandbücher Punkt für Punkt abgearbeitet. „In diesem Modus fuhren wir, bis wir das Problem isoliert und behoben hatten, und zwar 24 Stunden am Tag, 7 Tage die Woche“, erzählt der Oberaufseher über die IT-Sicherheit beim VW-Konzern. „Das ist ein Knochenjob.“

Wie werden Sie darauf aufmerksam, dass sich im Cyberspace eine Gefahr gegen Ihr Unternehmen zusammenbraut?
Michael Kramm: Manchmal erhalten wir Hinweise, etwa von den IT-Sicherheitsexperten aus dem Bundesinnenministerium, von Lieferanten, die Opfer eines Cyberangriffs wurden, oder von anderen Autoherstellern. Im vergangenen Jahr entdeckte ein großer Sicherheitsanbieter eine Kampagne, die mit einem Phishing-Versuch gezielt die deutsche Autoindustrie inklusive Händler und Werkstätten ins Visier nahm. So etwas versetzt uns sofort in den Aktionsmodus. Wir schauen uns das alles ganz genau an und fragen uns in jedem einzelnen Fall, ob ein solcher Angriff auch bei uns möglich gewesen wäre.

Und wenn einer Kundin oder einem Kunden an seinem gerade neu gekauften Fahrzeug etwas merkwürdig vorkommt?
Auch dann sind wir im Spiel. Im Normalfall fährt der Kunde ja zuerst zu seinem Händler. Der muss in der Lage sein, zu unterscheiden, ob es sich um einen technischen Fehler handelt, der in der Werkstatt behoben werden kann, oder ob tatsächlich 〉

jemand versucht, das Fahrzeug zu attackieren. Wir haben unsere Händler in den vergangenen drei Jahren intensiv geschult, damit sie das beurteilen können. Wenn ein Cyberangriff nicht auszuschließen ist, kümmern wir uns intensiv um das Fahrzeug. Wir steigen auf jeden Vorfall ein.

Was ist ein Vorfall?
Wenn irgendetwas sich nicht so verhält, wie es sein soll. Das reicht als Anhaltspunkt für einen Verdacht.

Mit wie vielen solcher Vorfälle haben Sie zu tun?
Hier am Standort Wolfsburg bearbeiten wir durchschnittlich 200 Fälle pro Monat. Das ist sozusagen unser tägliches Geschäft.

Etwas Komplexeres als die IT-Sicherheit in einem weltweit agierenden Autokonzern ist kaum vorstellbar. Michael Kramm mit seinem 160 Mitarbeitenden starken Team trägt die Verantwortung für den Schutz des Gesamtkonzerns vor den Angriffen krimineller Hacker. Aber damit ist es nicht getan. Jede Region auf der Welt, in der Volkswagen Fabriken betreibt, und jede einzelne Marke des Konzerns, von Seat und Škoda über VW und Audi bis Porsche, Bentley und Lamborghini, hat eine eigene Organisation für Cybersicherheit. Wenn alle virtuell miteinander konferieren, einmal im Jahr, „sind durchaus 700, 800 Leute an Bord", erzählt Kramm.

Alle arbeiten Hand in Hand, entwerfen gemeinsame Sicherheitsprogramme und planen bis ins letzte Detail konzertierte Roll-outs. Die Sicherheitsprofis wiederum kooperieren ständig mit der Elektronikentwicklung der einzelnen Marken, mit der Qualitätssicherung, dem Vertrieb, dem Rechtswesen. Das kostet einiges, Kramm spricht von einem jährlichen Budget in dreistelliger Millionenhöhe.

Ein besonders sensibler Punkt ist die Armada der Zulieferer. Einige wurden in jüngster Zeit Opfer von Cyberangriffen. Beim Abgastechnik- und Klimaspezialisten Eberspächer beispielsweise legten Hacker im Oktober vorigen Jahres die Rechnersysteme weltweit lahm; fast zwei Wochen stand an allen neun deutschen Standorten die Produktion still. Der Schaden: vermutlich weit mehr als 100 Millionen Euro.

Wie können Sie verhindern, dass kriminelle Hacker über die Zulieferer sensible Daten über Prototypen, Innovationen und Preise abgreifen? Oder sich über die IT-Schnittstellen direkt in Ihre Systeme fressen?
Bevor wir eine langfristige Partnerschaft mit einem Zulieferer eingehen, unterziehen wir das Niveau der IT-Sicherheit beim Lieferanten einem intensiven Check. Unsere Beschaffungsbedingungen haben wir in puncto Cybersecurity in den vergangenen Jahren sehr straff angezogen.

Gibt es denn keine einheitlichen, für alle Lieferanten verbindlichen Standards?
Zulieferer, die Entwicklungs- und Konstruktionsdaten mit Automobilherstellern austauschen wollen, müssen ihre Informationssicherheit über eine Plattform namens Tisax, ein Kürzel für Trusted Information Security Assessment Exchange, von unabhängigen Prüfern zertifizieren lassen. Auf dieser Plattform können wir den Sicherheitsstatus potenzieller Lieferanten ablesen.

„Eine absolute Sicherheit gibt es leider nicht. Aber wir tun alles Nötige, um möglichst nahe an die hundert Prozent zu kommen."

Ein Zertifikat ist das eine – selber nachschauen ist vielleicht sicherer. Tun Sie das auch?
Ja, in Einzelfällen. Wir haben ein Spezialistenteam im Konzern, das vor Ort geht, wenn ein Lieferant beispielsweise eine neue Software einführt. Wir unterziehen dann die IT des Zulieferers einem Stresstest. Besonders streng sind natürlich die Kriterien zur Verschlüsselung von Daten mit hohem oder sehr hohem Schutzbedarf.

Was wäre ein Beispiel für Daten mit hohem Schutzbedarf?
Das sind vor allem Informationen über Prototypen. Die meisten Zulieferer arbeiten ja gleichzeitig für mehrere Autohersteller. Sie müssen dafür sorgen, dass die Prototyp-Daten der verschiedenen Hersteller strikt voneinander getrennt werden und nur den jeweils dafür verantwortlichen Teams zugänglich sind.

In der vordigitalen Ära der Industriespionage kam es vor, dass Kartons mit geheimen Konstruktionsunterlagen und vertraulichen Informationen über Einkaufspreise und Herstellungskosten in Privatwohnungen von leitenden Mitarbeitenden gefunden wurden, die kurz zuvor von einem Hersteller zu einem Konkurrenten gewechselt waren. Heute muss sich dafür niemand mehr nächtens an den Kopierer stellen. Die Produktionsanlagen der Autofabriken sind weltweit vernetzt – und somit potenzielle Einfallstore für Industriespionage oder erpresserische Hacker, die mit einem Kryptotrojaner die Computer des Unternehmens verschlüsseln, Fabriken zum Stillstand bringen und die Daten, ähnlich wie bei einer Geiselnahme, erst nach einer Lösegeldzahlung wieder freigeben.

Angenommen es gäbe einen erfolgreichen Großangriff auf das Stammwerk in Wolfsburg – steht dann dort alles still?
Im schlimmsten Fall nicht nur dort. Die Fertigungssysteme werden heute ja nicht nur für eine Fabrik entwickelt, programmiert, aufgebaut und in Betrieb genommen. Sie finden sich, miteinander vernetzt, an mehreren Standorten unterschiedlicher Konzernmarken.

Wie schützen Sie sich gegen Angriffe auf die Produktion?
Indem wir das Schutzsystem von vornherein auf ein ganz anderes Niveau bringen. Wir schauen uns die Schnittstellen genau an. Von woher kommen die Daten, wohin werden sie wieder abgegeben? Jede neue Applikation wird vor ihrer Einführung einem IT-Sicherheitsassessment unterzogen und auch im laufenden Betrieb überwacht, wie sie sich verhält. Sobald wir eine Anomalie entdecken, steigen wir tiefer ein.

Die nächste Generation von Angreifern hat sich bereits warmgelaufen. Sie haben es nicht auf die Fabriken abgesehen, sondern attackieren gleich die Autos. Die Fahrzeuge der neuesten Generation sind „Connected Cars", im Grunde genommen elektrisch – oder einstweilen noch mit Verbrenner – angetriebene mobile Endgeräte, die ständig Daten generieren, verarbeiten und weitergeben. Smartphones auf Rädern sozusagen, vollgestopft mit hundert oder mehr elektronischen Steuergeräten, deren Software ohne Werkstatttermin drahtlos über die Cloud aktualisiert wird.

Derartige Fahrzeuge sind elektronisch nicht unverwundbar. White-Hat-Hacker haben in der Vergangenheit mehrfach demonstriert, dass es Angreifern im Extremfall gelingen kann, von außen die Kontrolle über ein Auto zu übernehmen, wenn die Sicherheitsarchitektur Lücken aufweist.

Sind erst einmal Millionen autonom fahrender Autos unterwegs, könnte das Bedrohungspotenzial weiter steigen – wenn auch dystopisch anmutende Szenen wie jene berühmte aus der achten Folge des Kino-Blockbusters „The Fast and the Furious", wo Hunderte von Cyberterroristen gehackte autonom fahrende Autos Massenkarambolagen verursachen und zu Dutzenden aus den oberen Etagen von Parkhäusern auf die Straße stürzen, von der Realität denkbar weit entfernt sind.

Beim Technologie-Wettstreit um das Connected Car will auch VW in der ersten Liga spielen. Vor allem der Rückstand zum amerikanischen Rivalen Tesla soll möglichst schnell aufgeholt werden. Die eigenen Entwicklungsabteilungen wurden auf Geheiß des Konzernvorstands bereits auf „Software First" getrimmt.

Ein Traditionshersteller wandelt sich in ein digitales Schnellboot mit angegliederter Blechbiegerei – was bedeutet das für die IT-Sicherheit?
Mit dem Connected Car wird das Wettrennen zwischen der IT-Sicherheit und potenziellen Angreifern auf eine neue Umlaufbahn katapultiert. Cybersicherheit ist jetzt Teil des gesamten Fahrzeuglebenszyklus. Das ist ein Paradigmenwechsel. Die IT-Sicherheit muss mit dem enormen und sich ständig beschleunigenden technologischen Wandel bei den Fahrzeugen Schritt halten. Es gibt keine Alternative, denn der Gegner wird keine Ruhe geben und jede Schwachstelle ausnutzen.

Hauptangriffspunkt ist die Fahrzeug-Software. Wie sorgen Sie da für Sicherheit?
Der Volkswagen-Konzern hat ja entschieden, diese Software selbst zu schreiben. Wir wollen dieses Zukunftsfeld nicht den Tech-Unternehmen aus dem Silicon Valley überlassen. Unsere Tochtergesellschaft Cariad entwickelt jetzt das gemeinsame zukünftige Betriebssystem für die Autos der VW-Marken, das vom Infotainment im Cockpit bis zum autonomen Fahren alles steuert. Das bietet uns die Chance, digitale Sicherheit von Anfang an mit höchster Priorität zu integrieren.

Cariad hat eine eigene IT-Sicherheitsorganisation. Lange bevor die Software auf dem Prototypenstand oder auf der Straße erprobt wird, sorgen die dortigen Kolleginnen und Kollegen mit harten Tests für einen größtmöglichen Schutz gegen Cyberattacken. Eine absolute Sicherheit gibt es leider nicht. Aber wir tun alles Nötige, um möglichst nahe an die hundert Prozent zu kommen.

Theoretisch ließe sich vielen Cyberkriminellen leicht das Wasser abgraben – wenn man nur möglichst früh, noch bevor sie einen Angriff starten, von ihren Plänen erführe. Hier und dort ist zu lesen, dass die Autohersteller White-Hat-Hacker, also firmeneigene oder durch Prämien entlohnte externe Hacker sowie Cybercrime-Sicherheitsspezialfirmen engagieren, damit sie absichtlich in die Systeme eindringen und die sozialen Medien, einschlägige Foren und vor allem das Darknet gezielt nach Hinweisen auf geplante oder laufende Angriffe durchforsten.

Das amerikanische Cybersecurity-Start-up Spycloud schleust sogar gezielt Spione in einschlägige Darknet-Foren ein. „Bei Volkswagen praktizieren wir so etwas in einem gewissen Rahmen", mehr ist Michael Kramm dazu nicht zu entlocken. Erkenntnisse aus den Weiten des Darknets über bevorstehende Attacken seien aber durchaus willkommen. Außerdem lasse man sich von White-Hat-Hackern ganz bewusst regelmäßig angreifen – „um festzustellen, wo es in unserer Sicherheitsarchitektur noch Lücken gibt". Der Mensch, schließt Kramm, „ist also in diesem Wettlauf zwischen uns und den Angreifern absolut nicht unwichtig. Da steht nicht nur IT gegen IT."

G DATA INDEX – CYBERSICHERHEIT

Kein Tag ohne neue Meldungen zu Cyberattacken. Jeder vierte Nutzer in Deutschland ist schon einmal Opfer von Cyberkriminalität geworden. Wie sicher fühlen wir uns angesichts der latenten Bedrohung – beruflich und privat? Halten wir uns für kompetent, informiert und für ausreichend geschützt? Der G DATA Index gibt Auskunft.

Turbulente Zeiten

Index-Veränderung gegenüber dem Basisjahr 2021; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2022

Lesehilfe: Der Wert des Index im Jahr 2021 beträgt 100. Ein Indexwert von 98 entspricht einem Rückgang von 2 Prozent gegenüber dem Wert des Vorjahres und bedeutet: Die gefühlte Sicherheit hat abgenommen. Ein Indexwert von 103 entspricht einem Anstieg von 3 Prozent gegenüber dem Wert des Vorjahres – die gefühlte Sicherheit hat also zugenommen.

Deutschland

Index

58,4 Referenzwert (2021)
57,0 2022
98

Wissen	Sicherheit		Risiko	
53,3 Referenzwert (2021)	74,3 Referenzwert (2021)		47,5 Referenzwert (2021)	
51,5 2022	71,4 2022		48,0 2022	
97	**96**		**101**	
	96 privates Umfeld	96 berufliches Umfeld	102 privates Umfeld	100 berufliches Umfeld

unter 30 Jahre

60,2 Referenzwert (2021)
59,9 2022
100

Wissen	Sicherheit		Risiko	
101	**98**		**100**	
	97 privates Umfeld	100 berufliches Umfeld	97 privates Umfeld	102 berufliches Umfeld

30 bis 49 Jahre

58,4 Referenzwert (2021)
56,8 2022
97

Wissen	Sicherheit		Risiko	
97	**95**		**103**	
	96 privates Umfeld	94 berufliches Umfeld	104 privates Umfeld	101 berufliches Umfeld

50 bis 64 Jahre

57,6 Referenzwert (2021)
55,7 2022
97

Wissen	Sicherheit		Risiko	
93	**97**		**100**	
	96 privates Umfeld	98 berufliches Umfeld	102 privates Umfeld	98 berufliches Umfeld

65 Jahre und älter

58,3 Referenzwert (2021)
59,8 2022
103

Wissen	Sicherheit		Risiko	
111	**98**		**101**	
	97 privates Umfeld	99 berufliches Umfeld	99 privates Umfeld	104 berufliches Umfeld

weiblich

56,2 Referenzwert (2021)
55,4 2022
98

Wissen	Sicherheit		Risiko	
99	**96**		**101**	
	96 privates Umfeld	97 berufliches Umfeld	103 privates Umfeld	99 berufliches Umfeld

männlich

60,3 Referenzwert (2021)
58,4 2022
97

Wissen	Sicherheit		Risiko	
95	**96**		**101**	
	96 privates Umfeld	96 berufliches Umfeld	101 privates Umfeld	100 berufliches Umfeld

Index
Wissen
Sicherheit
Risiko
privates Umfeld
berufliches Umfeld

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

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

Ein Anstieg des Vertrauensindex bedeutet eine Zunahme von Wissenskompetenz (Wissen) und Sicherheitsgefühl (Sicherheit) und eine Abnahme von Risikoempfinden (Risiko).

Eine Abnahme des Vertrauensindex bedeutet eine Reduktion von Wissenskompetenz (Wissen) und Sicherheitsgefühl (Sicherheit) und ein höheres Risikoempfinden (Risiko).

Referenzwert:
Der Referenzwert = der Anteil der Befragten in Prozent

Quelle: Statista im Auftrag von G DATA

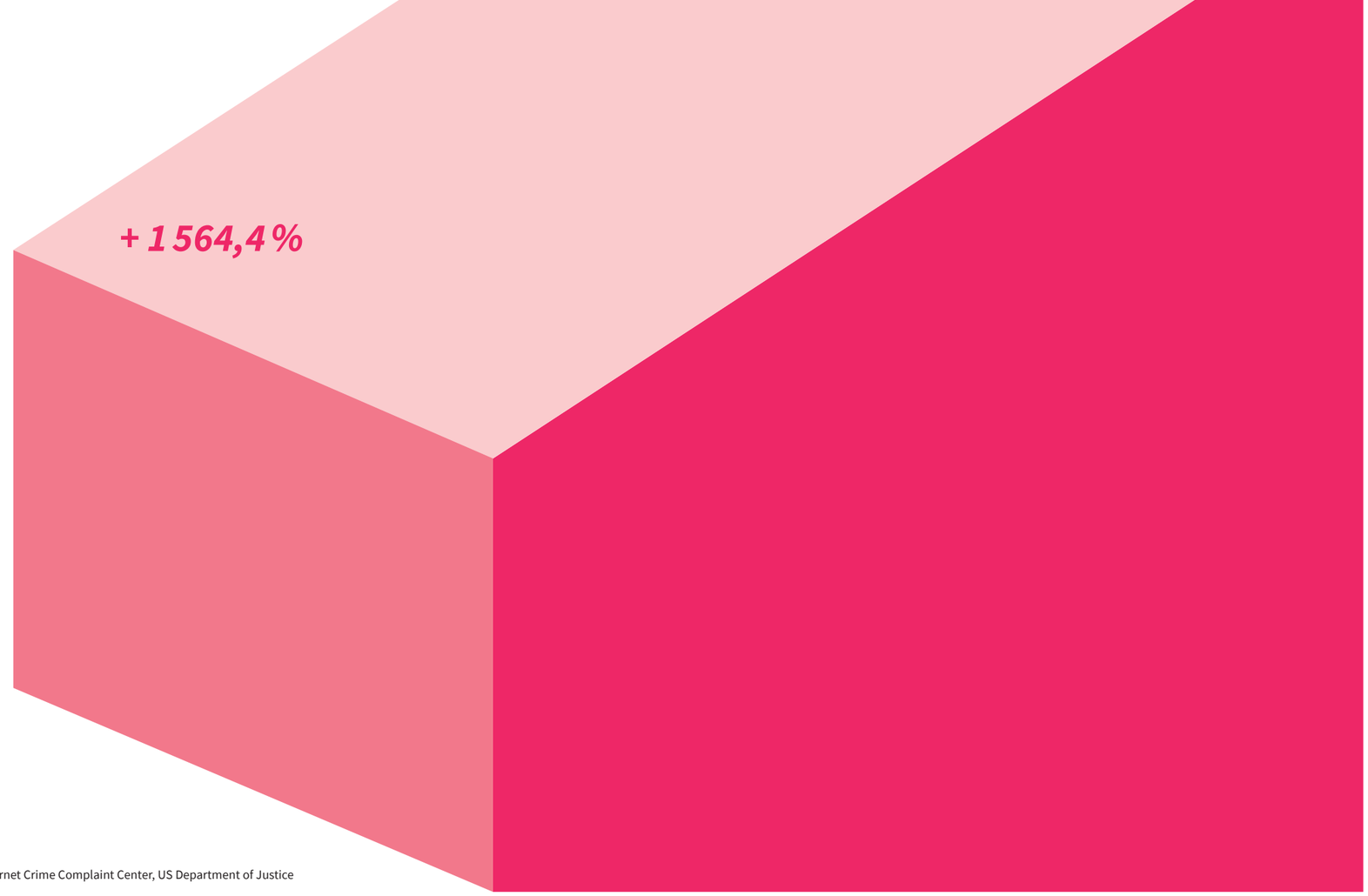
WELT

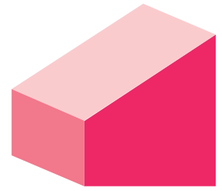
Die Zahl der Cyberattacken steigt, die Bedrohung für Länder und Infrastrukturen weltweit ist massiv. Immer neue Angriffstaktiken fluten die Systeme – und fast immer bildet der Mensch das Einfallstor für kriminelle Aggressoren. Wie groß sind die Risiken, womit müssen wir rechnen, wie gut sind wir gewappnet – und zu welchem Preis?

Manipuliert und abgezockt

Die Top-5-Straftaten nach Berichten an das Internet Crime Complaint Center (FBI); Zahl gemeldeter Fälle; weltweit

2016 2021 Veränderung 2016 – 2021



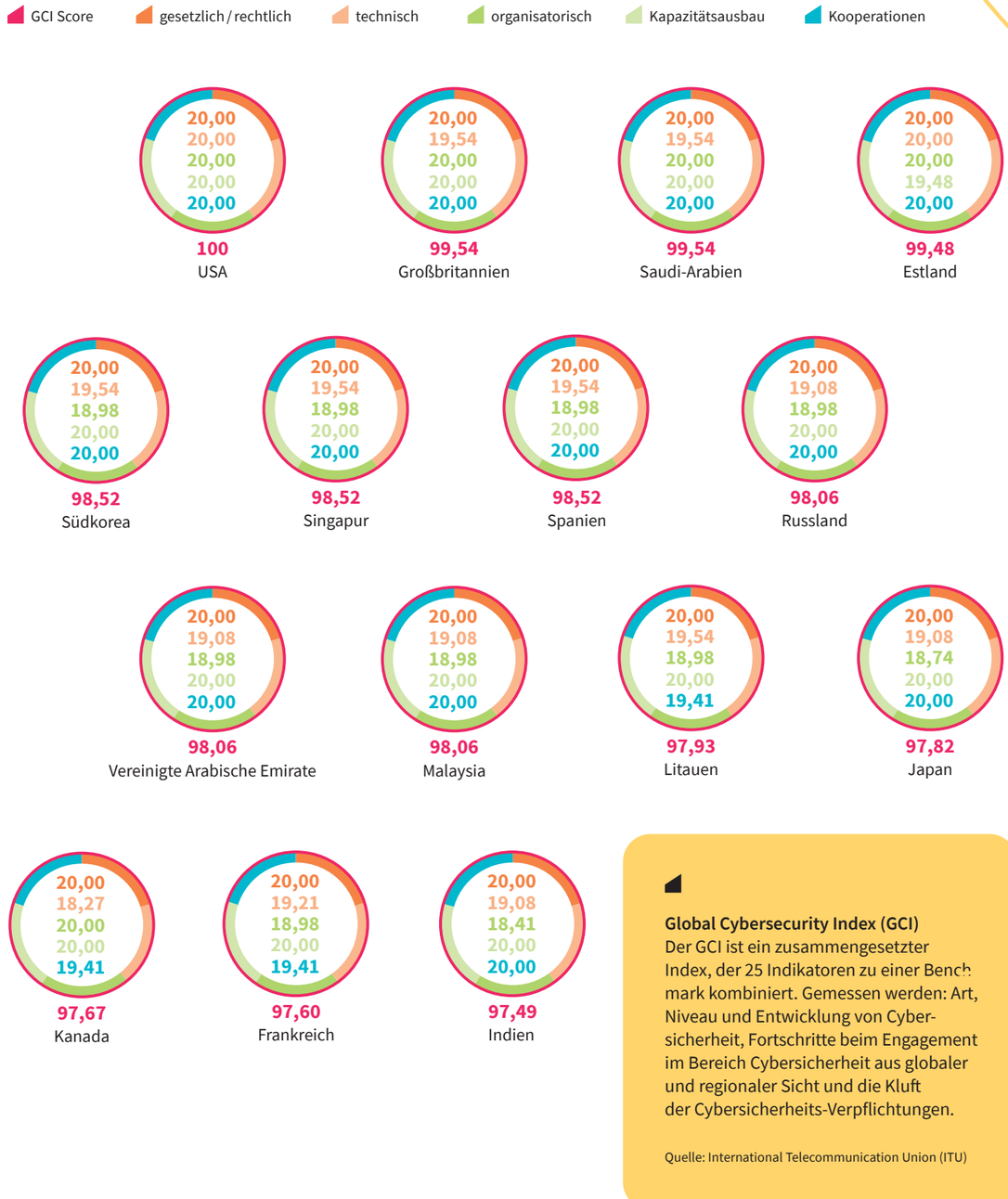


Quellen: FBI, Internet Crime Complaint Center, US Department of Justice

Cyberbegriffe-Übersicht im Glossar auf Seite 100 – 103

Benchmark: Vereinigte Staaten

Global Cybersecurity Index (GCI) – Länder mit dem höchsten Engagement in Cybersicherheit; 2020; Index



Global Cybersecurity Index (GCI)
Der GCI ist ein zusammengesetzter Index, der 25 Indikatoren zu einer Benchmark kombiniert. Gemessen werden: Art, Niveau und Entwicklung von Cybersicherheit, Fortschritte beim Engagement im Bereich Cybersicherheit aus globaler und regionaler Sicht und die Kluft der Cybersicherheits-Verpflichtungen.

Quelle: International Telecommunication Union (ITU)

Quelle: International Telecommunication Union (ITU)

Mittelmaß: Deutschland

GCI: Länder mit dem höchsten Engagement in Cybersicherheit nach Regionen; 2020; Index

Afrika

Mauritius	96,89
Tansania	90,58
Ghana	86,69
Nigeria	84,76
Kenia	81,70
Benin	80,06
Ruanda	79,95
Südafrika *	78,46
Uganda	69,98
Sambia	68,88

Nord- und Südamerika

USA *	100,00
Kanada *	97,67
Brasilien	96,60
Mexiko	81,68
Uruguay	75,15
Dominikanische Republik	75,07
Chile	68,83
Costa Rica	67,45
Kolumbien	63,72
Kuba	58,76

Arabische Staaten

Saudi-Arabien	99,54
Vereinigte Arabische Emirate	98,06
Oman	96,04
Ägypten	95,48
Katar	94,50
Tunesien	86,23
Marokko	82,41
Bahrain	77,86
Kuwait	75,05
Jordanien	70,96

Asien-Pazifik

Südkorea	98,52
Singapur	98,52
Malaysia	98,06
Japan	97,82
Indien	97,49
Australien	97,47
Indonesien	94,88
Vietnam	94,55
China	92,53
Thailand	86,50
Neuseeland *	84,04

Gemeinschaft unabhängiger Staaten

Russland	98,06
Kasachstan	93,15
Aserbaidschan	89,31
Usbekistan	71,11
Belarus	50,57
Armenien *	50,47
Kirgisistan	49,64
Tadschikistan *	17,10
Turkmenistan *	14,48

Europa

Großbritannien	99,54
Estland	99,48
Spanien	98,52
Litauen	97,93
Frankreich	97,60
Türkei	97,50
Luxemburg	97,41
Deutschland	97,41
Portugal	97,32
Lettland	97,28
Niederlande *	97,05

* keine Antwort auf den Fragebogen / die vom GCI-Team gesammelten Daten. Quelle: International Telecommunication Union (ITU)

Weltweit im Dienst der Sicherheit

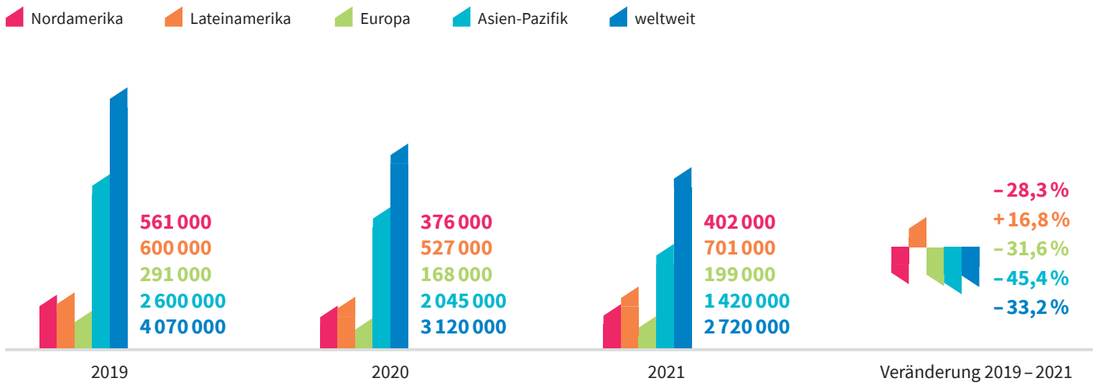
Zahl der Fachkräfte im Bereich Cybersicherheit; weltweit

	2019	2020	2021	Veränderung 2019 – 2021
Nordamerika	888 700	981 120	1 266 158	42,5 %
USA	804 700	879 157	1 142 462	42,0 %
Kanada	84 000	101 963	123 696	47,3 %
Lateinamerika	827 000	1 048 399	1 096 876	32,6 %
Mexiko	341 000	421 750	515 527	51,2 %
Brasilien	486 000	626 650	581 349	19,6 %
Europa	543 000	830 187	1 086 146	100,0 %
Großbritannien	289 000	365 823	300 087	3,8 %
Frankreich	121 000	118 302	146 808	21,3 %
Deutschland	**133 000**	**175 159**	**464 782**	**249,5 %**
Irland	k. A.	14 212	15 028	k. A.
Spanien	k. A.	122 284	124 336	k. A.
Niederlande	k. A.	34 406	35 106	k. A.
Asien-Pazifik	544 000	625 265	743 075	36,6 %
Australien	107 000	108 950	134 690	25,9 %
Japan	193 000	226 269	276 556	43,3 %
Singapur	43 000	57 765	92 744	115,7 %
Südkorea	201 000	232 281	239 085	18,9 %
weltweit	2 802 700	3 484 971	4 192 255	49,6 %

Quelle: (ISC)²

Weltweit händeringend gesucht

Personalmangel im Bereich Cybersicherheit nach Regionen; weltweit



Im Jahr 2021 fehlten weltweit **2,72 Millionen Fachkräfte** im Bereich Cybersicherheit. In **Deutschland** waren es **68 000**.

Quelle: (ISC)²

Gewaltige Investitionen

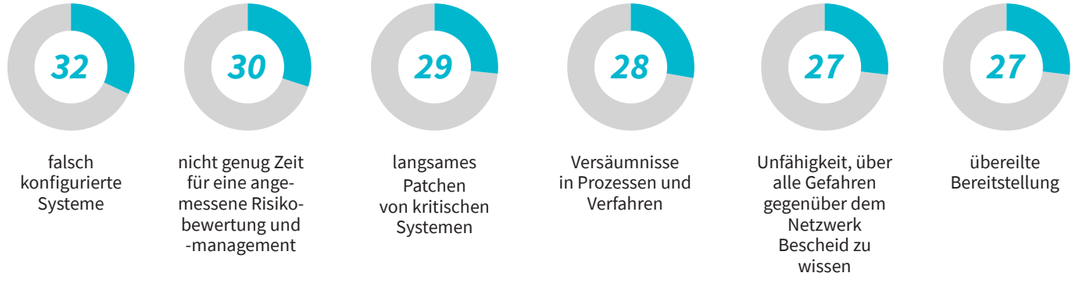
Top-Investitionen in Technologie, um dem Personalmangel entgegenzuwirken; weltweit; 2021; in Prozent *

Nutzung von Cloud-Dienstleistern	38
Erhöhung des Einsatzes von Intelligenz und Automatisierung für manuelle Cybersicherheitsaufgaben	37
Anwendung von Intelligenz und Automatisierung bei bestehenden Prozessen	37
Einbeziehung von Intelligenz und Automatisierung als Teil der Lösungsauswahlkriterien	35
frühere Einbindung von Cybersicherheitsmitarbeitenden in Produktdesign und -entwicklung	34
DevSecOps	34
Nutzung von Sicherheitssoftware-as-a-Service	33
frühere Einbindung von Cybersicherheitsmitarbeitenden in Beziehungen mit Dritten	32
Entlastung von vorhandenem Cybersicherheitspersonal, damit der Fokus auf wichtigen Aktivitäten liegt	31
Einsatz von Vertragspartnerinnen und Vertragspartnern	23
Nutzung neuer Geschäftsmodelle	23

* Mehrfachauswahl möglich. Quelle: (ISC)²

Gewaltige Probleme

Konsequenzen von Personalmangel im Bereich Cybersicherheit; weltweit; 2021; in Prozent *



* Mehrfachauswahl möglich. Quelle: (ISC)²

Gewaltige Unterschiede

Durchschnittliches Gehalt von Fachkräften im Bereich Cybersicherheit; weltweit; 2021; in Euro

Nordamerika	101 377
Lateinamerika	27 595
Europa	66 473
Asien-Pazifik	51 783
mit Cybersicherheitszertifizierung	77 557
ohne Cybersicherheitszertifizierung	49 696

Quelle: (ISC)²

Vervielfacht

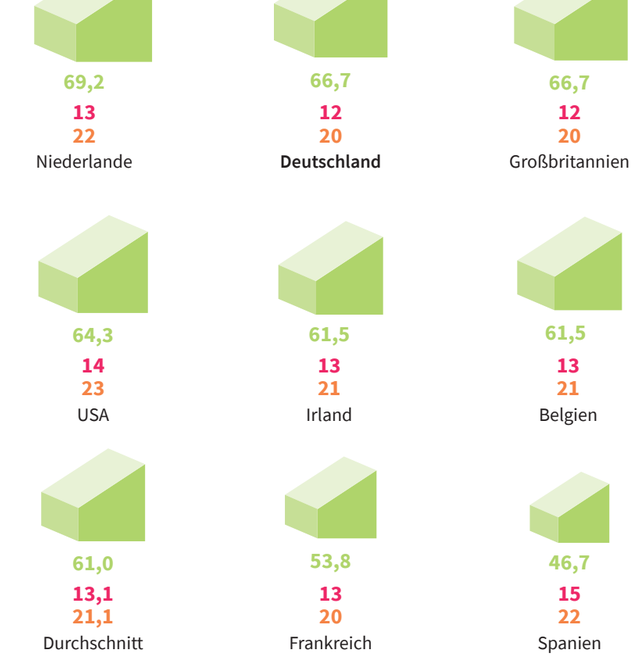
Durchschnittliche Jahresausgaben für Cybersicherheit nach Unternehmensgröße; ausgewählte Länder (B, F, D, IRL, NL, E, GB, USA); 2021; in Euro *

	2020	2021
1 bis 9 Mitarbeitende	11 643	104 591
10 bis 49 Mitarbeitende	69 534	334 045
50 bis 249 Mitarbeitende	217 538	269 163
250 bis 999 Mitarbeitende	755 400	1 629 403
1 000 Mitarbeitende und mehr	7 029 440	11 045 650

* Nach Angaben der Expertinnen und Experten, die in Unternehmen für die Strategie zur Cybersicherheit zuständig sind. Quelle: Hiscox

Vergrößert

Anteil der Ausgaben für Cybersicherheit am IT-Budget; ausgewählte Länder; in Prozent



Quelle: Hiscox

Vermessen

Digitalisierungsgrad nach DESI-Index; Europäische Union; 2021; Index

Dänemark	70,1
Finnland	67,1
Schweden	66,1
Niederlande	65,1
Irland	60,3
Malta	59,6
Estland	59,4
Luxemburg	59,0
Spanien	57,4
Österreich	56,9
Belgien	54,1
Deutschland	**53,7**
Slowenien	52,8
Litauen	51,8
EU	50,7
Frankreich	50,6
Portugal	49,9
Lettland	49,5
Tschechien	47,4
Kroatien	46,0
Italien	45,5
Zypern	43,5
Slowakei	43,2
Ungarn	41,2
Polen	41,0
Griechenland	37,3
Bulgarien	36,8
Rumänien	32,9

Quelle: Europäische Kommission

DESI = Digital Economy and Society Index
Der **DESI-Gesamtindex**, 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 %).
Humankapital: Die DESI-Dimension Humankapital berechnet als gewichteter Durchschnitt der beiden Subdimensionen: 1a) Internet-Nutzerkompetenz (50 %) und 1b) Fortgeschrittene Fähigkeiten und Entwicklung (50 %).
Konnektivität: Die DESI-Konnektivitätsdimension berechnet als gewichteter Durchschnitt der vier Subdimensionen: 2a) Festnetz-Breitband-Nutzung (25 %), 2b) Festnetz-Breitband-Abdeckung (25 %), 2c) Mobiles Breitband (40 %) und 2d) Breitband-Preise (10 %).
Integration digitaler Technologien: Die DESI Integration of Digital Technology Dimension berechnet als gewichteter Durchschnitt der drei Subdimensionen: 3a) Digitale Intensität (15 %), 3b) Digitale Technologien für Unternehmen (70 %) und 3c) E-Commerce (15 %).
Digitale öffentliche Dienste: Die DESI-Dimension „Digitale öffentliche Dienste“ berechnet aus der Punktzahl für 4a) E-Government.
Quelle: Europäische Komission

Verschieden

Komponenten des DESI-Index; Europäische Union; 2021; Index

	Humankapital	Konnektivität	Integration von digitalen Technologien	Digitale öffentliche Dienste
Dänemark	30,60	23,16	28,74	87,09
Finnland	35,55	15,48	31,53	86,72
Schweden	32,28	17,22	29,14	83,95
Niederlande	30,77	20,95	26,46	79,90
Irland	27,04	16,58	23,11	82,61
Malta	24,55	15,13	27,44	84,19
Estland	28,96	12,75	20,72	91,76
Luxemburg	28,09	17,24	21,57	79,36
Spanien	24,17	17,86	20,06	80,68
Österreich	26,67	16,34	21,02	79,83
Belgien	25,39	13,85	25,05	65,83
Deutschland	**27,62**	**17,21**	**17,89**	**67,47**
Slowenien	23,90	15,62	21,69	67,99
Litauen	23,07	11,51	21,53	78,05
EU	**23,53**	**14,66**	**19,57**	**68,05**
Frankreich	23,68	13,60	18,67	72,99
Portugal	22,78	13,67	19,58	68,95
Lettland	20,55	13,81	14,97	79,63
Tschechien	23,58	13,32	18,80	58,59
Kroatien	23,36	13,89	19,95	51,97
Italien	17,56	12,30	22,12	63,19
Zypern	19,84	13,06	16,52	61,82
Slowakei	21,88	13,28	14,83	53,72
Ungarn	20,24	15,13	11,97	49,16
Polen	18,85	12,21	13,17	55,10
Griechenland	20,52	11,96	16,56	41,94
Bulgarien	16,35	10,72	12,45	56,05
Rumänien	16,53	14,41	13,52	21,49

Quelle: Europäische Kommission

Im Verbund

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

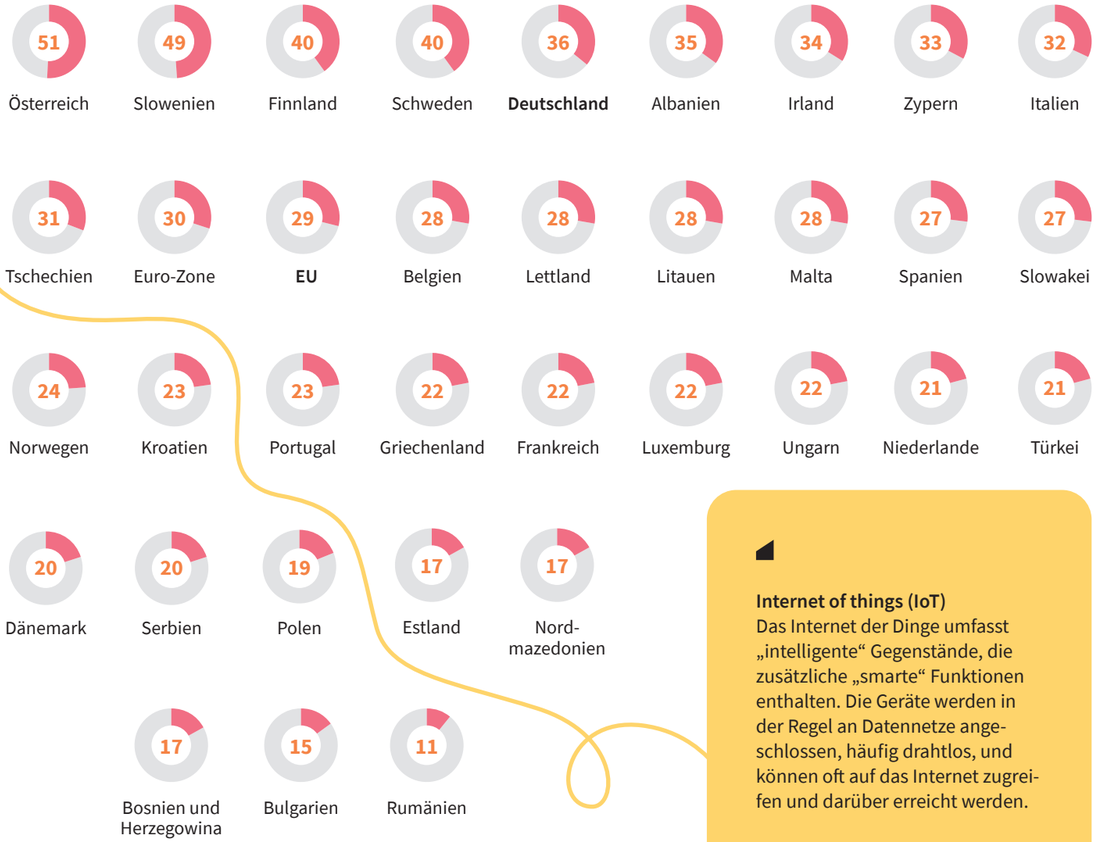
2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
7,74	8,74	10,07	11,57	13,15	14,76	16,44	18,15	19,91	21,72	23,57	25,44

Veränderung 2019 – 2030: **228,7 %**

Quelle: Transforma Insights

Im Unternehmen

Nutzung von IoT-Geräten oder -Systemen in Unternehmen *; Europa; 2021; in Prozent



Internet of things (IoT)
Das Internet der Dinge umfasst „intelligente“ Gegenstände, die zusätzliche „smarte“ Funktionen enthalten. Die Geräte werden in der Regel an Datennetze angeschlossen, häufig drahtlos, und können oft auf das Internet zugreifen und darüber erreicht werden.

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

* Alle Unternehmen, ohne den Finanzsektor (10 oder mehr Mitarbeitende und Selbstständige). Quelle: Eurostat

Im Wachsen

Prognose des weltweiten Umsatzes für öffentliche Cloud-Dienste für Endnutzerinnen und Endnutzer; weltweit; in Millionen Euro *

	2019	2020	2021	2022	prognostizierte Veränderung 2019 – 2022
Cloud Business Process Services (BPaaS)	40 368	40 388	42 416	46 894	**16,2 %**
Cloud Application Infrastructure Services (PaaS)	33 493	40 566	50 267	63 140	88,5 %
Cloud Application Services (SaaS)	91 129	90 000	103 689	128 334	40,8 %
Cloud Management and Security Services	11 461	12 540	13 553	15 895	38,7 %
Cloud System Infrastructure Services (IaaS)	39 694	51 852	69 352	94 280	137,5 %
Desktop as a Service (DaaS)	550	1 068	1 730	2 354	**328,1 %**
Gesamtmarkt	**216 694**	**236 415**	**281 009**	**350 897**	**61,9 %**

* Summe kann wegen Rundungen abweichen. Quelle: Gartner

Im Werden

Gründe für Unternehmen, cloudfähige Infrastruktur zu nutzen; IT-Entscheiderinnen und -Entscheider weltweit; 2020; in Prozent *

* Mehrfachauswahl möglich. Quellen: Vanson Bourne, Nutanix

Im Plan

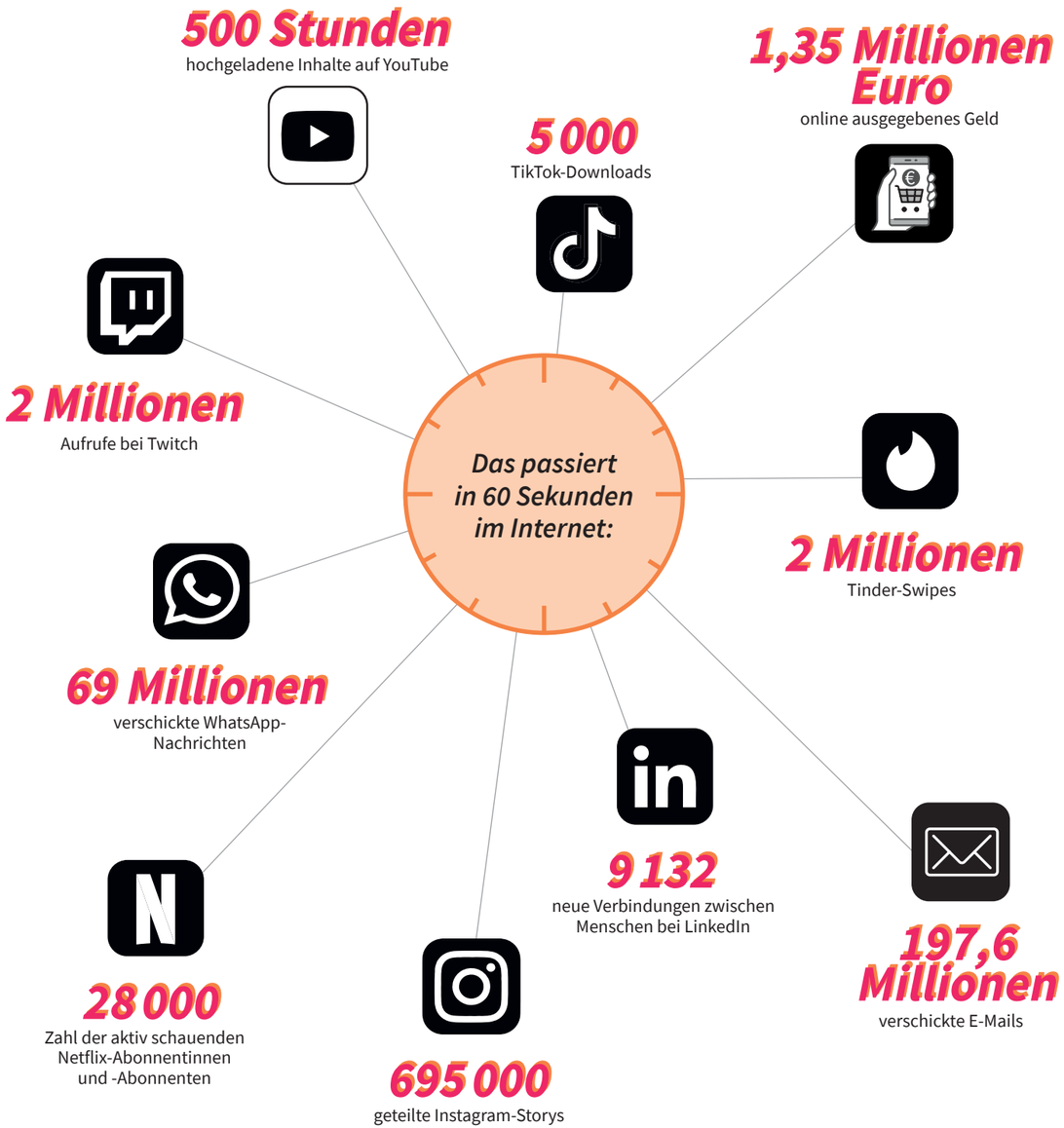
IT-Prioritäten in Unternehmen in den nächsten 12 bis 18 Monaten; IT-Entscheiderinnen und -Entscheider weltweit; 2020; in Prozent *

Sicherheitshaltung verbessern	49
5G-Technologie implementieren	46
Speichertechnologien bzw. -kapazitäten	45
Verwaltung von Multiclouds und Geschäftseffizienz verbessern	44
KI / AI-Technologien übernehmen	42
Datenbanktechnologien bzw. -kapazitäten	41
Geschäftskontinuität und Notfallwiederherstellung verbessern	41
Entwicklung und / oder Integration von cloudnativen Technologien	40

* Mehrfachauswahl möglich. Quellen: Vanson Bourne, Nutanix

Datenexplosionen

Geschätzte Menge an neu kreierten Daten im Internet pro Minute; weltweit; 2021



Quellen: World Economic Forum, Accenture

Angriffsoffensiven

Erwarteter Anstieg von Angriffen und meldepflichtigen * Vorfällen in 2022; Führungskräfte in Unternehmen weltweit; 2021; in Prozent **

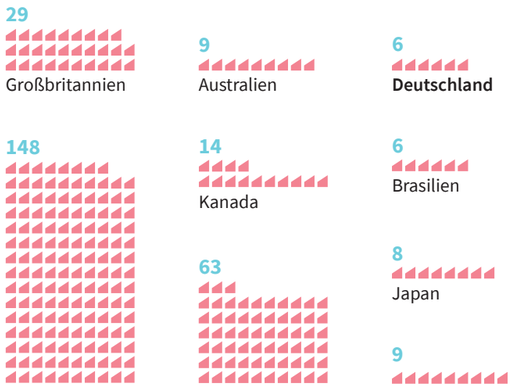
* nach DSGVO; ** Mehrfachauswahl möglich. Quelle: PricewaterhouseCoopers

Milliarden für Erpresser

Die Gefahr von Cyberattacken steigt Jahr für Jahr. Nach Schätzungen des Magazins *Cybersecurity Ventures* wurde in 2021 alle 11 Sekunden eine Ransomware-Attacke auf ein Unternehmen gestartet. Der durch Ransomware verursachte Schaden soll im Jahr 2031 weltweit mehr als 220 Milliarden US-Dollar betragen.

Weltweit

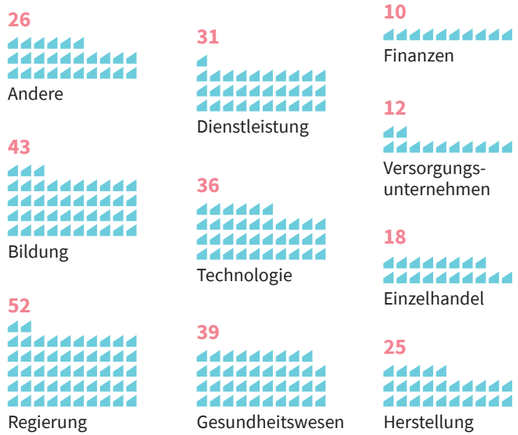
Zahl der öffentlich bekannt gewordenen Ransomware-Attacken nach Ländern; weltweit; 2021



Quelle: BlackFog

Industrieweit

Zahl der öffentlich bekannt gewordenen Ransomware-Attacken nach Industriesektor; weltweit; 2021



Quelle: BlackFog

Gestört

Anteil von Unternehmen, deren Geschäftsbetrieb von Ransomware gestört wurde; Entscheiderinnen und Entscheider aus der IT; weltweit; in Prozent

Durchschnittliche Ausfallzeit, die Unternehmen aufgrund von Ransomware-Attacken hatten (2020): **6 Tage**

Quelle: Mimecast

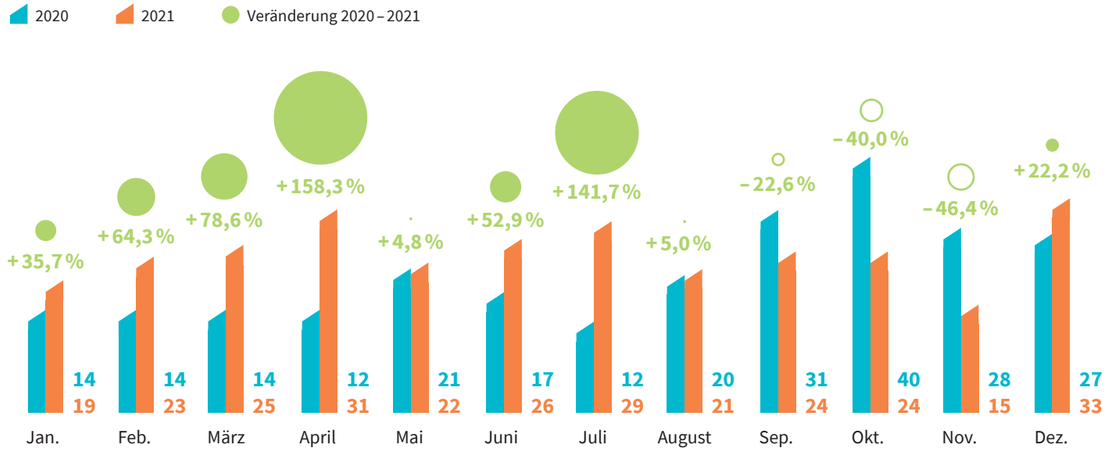
Gezahlt

Anteil an Unternehmen, die ihre Daten nach einer Ransomware-Attacke wiederherstellen konnten; Entscheiderinnen und Entscheider aus der IT; weltweit; 2020; in Prozent

Quelle: Mimecast

Gezählt

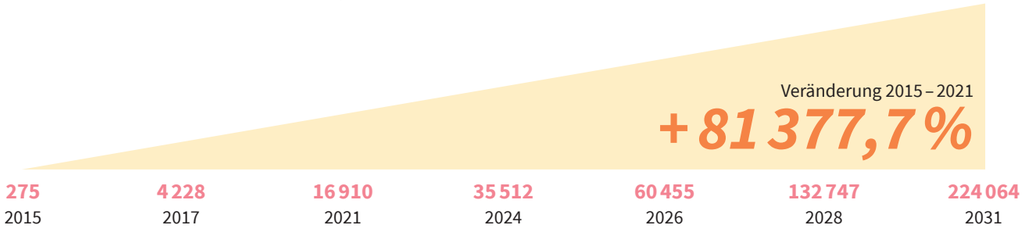
Zahl der öffentlich bekannt gewordenen Ransomware-Attacken je Monat; weltweit; 2021



Quelle: BlackFog

Geschätzt

Kosten für Schäden durch Ransomware; in Millionen Euro



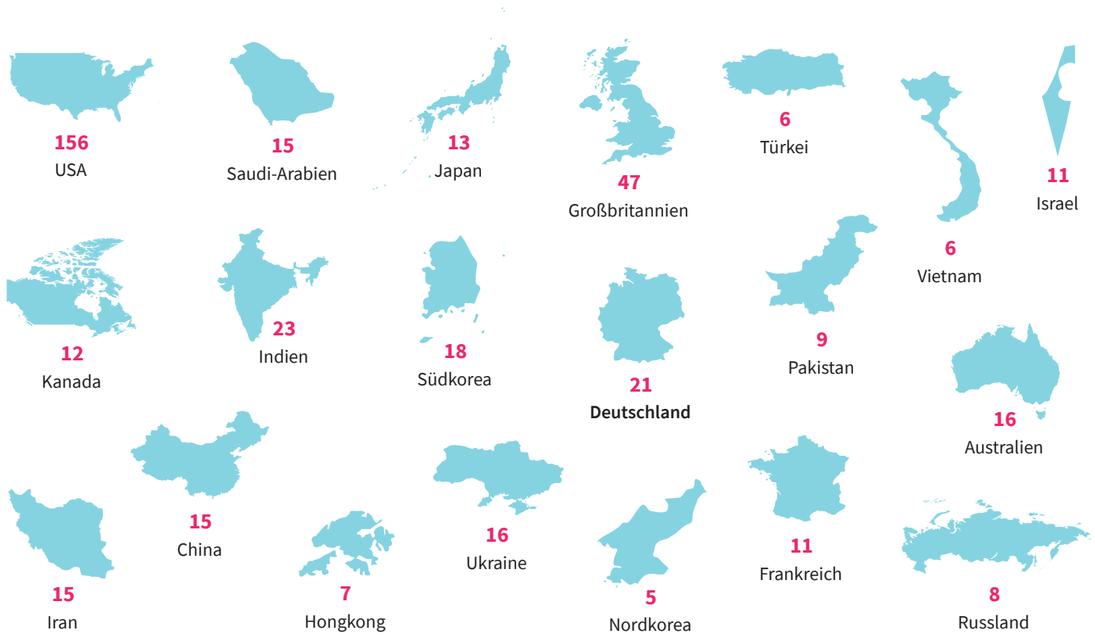
Quelle: Cybersecurity Ventures

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 einen Angriff auf das verfügbare Sicherheitsziel und eine Form digitaler Erpressung.

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Erhebliche Angriffe

Zahl der erheblichen Cyberangriffe pro Land; ausgewählte Länder; weltweit; 2006 – 2020



Quellen: Specops, CSIS

Erhebliche Kosten

Durchschnittliche Kosten von Cyberattacken in Unternehmen nach Mitarbeiterzahl; ausgewählte Länder weltweit *; 2021; in Tausend Euro

1 bis 9 Mitarbeitende	6,8
10 bis 49 Mitarbeitende	10,1
50 bis 249 Mitarbeitende	8,5
250 bis 999 Mitarbeitende	14,4
1000 Mitarbeitende oder mehr	20,3

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

Erhebliche Cyberangriffe … sind Angriffe auf Regierungsbehörden, Verteidigungs- und Hightech-Unternehmen eines Landes oder Wirtschaftsverbrechen, die einen Verlust von mehr als einer Million Dollar bedeuten.

Quellen: Specops, CSIS

Erhebliche Lecks

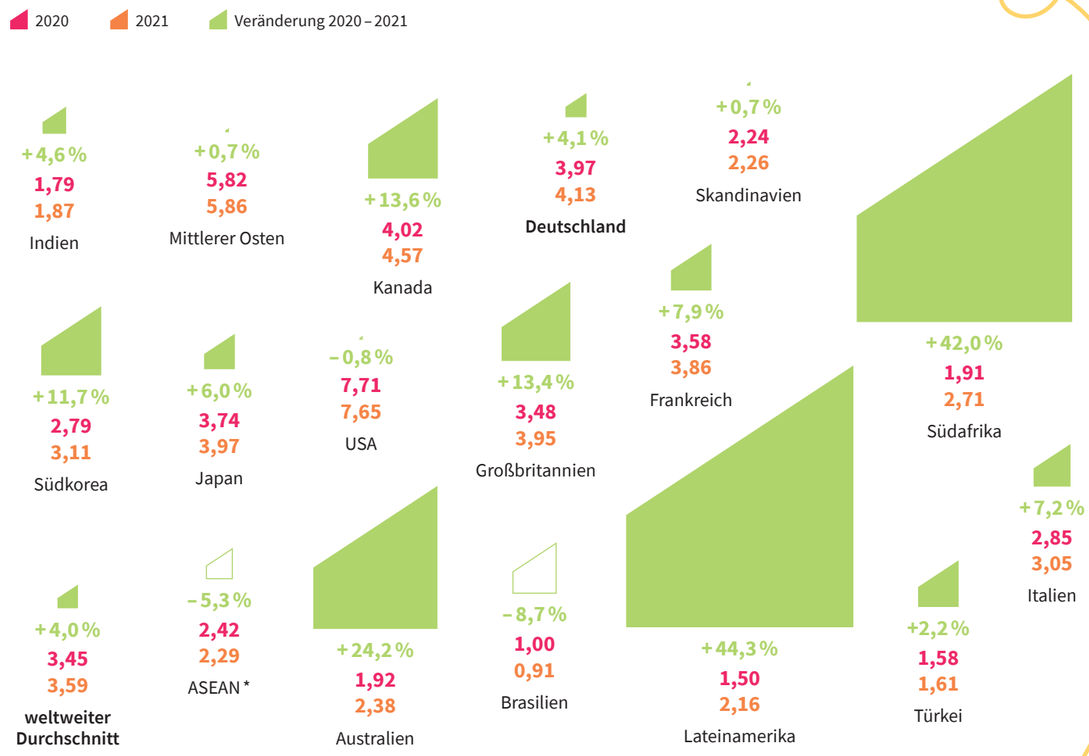
Top-10-Datenlecks weltweit; Zahl gefährdeter Accounts; 2014 – 2021 *; in Millionen

CAM4 (März 2020)	10 880
Yahoo (Oktober 2017)	3 000
Aadhaar (März 2018)	1 100
First American Financial Corp. (Mai 2019)	885
Verifications.io (Februar 2019)	763
LinkedIn (Juni 2021)	700
Facebook (April 2019)	533
Yahoo (2014)	500
Starwood (Marriott) (November 2018)	500
Adult Friend Finder (Oktober 2016)	412

* Datenabruf am 2.3.2022. Quelle: UpGuard

Was Pannen kosten

Durchschnittliche Gesamtkosten von Datenschutzpannen; ausgewählte Länder / Regionen; weltweit; in Millionen Euro



* Verband südostasiatischer Nationen (Brunei, Indonesien, Kambodscha, Laos, Malaysia, Myanmar, Philippinen, Singapur, Thailand, Vietnam).
Quellen: Ponemon Institute und IBM Security

Was Angreifer interessiert

Die Top-5-Straftaten nach Berichten an das Internet Crime Complaint Center (FBI); Zahl gemeldeter Fälle; weltweit

	2019	2020	2021
Phishing	114 702	241 342	323 972
Nichtzahlung / Nichtlieferung	61 832	108 869	82 478
Erpressung / Wucher	43 101	76 741	39 360
persönliche Datenpanne	38 218	45 330	51 829
Identitätsdiebstahl	16 053	43 330	51 629

Quellen: FBI, Internet Crime Complaint Center, US Department of Justice

Eine Datenschutzverletzung ist in der Studie „Cost of a Data Breach Report 2021“ definiert als ein Ereignis, bei dem der Name einer Person und medizinische Daten und / oder finanzielle Daten oder eine Debitkarte potenziell gefährdet sind – entweder in elektronischem oder Papierformat. Die in der Studie berücksichtigten Verstöße reichten von 2 000 bis 101 000 gefährdeten Datensätzen.

Quellen: Ponemon Institute und IBM Security

Bezahlt

Die höchsten Bußgelder für Datenschutzverstöße; weltweit; 2019 – 2022 *; in Euro

USA
24.07.19
Facebook Inc.
4 536 999 350
Verstoß gegen frühere FTC-Datenschutzanordnungen und FTC-Gesetz.

China
21.07.22
DiDi
1 165 011 903
Verstöße gegen Gesetze zur Netzwerksicherheit, Datensicherheit und zum Schutz persönlicher Informationen.

Luxemburg
30.07.21
Amazon Europe Core S.à r.l
746 000 000
Verstöße im Zusammenhang mit der Anzeige von Werbung und der Weitergabe von Daten an Dritte.

USA
22.07.19
Equifax Inc.
508 130 081
Unzureichende Schutzmaßnahmen ermöglichten Diebstahl von Bonitätsdaten von 147 Mio. Betroffenen.

Irland
02.09.21
WhatsApp Ireland Ltd.
225 000 000
Verletzung der Informationspflichten, insbesondere bzgl. Datenübermittlung an andere Facebook-Unternehmen.

USA
25.05.22
Twitter Inc.
140 765 766
Unberechtigte Verwendung der E-Mail-Adressen und Telefonnummern von Nutzern zur personalisierten Werbung.

Frankreich
06.01.22
Google LLC
90 000 000
Keine Möglichkeit, Cookies auf www.google.fr und www.youtube.com ebenso einfach abzulehnen wie sie anzunehmen.

USA
06.08.20
Capital One
67 487 768
Fehlende Sicherheitsmaßnahmen ermöglichen Hackern Zugriff auf Daten von über 106 Mio. Kreditkartenkunden.

Frankreich
06.01.22
Google Ireland Limited
60 000 000
Keine Möglichkeit, Cookies auf www.you tube.com und auf www.google.fr ebenso einfach abzulehnen wie sie anzunehmen.

Frankreich
06.01.22
Facebook Ireland Limited
60 000 000
Keine Möglichkeit, Cookies auf www.facebook.com ebenso einfach abzulehnen wie sie anzunehmen.

* Datenabruf am 3.8.2022. Quelle: DSGVO-Portal

Befürchtet

Meistgefürchtete Gründe für Betriebsunterbrechnungen von Unternehmen; Expertinnen und Experten für Risikomanagement weltweit; 2021; in Prozent *

Cybervorfälle	**52**
Naturkatastrophen	36
Ausbruch einer Pandemie	35
große Transport- bzw. Versandunterbrechungen	30

* Mehrfachnennungen möglich. Quelle: Allianz

Beunruhigt

Größte Sorgen von Unternehmen im Bereich IT-Sicherheit; Expertinnen und Experten für Risikomanagement weltweit; 2021; in Prozent *

Welche Cyberrisiken beunruhigen Ihr Unternehmen am meisten im nächsten Jahr?

	2020	2021	Veränderung 2020 – 2021
steigende Ransomware-Attacken	48	57	**18,8 %**
Datenpannen	56	57	1,8 %
Verletzlichkeit der IT-Systeme aufgrund steigender Remote Work	53	34	– 35,8 %
Unterbrechungen / Störungen der digitalen Lieferketten, Cloud	32	33	3,1 %
Technologie / Service Plattformen			

* Mehrfachnennungen möglich. Quelle: Allianz

Identifiziert

Ursachen für Sicherheitsvorfälle; ausgewählte Regionen *; Entscheiderinnen und Entscheider im Bereich IT- und Unternehmenssicherheit; 2021; in Prozent **

Wie viele der Sicherheitsvorfälle in Ihrem Unternehmen im vergangenen Jahr wurden durch die folgenden Faktoren verursacht?

_nicht böswilliger Benutzerfehler (z. B. Phishing oder nicht böswillige Verstöße gegen Sicherheitsrichtlinien)	44
_nicht aktualisierte Schwachstellen in der Software	27
_Sicherheitslücken bei Drittpersonen oder -organisationen (z. B. Managed Service-Provider oder andere Partner)	27
_Fehlkonfiguration von Diensten oder Systemen, entweder on- oder off-premise	26
_unerwartete / unterschätzte Geschäftsrisiken, die eine Schwachstelle aufgedeckt haben (Pandemie, Personalwechsel usw.)	22
_Zero-Day-Lücke	16
_gestohlene Zugangsdaten	16
_kompromittierte aktive Identitäten	16
_Verstöße gegen die Software-Lieferkette	15
_böswillige vertrauenswürdige Benutzer (ein vorsätzlicher Insider-Angriff)	13
_weiß nicht	9
_anderes	5
Anteil mit bekannter Ursache der Vorfälle	91

* Nordamerika 57 %, APAC (Wirtschaftsraum Asien Pazifik) 35 %, EMEA (Wirtschaftsraum Europa, Naher Osten und Afrika) 17 %. ** Mehrfachauswahl möglich. Quelle: Foundry

Dokumentiert

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

1999	1 579
2000	1 243
2001	1 573
2002	2 436
2003	1 603
2004	2 779
2005	4 900
2006	7 254
2007	6 764
2008	7 322
2009	5 160
2010	5 341
2011	5 336
2012	6 723
2013	7 495
2014	10 453
2015	9 574
2016	11 323
2017	19 401
2018	21 862
2019	21 463
2020	31 089
2021	30 346
2022 *	8 623
Veränderung 1999 – 2021	**1 822 %**

* Stand 2022: 23.3.2022. Quelle: CVE

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. Erfasst wurden Candidate, Entry und Status, um einen umfassenden Überblick zu vermitteln.

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

Halbherzige Pläne

Pandemiebedingte Anpassungen der Strategie zur Cybersicherheit; weltweit; 2020; in Prozent *

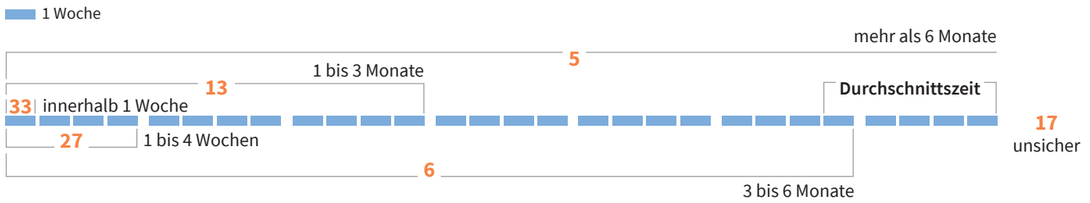
Welche der folgenden Veränderungen werden sich am ehesten durch die Erfahrung mit COVID-19 auf die Cybersicherheit in Ihrer Branche auswirken?

Cybersicherheit und Datenschutz sind in jede Geschäftsentscheidung oder jeden Plan integriert.	50
neuer Prozess der Budgetsetzung für Cyberausgaben oder -investitionen	44
bessere und genauere Quantifizierung des Cyberrisikos	44
häufigere Interaktionen zwischen CISO und CEO oder Vorständen	43
größere Belastbarkeitstests für Ereignisse mit geringer Wahrscheinlichkeit und starken Auswirkungen	43
keine Änderung aufgrund von COVID-19	4
unbekannt / unsicher	1

* Mehrfachauswahl möglich. Quelle: PricewaterhouseCoopers

Lange Leitungen

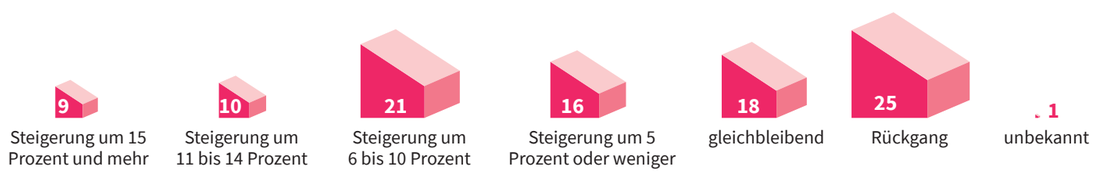
Zeit, die vergeht, bis Sicherheitsvorfälle entdeckt werden; ausgewählte Regionen *; Entscheiderinnen und Entscheider im Bereich IT- und Unternehmenssicherheit; 2021; in Prozent



* Nordamerika 57 %, APAC (Wirtschaftsraum Asien Pazifik) 35 %, EMEA (Wirtschaftsraum Europa, Naher Osten und Afrika) 17 %. Quelle: Foundry

Moderate Steigerungen

Entwicklung des Cyberbudgets für 2022; Führungskräfte aus den Bereichen Wirtschaft, Technologie und Sicherheit; weltweit; 2021; in Prozent



Quelle: PricewaterhouseCoopers

Höhere Sicherheiten

Globale jährliche Ausgaben für Cybersicherheit und Cyberversicherung; weltweit; in Milliarden Euro

	2015	2016	2017	2018	2019	2020	Veränderung 2015 – 2020
Ausgaben für Cybersicherheit	68,1	74,1	78,8	113,6	107,1	108,8	**+46,9 %**
Ausgaben für Cyberversicherungen (GWP)	2,3	2,9	3,5	5,3	4,5	7,0	**+211,7 %**

Quellen: Marsh, Microsoft, Gartner, Munich Re

Ausgegeben

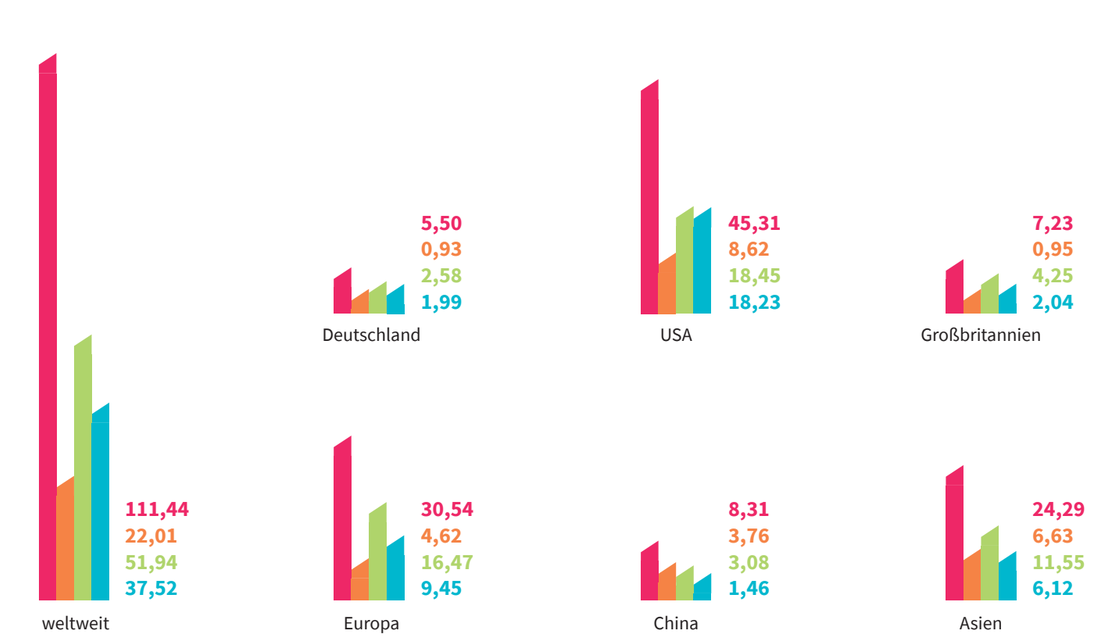
Ausgaben für IT-Sicherheit je Cybersicherheitssegment; weltweit; in Millionen Euro

	2019	2020	2021	Veränderung 2019 – 2021
Sicherheitsdienstleistungen	55 338,4	56 969,0	61 297,9	10,8 %
Schutz der Infrastruktur	14 750,0	17 914,6	20 210,5	37,0 %
Ausstattung zur Netzwerksicherheit	11 952,7	13 680,6	14 390,8	20,4 %
Identitäts- und Zugangsmanagement	8 783,0	10 537,6	11 767,1	34,0 %
Sicherheitssoftware für Konsumentinnen und Konsumenten	5 583,9	5 696,9	5 910,2	5,8 %
integriertes Risikomanagement	4 067,0	4 254,1	4 627,5	13,8 %
Anwendungssicherheit	2 763,4	2 918,1	3 160,6	14,4 %
Datensicherheit	2 376,8	2 609,9	2 963,6	24,7 %
andere Software zur Informationssicherheit	1 969,6	2 018,9	2 136,6	8,5 %
Cloud Security	392,0	520,9	711,1	81,4 %
gesamt	**107 976,8**	**117 121,3**	**127 174,3**	**17,8 %**

Quelle: Gartner

Eingenommen

Umsatz des Cybersicherheitsmarktes; ausgewählte Länder und Regionen; weltweit; 2021; in Milliarden Euro



Quelle: Cybersecurity Outlook Statista

Die Welt zu einem besseren Ort machen

Wie lässt sich Cybersecurity lehren? Was ist wichtig? Und wer eignet sich dafür? Dena Haritos Tsamitis leitet seit 20 Jahren das Information Networking Institute (INI) der Carnegie-Mellon, einer US-Elite-Universität für Computer Science und Cybersecurity. Sie unterscheidet ihre Studentinnen und Studenten in Skill Seeker und Non-Conformists.

Text: Christoph Koch

Angehende Unternehmer? Politiker? Entwickler? Sie sorgen jedenfalls für mehr Sicherheit.

Foto: picture alliance / Zoonar | lev dolgachov

Frau Tsamitis, Ihr Institut gilt als eines der weltweit führenden im Bereich Cybersicherheit. Wie hat sich das Angebot im Laufe der Zeit entwickelt?
Dena Haritos Tsamitis: Das Information Networking Institute (INI) wurde 1989 gegründet. Den Masterstudiengang Information Security bieten wir seit 2003 an, im selben Jahr startete das CyLab.

Ursprünglich sollte das CyLab unser Forschungsarm sein und das INI sich um die Ausbildung kümmern. Mittlerweile überschneidet sich das ein wenig. Am CyLab arbeiten heute auch Wissenschaftler aus anderen Fachbereichen, mit denen es Berührungspunkte im Bereich Cybersicherheit gibt, etwa aus dem Ingenieurwesen oder der Softwareentwicklung. Auch die Sozialwissenschaften gehören dazu, schließlich basieren viele Angriffe heute darauf, dass man das Vertrauen eines Menschen erwirbt, damit er Informationen liefert, statt ein digitales Passwort zu knacken.

Wie erstellt man überhaupt ein Curriculum für ein Feld, das sich so schnell und konstant wandelt wie Cybersicherheit?
Das ist in der Tat nicht einfach, denn es werden unentwegt neue Sicherheitslücken entdeckt. Jeden Tag entwickeln irgendwo Menschen ein neues Computervirus oder versuchen sich illegal Zugang zu geschützten Daten zu verschaffen.

Unsere Gegner scheinen uns immer einen Schritt voraus zu sein, aber wir haben Strategien und Technologien entwickelt, um uns gegen diese Bedrohungen zu schützen. Es steht ja auch deutlich mehr auf dem Spiel. Die ersten Viren oder Würmer haben nur ein paar Rechner an einer Uni lahmgelegt. Heute ist Cyberkriminalität bekanntermaßen eine globale Bedrohung, die auch enorme wirtschaftliche Implikationen hat.

Bei sogenannten Deepfakes, also künstlich erzeugten Videoaufnahmen, sind außerdem psychologische und sozialwissenschaftliche Aspekte relevant. Deshalb ist es wichtig, dass wir uns nicht nur mit Code beschäftigen, sondern auch mit möglichst vielen anderen Bereichen der Universität vernetzen.

Wenn sich das Spielfeld jeden Tag verändert: Wie stellen Sie sicher, dass Sie nicht den Anschluss verlieren?
Wir geben unseren Studierenden ein technisches Fundament mit, zum Beispiel über Computertechnik, Informatik und Netzwerksysteme. Im Laufe ihres Studiums spezialisieren sie sich dann immer weiter und tauchen tiefer in einzelne Felder ein.

Was uns von anderen Programmen unterscheidet, ist die Tatsache, dass unsere Studierenden irgendwann gemeinsam mit einem Forscher ihrer Wahl eigenständig an einem komplett eigenen Projekt arbeiten. Das kann ein Coding-Problem sein, das bisher niemand gelöst hat, oder das Reverse Engineering einer bestehenden Angriffs-Software, um besser zu verstehen, wie sie funktioniert.

Unsere Studierenden spezialisieren sich in verschiedenen Bereichen und schlagen anschließend sehr unterschiedliche Laufbahnen ein. Manche landen bei großen Tech-Konzernen, andere arbeiten für die Regierung, wieder andere gründen Start-ups, die oft aus Projekten entspringen, die sie hier bei uns begonnen haben.

Was uns ebenfalls wichtig ist: dass wir ethische Fragen und Themen wie Mitarbeiterführung behandeln. Das sind keine Soft Skills, sondern sehr essenzielle Fähigkeiten. Akademische Integrität, Konfliktlösung und Verhandlungsstrategien sind wichtige Dinge, die Menschen über ihre gesamte berufliche Laufbahn brauchen werden – und oft auch in ihrem Privatleben.

Nach wem suchen Sie für Ihr Programm? Welche Eigenschaften sind wichtig, um im Bereich Cybersecurity erfolgreich zu sein?
Grundsätzlich suchen wir nach Menschen, die zumindest einen kleinen technischen Hintergrund besitzen. Früher sollten es konkrete Vorkenntnisse in Informatik oder Computertechnik sein, heute fassen wir das ein wenig 〉

„Heute steht deutlich mehr auf dem Spiel."

Dena Haritos Tsamitis kam im Jahr 2000 an die Carnegie-Mellon Universität und war ab 2002 stellvertretende Direktorin des Information Networking Institute (INI), bevor sie 2004 die Position der Direktorin übernahm. Die Tochter von griechischen Einwanderern engagiert sich für mehr Diversität im Bereich Informatik und gründete 2005 mit anderen die Organisation Women@INI (WINI). Sie ist außerdem Gründungsdirektorin des Carnegie Mellon CyLab, das sich der Erziehung, Bildung und Aufklärung im Bereich Cybersicherheit widmet.

weiter. Zahlenverständnis und etwas Erfahrung mit Programmierung schaden sicher ebenfalls nicht.

Aber wir haben auch gelernt, dass es sehr große Unterschiede zwischen den Geschlechtern und Kulturen gibt, wenn es darum geht, wie jemand seine Fähigkeiten einschätzt. Wenn man in einer Stellenausschreibung sehr spezifische Voraussetzungen benennt, werden sich Frauen beispielsweise nur bewerben, wenn sie alle Anforderungen erfüllen. Männer hingegen heben unserer Erfahrung nach schon die Hand, wenn sie etwa 60 Prozent der Vorgaben genügen. Also haben wir unsere Anforderungen etwas weniger spezifisch formuliert – und bekamen prompt eine diversere Bandbreite an Bewerbungen. Heute bringen die Menschen an unserer Uni sehr unterschiedliche Lebenserfahrungen mit, von denen wir profitieren.

Seit Sie das INI leiten, ist der Frauenanteil unter den Studierenden drastisch gestiegen. Wo liegt er inzwischen?
Als ich 2002 als stellvertretende Direktorin anfing, waren 2 Frauen unter den 34 Studierenden, die neu bei uns anfingen. Das sind lediglich 6 Prozent! Inzwischen sind wir bei 45 Prozent Studentinnen angekommen, und unsere Lehrkräfte sind zu 50 Prozent weiblich. So etwas geht natürlich nicht über Nacht. Und es geht nur, wenn man wirklich darauf achtet und sich zum Ziel setzt, mehr Frauen für das Thema Cybersicherheit zu interessieren und zu begeistern. In der gesamten Branche liegt der Frauenanteil immer noch bei 24 Prozent – wir haben also einen weiten Weg vor uns.

Wie haben Sie es geschafft, den Anteil von 6 Prozent auf 45 zu erhöhen?
Es gibt das Vorurteil, dass die Standards gesenkt oder Lehrpläne angepasst werden müssen, um Frauen für technische Studiengänge zu gewinnen. Aber das stimmt nicht. Wir haben stattdessen unsere akademische Kultur geändert und die Aktivitäten, die wir im Hörsaal und außerhalb betreiben.

Am INI studieren heute 45 Prozent Frauen, die Lehrkräfte sind zur Hälfte weiblich.

Foto: Adobe Stock

Es geht aber längst nicht nur um Geschlechterfragen: In unserem Leitbild steht, dass alle Menschen bei uns willkommen sind – unabhängig von ethnischer Herkunft, Religion, Geschlecht, Alter, Behinderung, sexueller Orientierung und Selbstidentität. Es reicht aber nicht, das nur zu behaupten. Man muss es auch leben.

Wie zum Beispiel?
Wichtig ist beispielsweise die Interaktion im Seminarraum: Inklusive Pädagogik bedeutet, sich zu fragen, wie man die Studierenden ermutigt, sich zu beteiligen.

Vor 20 Jahren, als dort fast ausschließlich weiße männliche US-Amerikaner saßen, hat es genügt, zu warten, bis jemand sich meldet. Aber was ist, wenn manche Studierenden sich nicht damit wohlfühlen, sich zu Wort zu melden? Wie kann ich die einbeziehen? Wie dafür sorgen, dass sie sich wertgeschätzt und willkommen fühlen?

Ich nehme solche Dinge sehr ernst. In meinen Augen muss eine Ausbildung immer mehr sein als die Summe der Kurse, die man belegt.

Haben die Bewerberinnen und Bewerber eine klare Vorstellung, wohin sie nach ihrem Studium wollen?
Es gibt zwei große Gruppen. Die einen nenne ich die Skill Seeker: Sie haben bereits einen Pfad im Kopf und wollen etwas ganz Konkretes bei uns lernen, um dann beispielsweise für Google zu arbeiten. Diese Kandidatinnen und Kandidaten sind oft sehr erfolgreich, aber wir versuchen dennoch, ihnen auch zu zeigen, was links und rechts ihres Pfads liegt, und ihre Perspektive zu erweitern.

Die zweite Gruppe würde ich als Non-Conformists oder Change Makers bezeichnen: Das sind Studierende, die häufig keinen klassischen Bildungsweg hinter sich haben und kein klares Berufsziel, dafür aber ein sehr breites Interessenspektrum. Sie besitzen oft vielfältigere Perspektiven und Lebenserfahrungen und können sich vorstellen, ihre neu erworbenen Talente und Fähigkeiten zu nutzen, um etwas zu verändern. Sie müssen oft noch ein paar Grundlagenkurse zum Beispiel im Bereich Informatik belegen, können dann aber sehr erfolgreich sein.

„Wir lassen nichts unversucht, um Leute zu erreichen, die zu uns passen könnten."

Wie finden Sie talentierte Bewerberinnen und Bewerber für Ihre Studienplätze?
Wir gehen auf Konferenzen, nicht nur auf große Fachmessen, sondern auch auf Hacker-Events wie die Def Con. Wir gehen auch gezielt zu Veranstaltungen wie der Grace Hopper Celebration oder der Tapia Conference, die sich für mehr Diversität in der IT-Branche einsetzen. Wir haben Partnerschaften mit Unternehmen, die ihr Wissen über Cybersicherheit ausbauen wollen. Und wir veranstalten Hackathons.

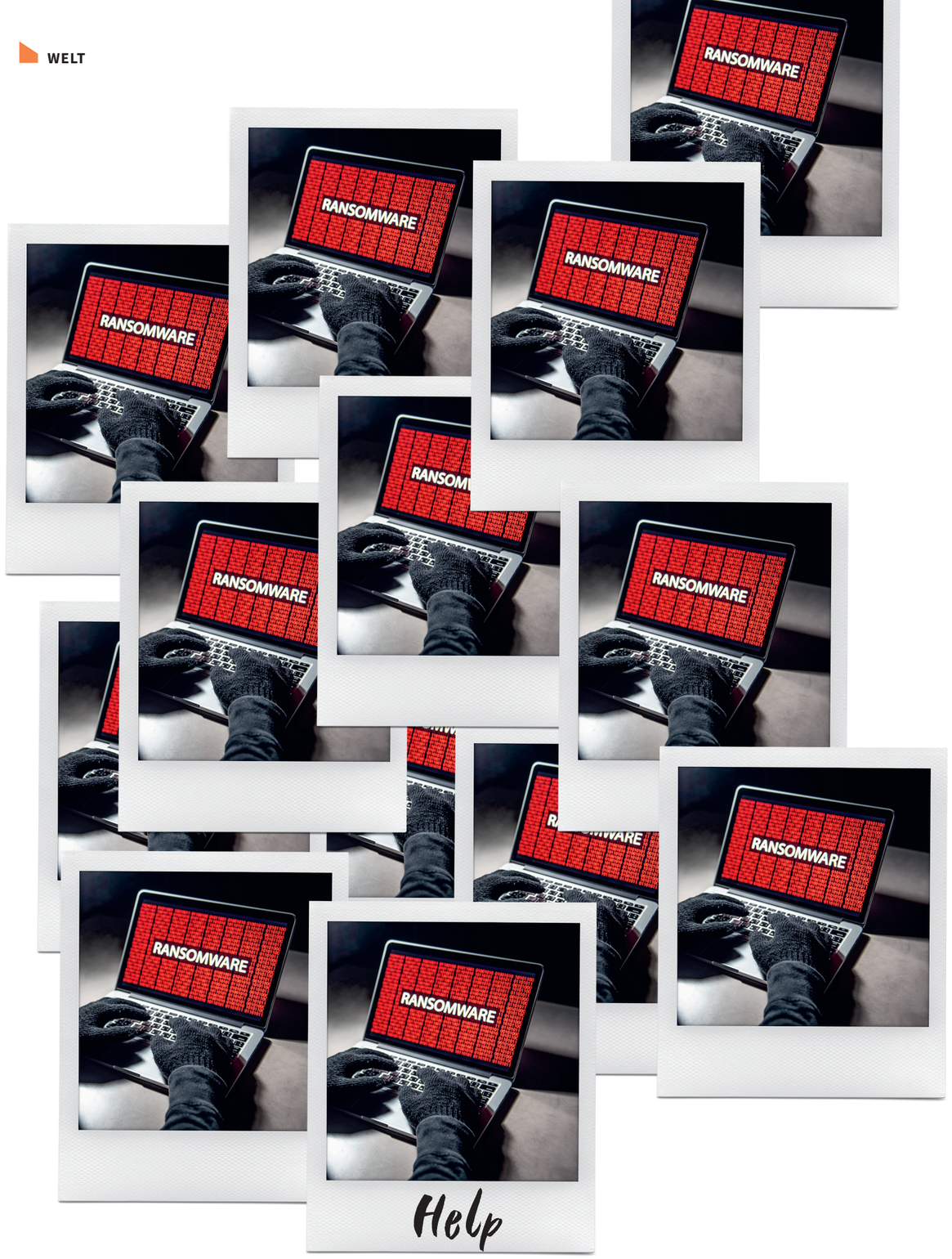
Nächste Woche besuche ich eine örtliche High School und erzähle den Schülern dort, was wir machen. Wir haben mit PicoCTF auch ein Online-Spiel entwickelt, das den Bereich Cybersicherheit für Kinder und Jugendliche zugänglich machen soll. An den Wettbewerben, die im Spiel stattfinden, haben schon Zehntausende von Schülerinnen und Schülern teilgenommen. Kurzum: Wir lassen nichts unversucht, um Leute zu erreichen, die zu uns passen könnten und haben uns so mit der Zeit eine Art Pipeline gebaut.

Was würden Sie einem jungen Menschen raten, der sich für den Bereich Cybersicherheit interessiert?
Mittlerweile ist es eine Floskel, zu sagen, dass man die Welt zu einem besseren Ort machen möchte, aber wer in der IT- und Cybersicherheit arbeitet, kann das wirklich: Unser Stromnetz, die Infrastruktur, unsere Versorgung mit Nahrungsmitteln – so viel hängt mittlerweile davon ab, dass unsere Computersysteme laufen, ohne gehackt oder lahmgelegt zu werden. Das ist also eine Laufbahn, bei der einiges auf dem Spiel stehen kann.

Das sollte allerdings niemanden abschrecken. Und man darf auch keine Angst davor haben, dass die Konkurrenz sehr stark ist. Wenn man in der Schule die oder der Klassenbeste war und dann im Studium neben lauter Leuten sitzt, die das auch waren, kann das sehr belastend sein. Viele Studierende beginnen zu zweifeln und fragen sich: Bin ich gar nicht so gut? Bin ich nur durch einen Fehler aufgenommen worden?

Sie sprechen vom sogenannten Impostor-Syndrom, richtig?
Ja, das ist ein Thema, das mir sehr wichtig ist, denn ich habe selbst darunter gelitten. Ich frage mich bis heute manchmal, wenn ich in ein wichtiges Meeting gehe, was ich dort verloren habe. Wollen die anderen mich wirklich dabeihaben? Ich kenne so viele Menschen, die im Laufe ihrer Karriere unter dem Impostor-Syndrom litten – und ich versuche, so vielen wie möglich ihre Ängste und Zweifel zu nehmen und ihnen Strategien zur Überwindung ihrer Unsicherheit zu vermitteln.

Einer unserer Studierenden, ein indischer Student namens Harshvardhan, hat sich bei uns beworben, nachdem er einen Online-Vortrag von mir zu diesem Thema gehört hatte. Er litt auch unter dem Syndrom, ohne zu wissen, wie verbreitet das Phänomen ist. Er bekam einen Studienplatz am INI und ist heute der Cybersicherheitsberater der indischen Regierung.



Die Ersthelferin

Wenn ein Unternehmen Opfer eines Cyberangriffs wird, klingelt ihr Telefon: Kira Groß-Bölting ist die erste Ansprechpartnerin für gehackte Firmen. Ihre wichtigste Qualifikation? Zuhören können.

Text: Christoph Koch

• Statt einer Taschenlampe benutzen sie eine Computertastatur. Statt durch ein aufgebrochenes Fenster zu klettern, nutzen sie einen offenen Port oder andere digitale Schwachstellen. Aber genau wie reguläre Einbrecher schlagen auch Cyberkriminelle bevorzugt in der Nacht zu. „Die Beschäftigten kommen morgens ins Büro und stellen fest, dass nichts mehr geht“, beschreibt Kira Groß-Bölting den Moment, wenn der Einbruch in die IT-Infrastruktur bemerkt wird. „Am häufigsten sehen wir mittlerweile Ransomware-Angriffe, bei denen das komplette System inklusive Back-ups verschlüsselt wurde und nur gegen eine Lösegeldzahlung wieder freigegeben wird.“

Kira Groß-Bölting, Undercut und den Rest der roten Haare zu einem Pferdeschwanz zusammengebunden, ist die Frau, bei der dann das Telefon klingelt. Sie ist Incident-Response-Koordinatorin bei G DATA Advanced Analytics. Sozusagen eine Mischung aus Feuerwehrleitstelle, Seelsorge, Ersthelferin und Überdruckventil. Wie beschreibt sie ihren Beruf ihrer Familie gegenüber oder auf einer Party? „Ich sage dann so etwas wie: Ich habe die Verantwortung, Firmen in digitalen Notfallsituationen erstzubetreuen und im Team die direkte Planung für das weitere Vorgehen zu übernehmen.“

Groß-Bölting versucht, so schnell wie möglich ein Bild der Lage zu bekommen: Was genau ist passiert? Läuft der Angriff vielleicht noch? Welche Systeme sind betroffen, welche noch funktionsfähig? Wurden bereits Maßnahmen ergriffen – und wenn ja, haben sie vielleicht alles noch schlimmer gemacht?

„Egal wie gut eine Firma auf einen Cyberangriff vorbereitet ist“, sagt Groß-Bölting: „Wenn der Ernstfall eintritt, herrscht fast immer erst mal Chaos und Überforderung. Meine Aufgabe ist es dann, die Übersicht zu behalten.“

Einer späht aus, einer räumt ab

Die Zahl der Cyberangriffe nimmt seit Jahren deutlich zu. Allein in Deutschland wurden im vergangenen Jahr 146 363 Delikte gemeldet, 12 Prozent mehr als im Vorjahr, so das Bundeskriminalamt. Je nach Art der Befragung klagen zwischen 46 und 88 Prozent der deutschen Unternehmen über Cyberattacken. Der Branchenverband Bitkom geht für das Jahr 2021 von 〉

einem Gesamtschaden in Höhe von 223 Milliarden Euro in der deutschen Wirtschaft aus.

Vor allem Ransomware-Angriffe sind beliebt, also quasi die Geiselnahme eines fremden Rechners oder einer IT-Infrastruktur durch Verschlüsselung. Für solche Angriffe ist kein großes Informatik- oder Hacker-Latinum notwendig, sondern nur ein wenig kriminelle Energie: Ransomware-Bausätze finden sich online, inklusive Anleitung.

Häufig erfolgt auch eine Art Arbeitsteilung: Der eine späht aus, der andere räumt ab. „Eine Person oder Gruppe scannt im Internet erreichbare Systeme nach bekannten Schwachstellen“, sagt Groß-Bölting. „Davon gibt es Hunderte. Im Idealfall werden die Schwachstellen durch Updates zügig geschlossen.“ Doch nicht alle Firmen sind immer komplett auf dem aktuellen Stand, was ihre Software betrifft. „Wenn Angreifer eine solche Sicherheitslücke gefunden haben, legen sie so etwas wie einen Türöffner auf dem System der Firma ab, der weiterhin Zugriff sicherstellt. Diesen Zugang verkaufen sie an die eigentlichen Ransomware-Angreifer, die dann manuell den Verschlüsselungsangriff starten.“

Nicht zahlen, sondern anzeigen

Ist es einmal so weit gekommen und der Angriff erfolgreich, wird es ungleich schwerer, den Betroffenen zu helfen. „Bei der klassischen Ransomware-Verschlüsselung muss man den Leuten leider die Illusion nehmen, dass man die Daten wiederherstellen kann“, sagt Groß-Bölting.

Trotzdem rät sie allen betroffenen Firmen davon ab, mit den Erpressern in Verhandlung zu gehen. „Zuallererst sollte man zur Polizei gehen und Anzeige erstatten“, sagt sie. Jedes Bundesland verfügt über eine eigene Anlaufstelle speziell für Cybercrime, die mit dem Thema vertraut ist. Eine Strafanzeige ist wichtig, damit die Behörden Ermittlungen einleiten können. „Wenn alle Angegriffenen brav das geforderte Lösegeld bezahlen, bleibt Ransomware ein lukratives Geschäft und wird als Problem eher noch wachsen.“

„Ich gebe allen möglichst schnell kleinere Aufgaben zu erledigen, damit sie wieder ins Handeln kommen und aus diesem Gefühl der Ohnmacht herausfinden.“

Kira Groß-Bölting – intern nur liebe- und respektvoll KGB genannt – ist keine studierte Informatikerin. Die gelernte Bürokauffrau stieg 2016 als Teamassistenz bei G DATA Advanced Analytics ein. Damals war die Ausgründung der G DATA Gruppe gerade ein halbes Jahr alt. „Ich habe also viele Prozesse und Strukturen von Anfang an mit begleitet und mit aufgebaut“, sagt sie. „IT hat mir schon immer Spaß gemacht und mich interessiert. Aber ich habe keine formale Ausbildung in diesem Bereich.“

Als die ersten Notfallanrufe bei GDATA eingingen, landeten sie zunächst bei ihr, der Teamassistenz. „Mein persönlicher Ehrgeiz hat dann dafür gesorgt, dass ich das möglichst gut machen und das Team möglichst gut vorbereiten wollte für den Einsatz.“

KGB bildete sich fachlich fort, gleichzeitig wuchs G DATA und das Problem mit Schadsoftware-Attacken wurde von Jahr zu Jahr größer. Groß-Bölting arbeitet neben ihrer Tätigkeit als Incident-Response-Koordinatorin auch noch im Service-Management – doch die Tage, an denen das Notfall-Telefon nicht klingelt, sind mittlerweile selten.

Wichtiger als die Zahl der Programmiersprachen, die man beherrscht, sind in ihrem Job Eigenschaften wie Empathie und Kommunikationsgeschick. „Die Leute, die anrufen, sind in den allermeisten Fällen deutlich überfordert“, sagt KGB. „Alle Prozesse, die sie vorher für einen solchen Notfall ausgetüftelt haben, stehen auf dem Prüfstand.“ Je nach Typ reagieren die Anruferinnen oder Anrufer dabei sehr unterschiedlich. Manche sind wütend, andere ängstlich. Das Gefühl, das jedoch alle eint, ist Hilf-losigkeit. „Ehrlichkeit ist dann für mich das beste Mittel. Damit kann ich auch die Lauten und Ärgerlichen einfangen. Außerdem gebe ich allen möglichst schnell kleinere Aufgaben zu erledigen, damit sie wieder ins Handeln kommen und aus diesem Gefühl der Ohnmacht herausfinden.“

Viele Unternehmen, die Opfer eines Hackerangriffs geworden sind, stellen schnell die Schuldfrage. Wie konnte es dazu kommen? Wer hat geschlampt, war leichtsinnig, vielleicht sogar verantwortungslos? Groß-Bölting warnt davor, unter den Mitarbeitenden nach einer Person zu suchen, der man die Schuld zuschieben kann. Letztlich helfe es niemandem weiter, Zeit und Ressourcen auf die Ermittlung zu verwenden, wer denn nun zum Beispiel auf einen Phishing-Link in einer E-Mail geklickt hat. „Solche Dinge passieren. Es ist wichtiger, sich darauf zu konzentrieren, den Schaden schnell und bestmöglich zu beheben, anstatt jemanden aus der Belegschaft an den Pranger zu stellen“, sagt Groß-Bölting. „Noch dazu, weil dadurch schlimmstenfalls ein Klima der Angst entsteht, in dem niemand mehr den kleinsten Fehler zugibt. Dabei kann genau das wichtig sein, um einen Angriff frühzeitig zu erkennen und Schlimmeres zu verhindern.“

Tatsächlich werden auch die Tricks der Angreifer immer raffinierter: Anfragen, die den echten Namen eines tatsächlichen Teammitglieds enthalten. Webseiten, die genauso aussehen wie das interne System. Von den guten alten Spam-Mails, in denen ein nigerianischer Prinz ein Milliardenerbe in Aussicht stellt, sind diese modernen Phishing- und Social-Engineering-Taktiken so weit entfernt wie ein raffinierter Trickbetrüger von einem Einbrecher, der am helllichten Tag versucht die Tür einzutreten. „Letztlich kann es allen passieren, dass sie oder er in der Eile des Tagesgeschäftes mal auf einen falschen Link klickt“, sagt Kira Groß-Bölting.

Bloß nicht ausschalten!

Trotzdem sind Unternehmen nicht völlig machtlos, und es ist durchaus sinnvoll, sich vorzubereiten und mit dem Thema Cyberangriff auseinanderzusetzen. „Viele Firmen denken, sie seien zu klein und unwichtig, um für Cyberkriminelle interessant zu sein“, sagt Groß-Bölting. „Doch das stimmt nicht. Jede Firma hat Daten, die ihr wichtig sind, und wenn es eine Sicherheitslücke gibt, findet sich irgendwann jemand, der sie ausnutzt. Und sei es nur, um ein paar Dollar zu erpressen.“

Ein Notfallplan ist also unerlässlich. Dabei ist es vor allem wichtig, eine Informationskette und Ansprechpersonen festzulegen. Wem sollen Mitarbeitende Bescheid sagen, wenn sie den Verdacht haben, dass etwas falsch läuft? „Dabei muss auch feststehen, wer im Notfall etwas entscheiden darf“, sagt Groß-Bölting. „Das müssen manchmal sehr schnelle und radikale Entscheidungen sein, die am besten eine Person trifft, die sich technisch genug auskennt, um nicht alles noch schlimmer zu machen.“

Denn Letzteres kann schnell passieren. Einer der größten Fehler, den betroffene Unternehmen leider häufig machen, ist, alle Systeme auszuschalten. Dabei gehen oft wichtige forensische Spuren verloren: „Moderne Schadsoftware legt sich oftmals im Arbeitsspeicher ab“, sagt Groß-Bölting. „Dadurch verschwindet sie beim Ausschalten des Systems, und wir wissen nicht mehr, womit wir es zu tun haben.“

Das Problem selbst – also zum Beispiel die Verschlüsselung aller Daten – bleibt natürlich auch nach dem Ausschalten erhalten. Die Devise „Einfach mal ausschalten und wieder einschalten“, die sich sonst bei so manchem Tech-Schluckauf bewährt, ist in diesem Fall also nicht nur nutzlos, sondern erschwert auch die Detektivarbeit von Kira Groß-Böltings Kolleginnen und Kollegen.

Was deren Arbeit wiederum erleichtert: wenn Unternehmen den Zeitraum erhöhen, für den die Logdaten ihrer Server gespeichert werden. „Je mehr Daten da sind und je besser wir nachvollziehen können, was auf den Systemen passiert ist, desto besser können wir helfen“, sagt Groß-Bölting. Die Grundeinstellung zum Beispiel bei den gängigen Windows-Servern sei da ein eher kurzer Zeitraum, und nicht für alle Features sei Logging überhaupt standardmäßig aktiviert – „aber das kann und sollte man umstellen.“

Sicherheit ist ein Vollzeitjob

Grundsätzlich empfiehlt sie Unternehmen, das Thema IT-Sicherheit ernster zu nehmen. Das bedeutet unter anderem, in hauptberufliches IT-Personal zu investieren. „Wenn ein Unternehmen mehr als hundert Mitarbeiter und Mitarbeiterinnen hat, kann es nicht sein, dass irgendjemand halbtags neben dem eigentlichen Job noch IT-Administration macht“, sagt Groß-Bölting.

Weitere essenzielle Tipps: Unbedingt für Back-ups sorgen, die offline, also nicht permanent mit dem Netzwerk verbunden sind, aber regelmäßig geprüft werden. Und an die Zeit nach einem Angriff denken und einen Plan für die Priorisierung beim Wiederaufbau erstellen. Welche Teile des Systems müssen zuerst wieder laufen? „Natürlich denkt jede Abteilung, sie sei die wichtigste“, sagt Groß-Bölting. „Aber wenn dann 20 Leute vor den IT-Verantwortlichen stehen und verlangen, dass ihr System als erstes wieder läuft, hilft das niemandem.“

Oft verfallen Unternehmen, die Ziel eines Cyberangriffs geworden sind, in eine Art Schockstarre aus Angst und Scham – wie Opfer gewöhnlicher Kriminalität auch. Viele Unternehmen halten den Angriff geheim, sei es aus Angst, unprofessionell zu wirken oder weil man sich einfach keine Blöße geben möchte. Weder vor der Konkurrenz noch vor der Kundschaft. Kira Groß-Bölting rät jedoch strikt davon ab, einen solchen Angriff unter den Teppich kehren zu wollen und gar nicht oder auch nur zögerlich zu kommunizieren.

„Bei Kundinnen oder Auftraggebern ist die Akzeptanz erfahrungsgemäß größer, wenn eine Firma in den offenen Austausch geht“, sagt sie. „Wenn man ganz klar sagt: Wir sind gehackt worden. Bei uns geht gerade gar nichts mehr, aber wir haben uns ein professionelles Team geholt, dass uns unterstützt, den Schaden zu beheben.“ Niemand müsse dabei inhaltlich und technisch in die Tiefe gehen. Aber sowohl die Beschäftigten als auch das Kunden- oder Partnernetzwerk zeitnah zu informieren und auf dem Laufenden zu halten sei wichtig, um allen Beteiligten die Gewissheit zu geben, dass man nicht machtlos und überfordert ist, sondern dass es vorangeht.

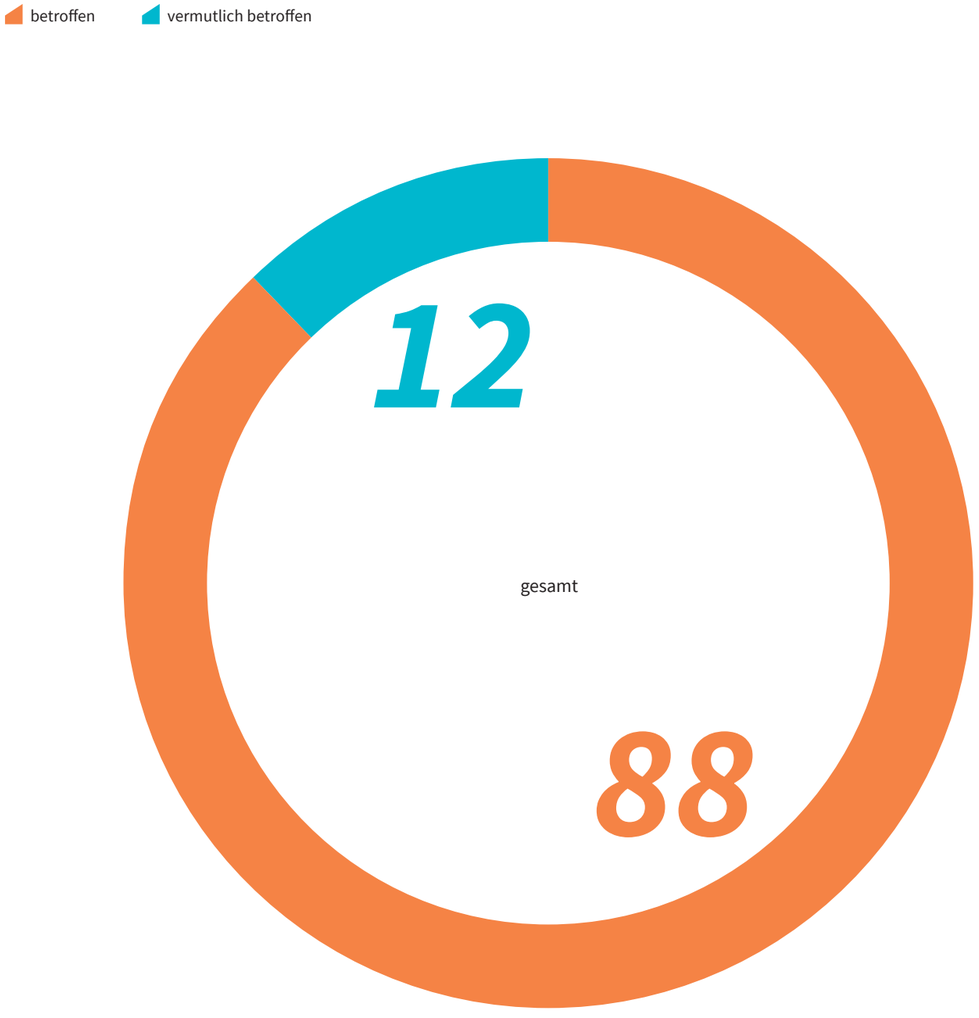
Sich schämen, Opfer eines Cyberangriffs geworden zu sein, sei ohnehin der falsche Ansatz: „Schuld sind nicht die Opfer, sondern die Täter“, sagt Groß-Bölting. „Und eine Welt, in der es eine hundertprozentig sichere IT gibt und niemand mehr einem Hacker-Angriff zum Opfer fällt, wird es wohl leider nie geben.“

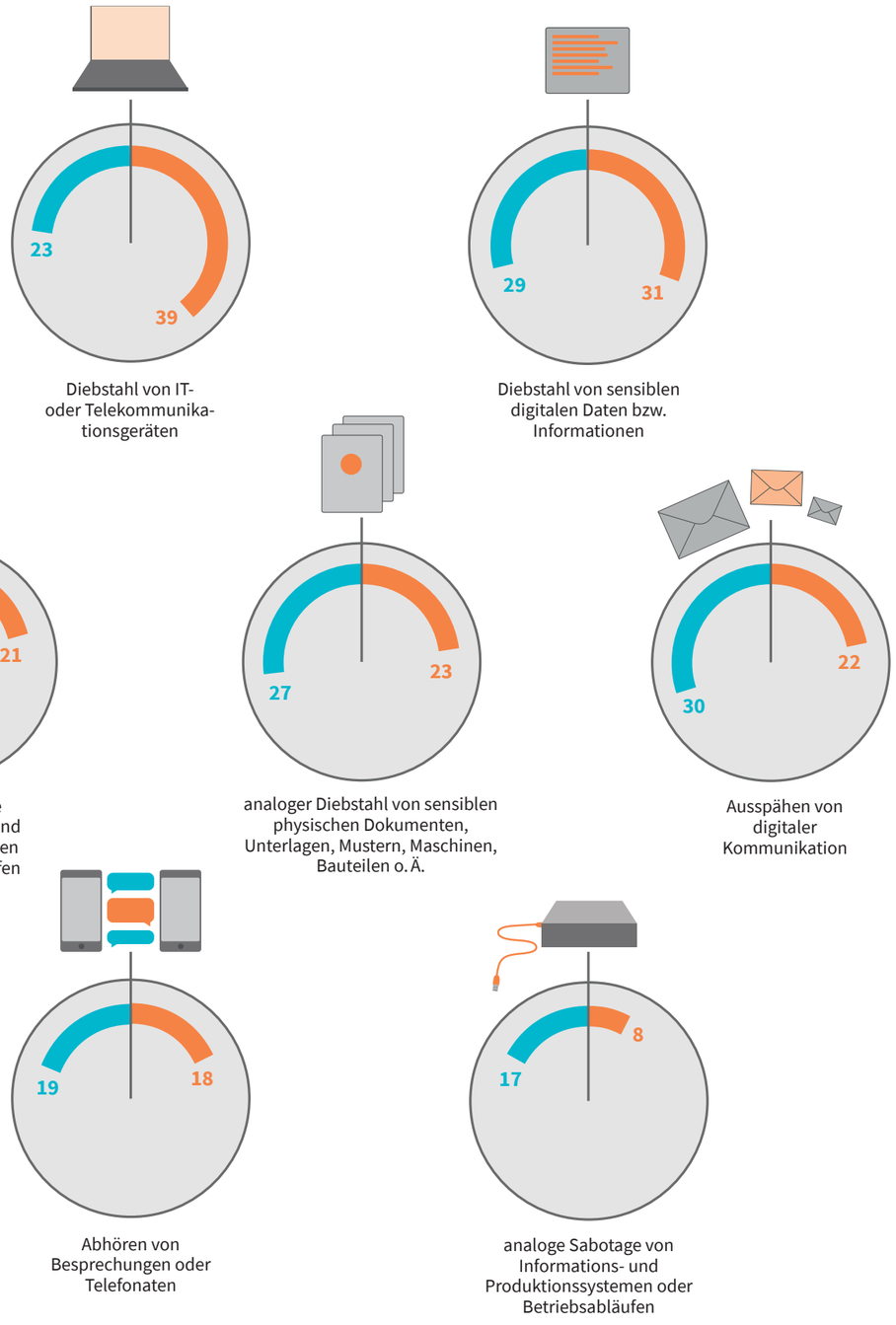
WIRTSCHAFT

Industrie 4.0, künstliche Intelligenz (KI), Internet of Things (IoT), mobiles Arbeiten: Unternehmen bieten Cyberkriminellen immer neue Angriffsflächen. Wo lauern die größten Gefahren? Welche Daten und Systeme stehen hoch im Kurs? Wie gut sind Firmen für den Ernstfall gewappnet? Und was tun, wenn der Schaden passiert ist?

Wir sind verwundbar

Handlungen von Cybercrime bei (vermutlich) betroffenen Unternehmen; Deutschland; 2021; in Prozent *





* Mehrfachauswahl möglich. Quelle: Bitkom e. V.

Cyberbegriffe-Übersicht im Glossar auf Seite 100 – 103.

Gestiegen

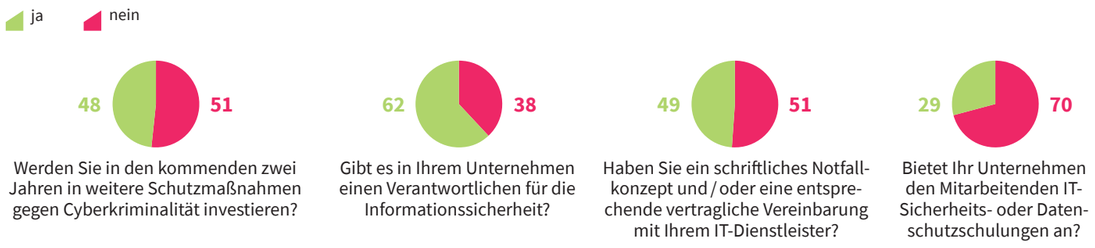
Dauer bis zur Wiederherstellung der Systeme nach Cyberattacken; Entscheiderinnen und Entscheider in kleinen und mittleren Unternehmen (n=300); Deutschland; 2021; in Prozent

	2019	2020	2021	Veränderung 2019 – 2021
weniger als 1 Tag	33	35	36	9,1 %
1 bis 3 Tage	48	42	21	– 56,3 %
4 Tage und länger	18	22	39	**116,7 %**

Quelle: Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GdV)

Gewagt

Wichtigkeit von Cybersicherheit; Entscheiderinnen und Entscheider in kleinen und mittleren Unternehmen; Deutschland; 2021; in Prozent



Quelle: Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GdV)

Geübt

Nutzung von IT-Schwachstellenmanagement; Unternehmen mit mehr als 100 Mitarbeitenden; Deutschland; 2021; in Prozent

Ja, es gibt ein formales Schwachstellenmanagement-Vorgehen inklusive Prozess und Policy.	76
Ja, es gibt ein informales Schwachstellenmanagement-Vorgehen. Das Schwachstellenmanagement wird unregelmäßig und bei Bedarf dezentral durchgeführt.	21
Nein, es gibt kein Schwachstellenmanagement. Die Einführung ist für die nächsten 12 Monate geplant.	3

Quelle: KPMGsgesellschaft

Geflickt

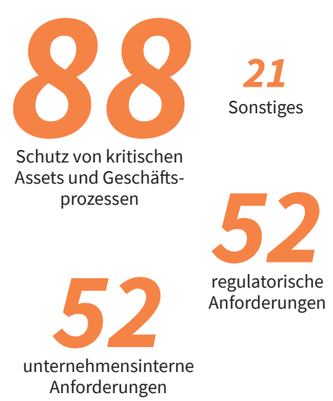
Häufigkeit der Installation von Patches; Unternehmen mit mehr als 100 Mitarbeitenden; Deutschland; 2021; in Prozent *

	wöchentlich	monatlich	quartalsweise	Sonstiges, z. B. anlassbezogen
Betriebssystem	22	56	13	28
Middleware	10	21	24	38
Cloud	26	17	4	65
IoT	0	6	0	89

* Mehrfachauswahl möglich. Quelle: KPMGsgesellschaft

Gefürchtet

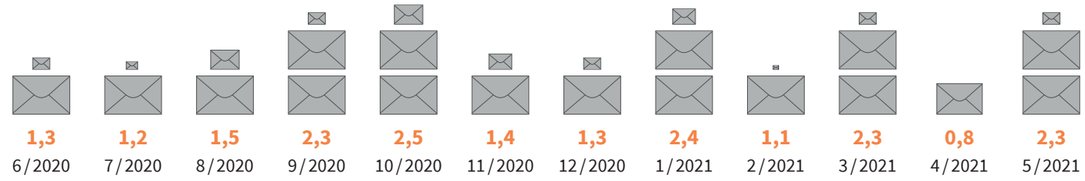
Treiber für die Durchführung von IT-Schwachstellenmanagement; Unternehmen mit mehr als 100 Mitarbeitenden; Deutschland; 2021; in Prozent *



* Mehrfachauswahl möglich. Quelle: KPMG Wirtschaftsprüfungsgesellschaft

Schwankend

Zahl von Spam-E-Mails je erwünschter Mail; Deutschland



Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Wachsend

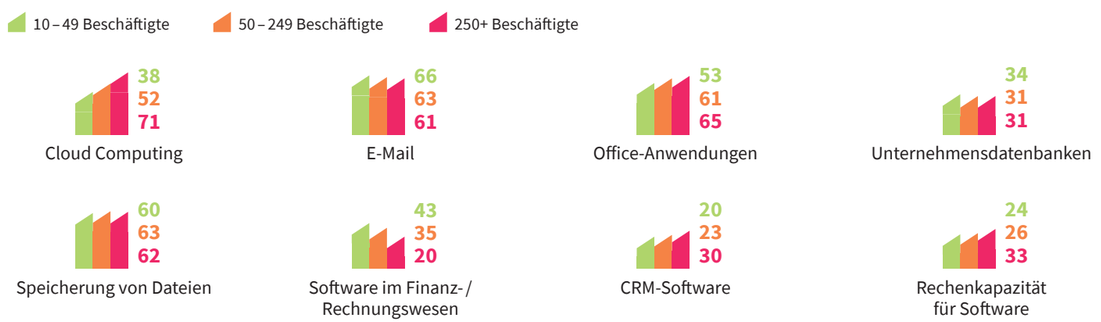
Nutzung von Cloud Services in Unternehmen ab 10 Beschäftigten; Deutschland

	2016	2021	Veränderung 2016 – 2021
Cloud Computing	16	28	75,0 %
E-Mail	49	65	32,7 %
Office-Anwendungen	31	55	77,4 %
Unternehmendatenbanken	33	33	0,0 %
Speicherung von Daten	63	61	– 3,2 %
Software im Finanz- / Rechnungswesen	26	40	53,8 %
CRM-Software	18	21	16,7 %
Rechenkapazität für Software	19	25	31,6 %
Anteil der Unternehmen, die im Jahr 2021 Cloud Services nutzen für …			
… ERP-Software			18
… Computerplattformen			23
… Sicherheits-Software			48

Quelle: Destatis

Wechselnd

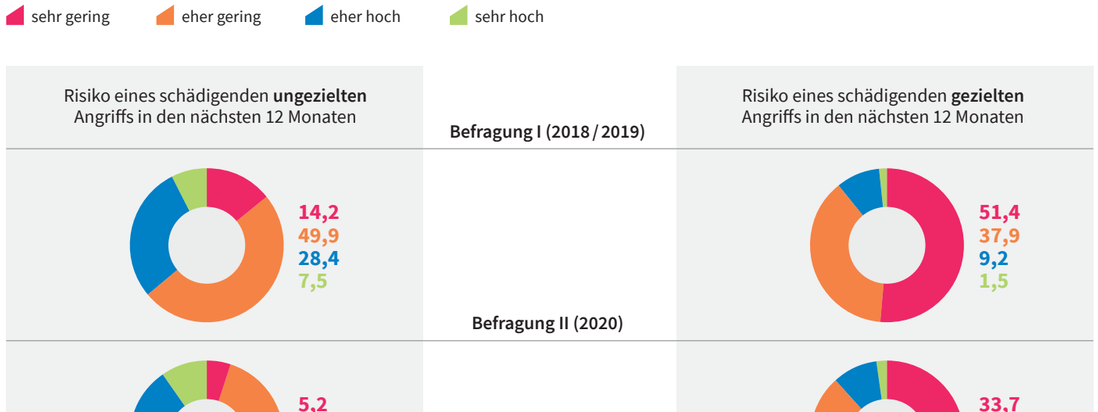
Nutzung von Cloud Services nach Beschäftigtengrößenklassen in Unternehmen ab 10 Beschäftigten; 2021; Deutschland



Quelle: Destatis

Das Bewusstsein wächst

Risikoeinschätzung im Unternehmen in Bezug auf einen Cyberangriff; Entscheidungsträgerinnen und Entscheidungsträger in Unternehmen; Deutschland; in Prozent



Quelle: Kriminologisches Forschungsinstitut Niedersachsen e. V.

Die Methoden variieren

Jahresprävalenzen nach Angriffsart; Entscheidungsträgerinnen und Entscheidungsträger in Unternehmen; Deutschland; in Prozent

	Befragung I (2018/2019)	Befragung II (2020)	Vergleich I und II
Angriffsarten insgesamt	**50,2**	**59,6**	**18,7 %**
Phishing	24,8	42,1	69,8 %
sonstige Schadsoftware	25,7	35,7	38,9 %
Spyware	18,3	16,2	– 11,5 %
Ransomware	20,6	14,2	– 31,1 %
CEO-Fraud	9,9	10,6	7,1 %
DDos	9,6	8,3	– 13,5 %
Defacing	4,5	0,9	– 80,0 %
manuelles Hacking	2,5	0,4	– 84,0 %

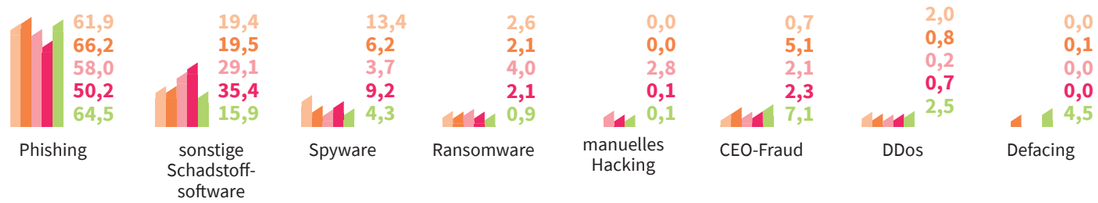
Quelle: Kriminologisches Forschungsinstitut Niedersachsen e. V.

In der **Prävalenzrate** werden alle Angriffe berücksichtigt, auf die das Unternehmen direkt reagieren musste, z. B. durch die Einleitung von Maßnahmen. Die Jahresprävalenz entspricht den Cyberangriffen in den vergangenen 12 Monaten. Die **Inzidenzrate** bildet die Zahl der Cyberangriffe in den vergangenen 12 Monaten je 100 Unternehmen ab.

Quelle: Kriminologisches Forschungsinstitut Niedersachsen e. V.

Verführt

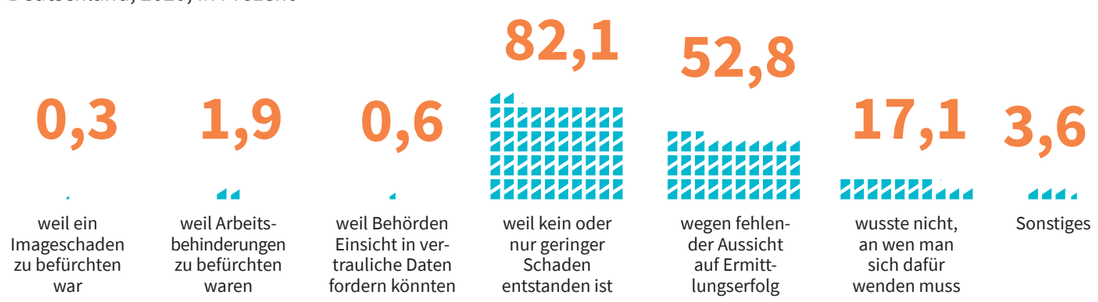
Anteil der erlebten Cyberangriffe nach Angriffsart und Beschäftigtengrößenklassen; Entscheidungsträgerinnen und Entscheidungsträger in Unternehmen; Deutschland; 2020; in Prozent



Quelle: Kriminologisches Forschungsinstitut Niedersachsen e. V.

Verschwiegen

Nichtanzeigegründe einer Cyberattacke; Entscheidungsträgerinnen und Entscheidungsträger in Unternehmen; Deutschland; 2020; in Prozent *



* Mehrfachauswahl möglich. Quelle: Kriminologisches Forschungsinstitut Niedersachsen e. V.

Gezählt

Inzidenzraten nach Angriffsart; Entscheidungsträgerinnen und Entscheidungsträger in Unternehmen; Deutschland; 2020; durchschnittliche Zahl der Cyberangriffe in 12 Monaten je 100 Unternehmen

Phishing	1 594
sonstige Schadsoftware	588
Spyware	319
Ransomware	68
Defacing	42
CEO-Fraud	36
manuelles Hacking	8
DDos	5

Quelle: Kriminologisches Forschungsinstitut Niedersachsen e. V.

Getroffen

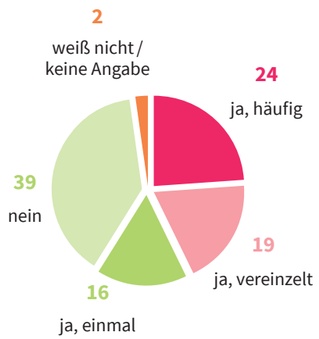
Schwerwiegendster Cyberangriff nach Angriffsart; Entscheidungsträgerinnen und Entscheidungsträger in Unternehmen; Deutschland; 2020; in Prozent *

Phishing	44,9
sonstige Schadsoftware	24,2
Ransomware	21,8
DDos	10,1
CEO-Fraud	5,7
Spyware	4,8
Defacing	1,9
manuelles Hacking	0,5
sonstiger Angriff	0,2

* Mehrfachauswahl möglich.
Quelle: Kriminologisches Forschungsinstitut Niedersachsen e. V.

Vorfälle

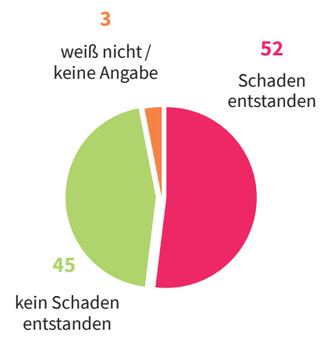
Durch Homeoffice entstandene Sicherheitsvorfälle; Unternehmen, bei denen Homeoffice generell möglich ist; Deutschland; 2021; in Prozent



Quelle: Bitkom e. V.

Schäden

Schäden durch Sicherheitsvorfälle im Homeoffice; Unternehmen, bei denen Homeoffice generell möglich ist; Deutschland; 2021; in Prozent



Quelle: Bitkom e. V.

Arbeitsmittel

Nutzung von privaten Geräten als Arbeitsmittel; zufällig ausgewählte abhängig Beschäftigte; Deutschland; 2021; in Prozent

Nutzen Sie bei Ihrer Arbeit zu Hause auch private Geräte als Arbeitsmittel?

Quelle: Deutscher Gewerkschaftsbund (DGB)

Risiko-Einschätzungen

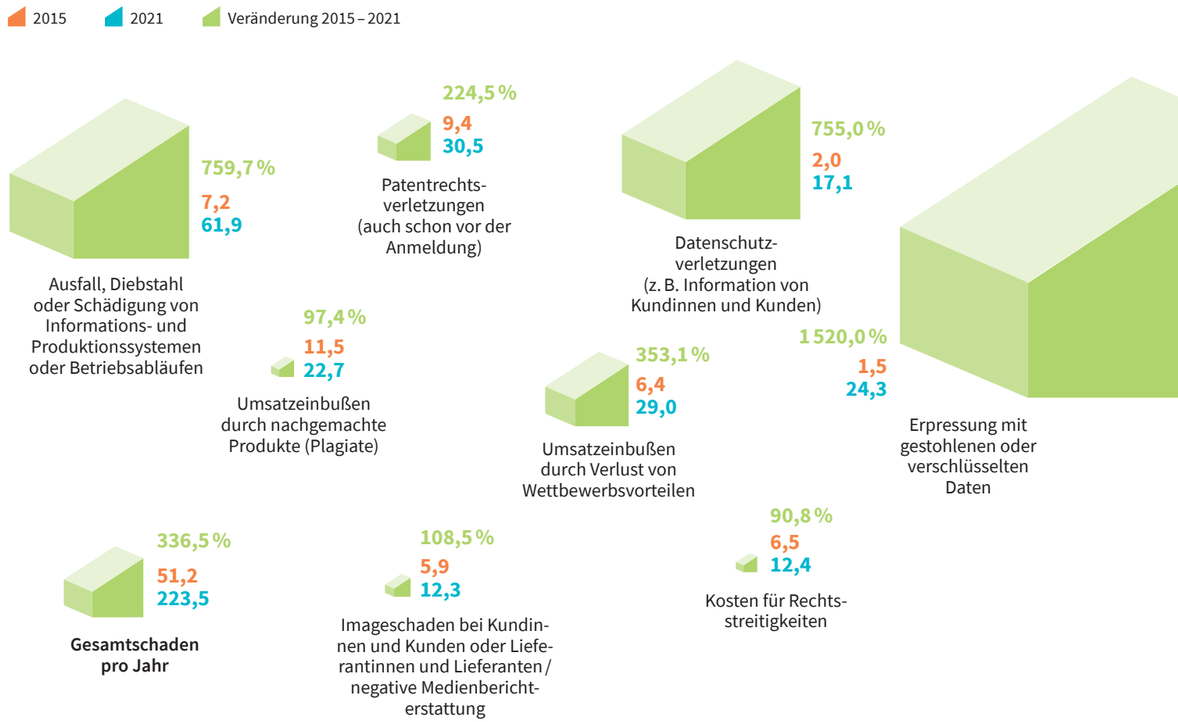
Einschätzung der Bedrohung von Unternehmen nach Schadsoftwarearten; Entscheidungsträgerinnen und Entscheidungsträger in Unternehmen; Deutschland; 2021; in Prozent *

	sehr bedrohlich	eher bedrohlich	eher nicht bedrohlich	überhaupt nicht bedrohlich	weiß nicht / k. A.
Ransomware-Angriff	57	39	≤2	≤2	4
Zero-Day-Exploit	57	38	4	≤2	≤2
Spyware-Angriff	52	31	10	7	7
Angriffe mit Quantencomputern	51	28	13	4	4
Backdoors bzw. Trapdoors	38	40	11	6	6
Mangel an qualifizierten IT-Sicherheitskräften	35	33	21	10	10
zunehmende Vernetzung von Geräten und Maschinen	33	39	23	4	4
Social Engineering	31	32	17	16	16
fehlkonfigurierte Cloud-Umgebung	31	25	21	17	17
zunehmende Fluktuation von Mitarbeitenden	24	45	24	6	6
Anzapfen von Rechenleistungen z. B. zum unbemerkten Schürfen von Kryptowährungen	11	38	28	16	16

* Werte ≤2 zur übersichtlicheren Darstellung ausgeblendet. Mehrfachauswahl möglich. Quelle: Bitkom e. V.

Erpresst, bestohlen, lahmgelegt

Schaden durch Cyberangriffe nach Delikttyp; Unternehmen, die in den vergangenen 12 Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren; Deutschland; in Milliarden Euro



Quelle: Bitkom e. V.

Bewertet

Bewertung des Risikos, von verschiedenen Tätergruppen geschädigt zu werden: großes oder sehr großes Risiko; Führungskräfte deutscher Unternehmen; 2021; in Prozent *

Organisiertes Verbrechen	68
Hacktivisten (z. B. Anonymous)	42
ausländischer Geheimdienst	30
konkurrierendes ausländisches Unternehmen	30
ehemalige Mitarbeitende	23
eigene Mitarbeitende	22
ausländische Kundinnen und Kunden oder Lieferantinnen und Lieferanten	18
konkurrierendes inländisches Unternehmen	17
sonstige Geschäftspartnerinnen und Geschäftspartner	10
inländische Kundinnen und Kunden oder Lieferantinnen und Lieferanten	8

* Mehrfachauswahl möglich. Quelle: EY

Betroffen

Cyberangriffe & Datenklau; Führungskräfte deutscher Unternehmen; 2021; in Prozent

Gab es in Ihrem Unternehmen bereits konkrete Hinweise auf Cyberangriffe bzw. Datenklau innerhalb der vergangenen zwei Jahre?

ja, mehrfach	27
ja, einmal	17
nein	56

Quelle: EY

Beispiel-Szenario Cyberangriff

Case:
Über eine Phishing-Mail schleust ein Hacker einen Trojaner in die Office-IT eines mittelständischen Maschinenbauers ein. Der Verschlüsselungstrojaner greift über eine Schnittstelle auf die Produktions-IT zu und legt das gesamte Firmennetzwerk lahm. Für die Freigabe verlangen die Cyberkriminellen ein hohes Lösegeld in Bitcoin.

Auswirkungen:
Der Trojaner verhindert den Zugang auf alle Rechner, die Produktion steht still, die Sicherheit von Betriebsgeheimnissen, Kunden- und Vertragsdaten ist nicht mehr gewährleistet. Das Unternehmen ist handlungsunfähig und informiert zunächst die Polizei über den Angriff. Polizei und Staatsanwaltschaft raten davon ab, das Lösegeld zu zahlen.

Quelle: Unternehmen Cybersicherheit – gemeinsame Initiative von VDMA und VSMA

Addiert

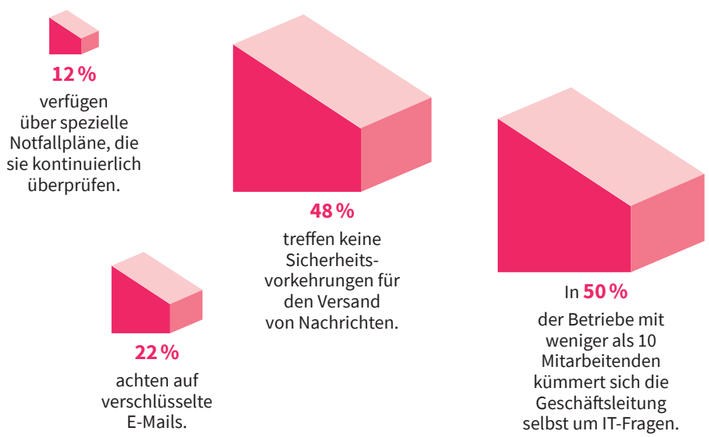
Beispiel-Szenario Cyberangriff: Kosten eines Cyberangriffs; Deutschland; 2020; in Euro

1. IT-Forensiker und Datenwiederherstellung	50 000
2. Betriebsunterbrechung und Produktionsausfall	160 000
3. Erfüllung von Datenschutzpflichten	20 000
4. PR- und Krisenkommunikation	20 000
5. Marketingmaßnahmen wegen Imageschaden	15 000
Gesamtkosten	**265 000**

Quelle: Unternehmen Cybersicherheit – gemeinsame Initiative von VDMA und VSMA

Unreflektiert

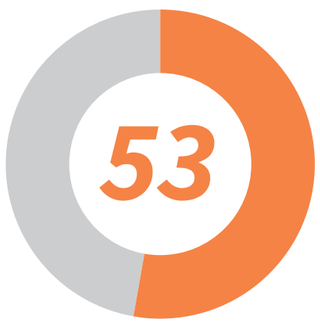
Cybersicherheit in deutschen Unternehmen; 2022; in Prozent



Quelle:Bundesministerium für Wirtschaft und Klimaschutz

Attackiert

Anteil der mittelständischen Unternehmen in Deutschland, von denen Daten (in den meisten Fällen E-Mail- / Passwort-Kombinationen) im Darknet zu finden waren; 2020; in Prozent



Quelle: Gesamtverband der Deutschen Versicherungswirtschaft e. V.

Variiert

Zahl neuer, bekannt gewordener Schadprogramm-Varianten; Deutschland

2020 2021

pro Tag
322 000
394 000

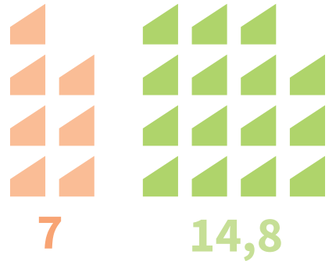
pro Jahr
117,4 Millionen
144 Millionen

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Infiziert

Zahl der Meldungen zu Schadprogramm-Infektionen; Deutschland; in Millionen

2020 2021



Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Alarmiert

Zahl der Mails und Websites mit Schadprogrammen in deutschen Regierungsnetzen

2020 2021

abgefangene Mails mit Schadprogrammen in deutschen Regierungsnetzen
35 000 44 000

Sperrung von Websites wegen enthaltener Schadprogramme
52 000 74 000

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Kreiert

Regionaler Ursprung von Cyberangriffen; befragte Unternehmen in Deutschland, die in den vergangenen 12 Monaten von Diebstahl, Industriespionage oder Sabotage betroffen waren; 2021; in Prozent *

*Mehrfachauswahl möglich. Quelle: Bitkom e. V.

Einfallstore

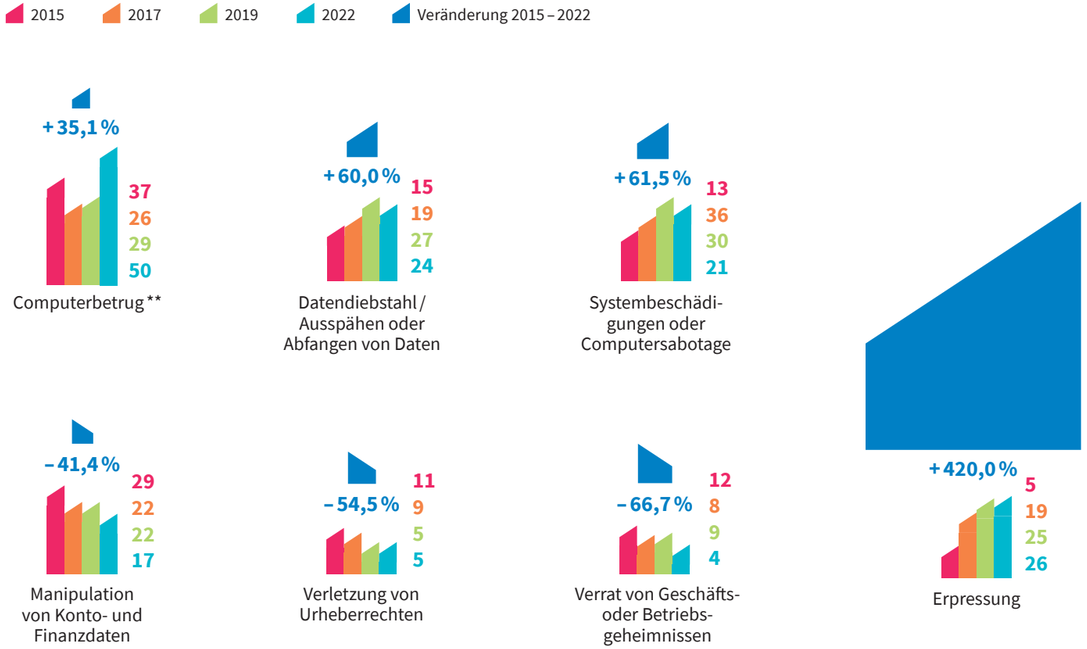
Begünstigende Faktoren für Cybercrime; Mitarbeitende von repräsentativ ausgewählten Unternehmen; Deutschland; in Prozent *

	2015	2017	2019	2022	Veränderung 2015 – 2022
Unachtsamkeit	88	89	90	95	8,0 %
mangelnde Sicherheitskultur bei Mitarbeitenden	77	84	86	86	11,7 %
Nichterkennen erster Anzeichen von Verdachtsfällen	76	80	85	84	10,5 %
unzureichend geschultes Personal	60	76	83	81	35,0 %
zunehmende Komplexität eingesetzter Technologie	82	81	83	78	– 4,9 %
ungenügende Sicherheit der IT-Syteme vor Angriffen	57	68	76	61	7,0 %
limitiertes Budget für Sicherheitsmaßnahmen	39	56	66	56	43,6 %
fehlende Ad-hoc-Kontrollen	44	52	56	56	27,3 %
verteilte Datenhaltung und damit mangelnde Kontrolle	39	56	60	54	38,5 %
nichts davon	2	1	0	1	– 50,0 %

* Mehrfachauswahl möglich. Quelle: KPMG

Vorkommnisse

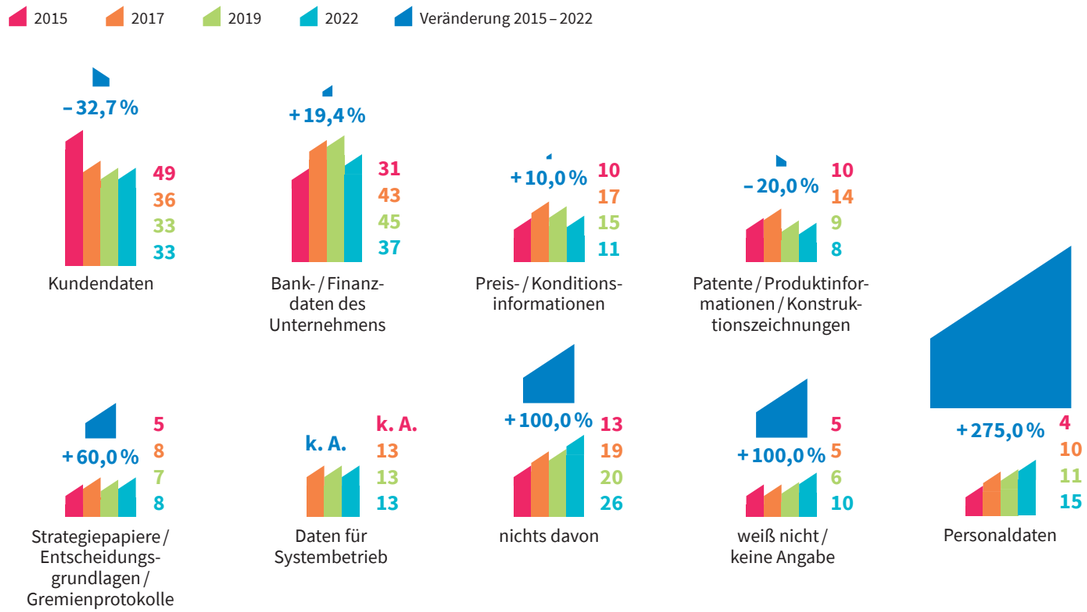
Betroffenheitsarten deutscher Unternehmen durch Cybercrime; Mitarbeitende von repräsentativ ausgewählten Unternehmen; Deutschland; in Prozent *



* Mehrfachauswahl möglich. ** betrügerische Handlungen unter Ausnutzung von Kommunikations- und Informationstechnologien und per Manipulation von Datenverarbeitungssystemen und -prozessen. Quelle: KPMG

Informationsarten

Von Cybercrime betroffene Informationsarten; Mitarbeitende von repräsentativ ausgewählten Unternehmen; Deutschland; in Prozent *



* Mehrfachauswahl möglich. Quelle: KPMG

Systeme

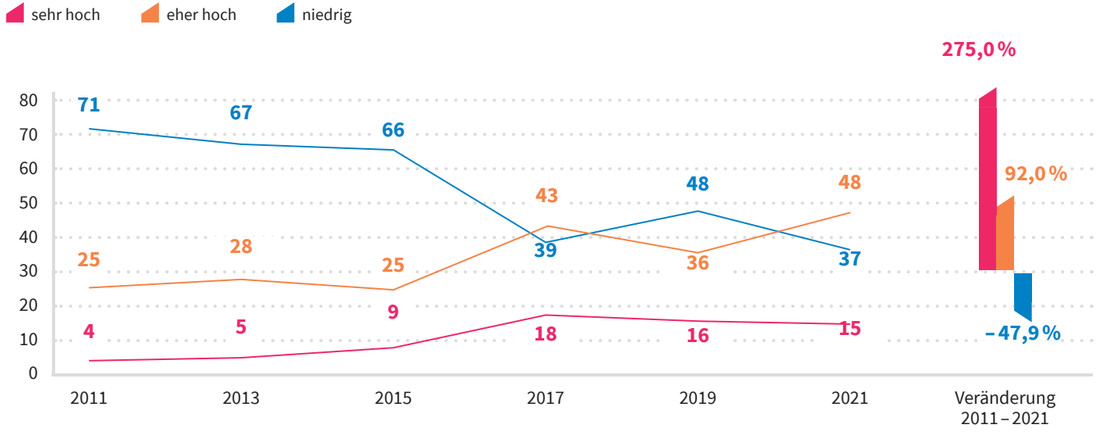
Angegriffene Systeme; Mitarbeitende von repräsentativ ausgewählten Unternehmen; Deutschland; in Prozent *

	2015	2017	2019	2022	Veränderung 2015 – 2022
Mailserver	46	53	61	67	45,7 %
Fileserver	15	25	25	32	113,3 %
Webserver	30	18	20	24	– 20,0 %
Client-PCs / Workstations	25	22	23	21	– 16,0 %
Laptops	15	17	17	18	20,0 %
Netzwerkgeräte bzw. Appliances	10	17	18	18	80,0 %
externer Zugang	9	11	15	16	77,8 %
Cloud-Services	4	3	6	11	175,0 %
Telefonanlage	12	9	8	9	– 25,0 %
bargeldlose Zahlungssysteme	30	14	11	8	– 73,3 %
mobile Geräte	11	11	10	7	– 36,4 %
Industriesteueranlagen	k. A.	3	2	4	k. A.
nichts davon	8	11	9	4	– 50,0 %
weiß nicht / keine Angabe	3	2	3	3	0,0 %

* Mehrfachauswahl möglich. Quelle: KPMG

Unheilvoll

Risiko-Einschätzung von Cyberangriffen für das eigene Unternehmen; Führungskräfte deutscher Unternehmen; in Prozent



Quelle: EY

Schmerzvoll

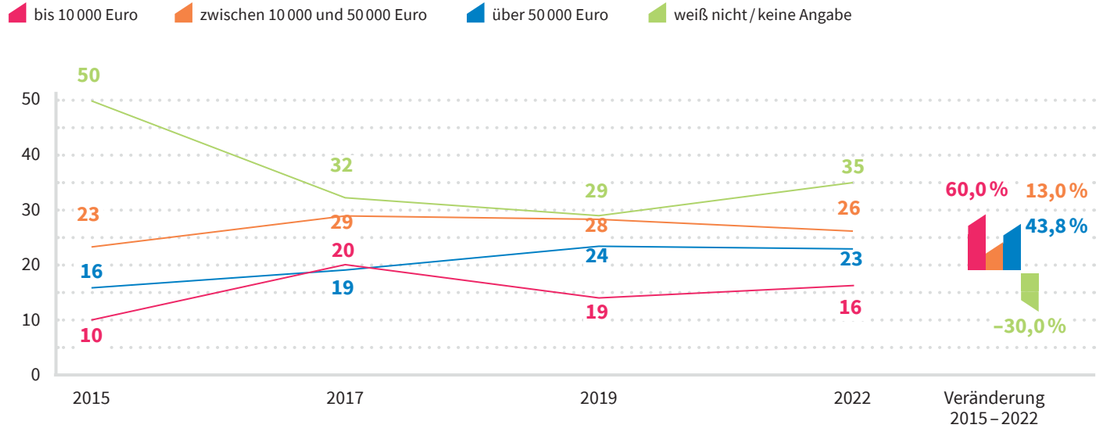
Entdeckung von Cybercrime-Handlungen; Mitarbeitende von repräsentativ ausgewählten Unternehmen; in Prozent

	2015	2017	2019	2022	Veränderung 2015 – 2022
offene Hinweise durch Unternehmensinterne	84	46	47	37	– 56,0 %
offene Hinweise durch Unternehmensexterne	58	32	25	22	– 62,1 %
Routineprüfung	52	44	36	33	– 36,5 %
Zufall	48	36	37	33	– 31,3 %
Meldung von automatisierten Systemen	47	41	40	40	– 14,9 %
Strafverfolgungs- bzw. Aufsichtsbehörden	22	12	9	9	– 59,1 %
Systemstörungen oder -ausfälle	19	38	33	37	94,7 %
Medienberichterstattung / Internetforen / sonstige Öffentlichkeit	15	12	12	19	26,7 %
anonyme Hinweise	5	4	4	3	– 40,0 %
durch Ombudsmann / Whistleblowing	5	4	2	2	– 60,0 %
Erpressung	3	15	17	16	433,3 %
Selbstanzeige durch Mitarbeitende	2	6	8	8	300,0 %
BSI	k. A.	k. A.	k. A.	13	k. A.
Hinweise Darknet	k. A.	k. A.	k. A.	4	k. A.
Bundes- oder Landesamt für Verfassungsschutz	k. A.	k. A.	k. A.	5	k. A.

* Mehrfachauswahl möglich. Quelle: KPMG

Sinnvoll

Investitionen im Bereich Cybercrime nach Jahr; Mitarbeitende von repräsentativ ausgewählten Unternehmen; Deutschland; in Prozent



Quelle: KPMG

Wertvoll

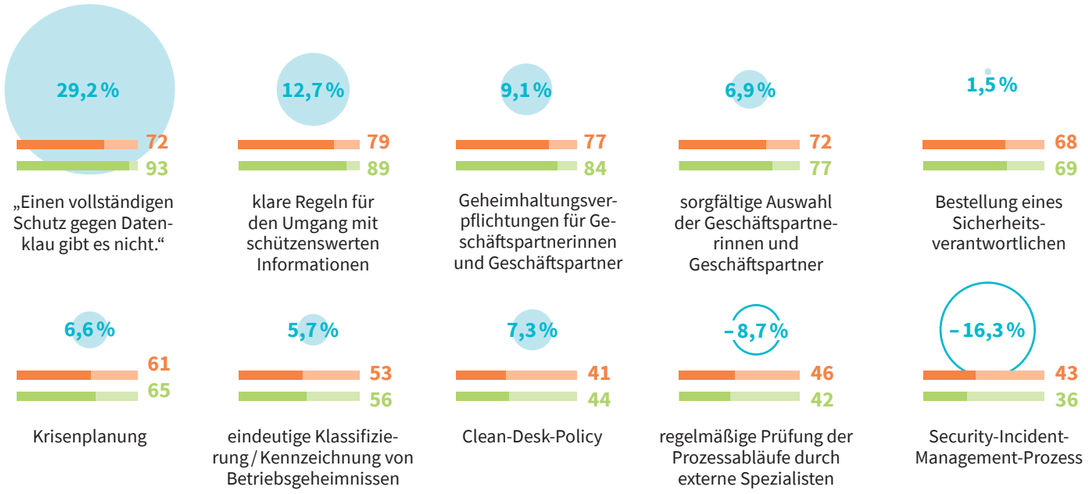
Investitionen in Sicherheitsvorkehrungen im Bereich IT-Sicherheit; Führungskräfte deutscher Unternehmen; in Prozent

	2019	2021	Veränderung 2019 – 2021
Firewall / VPN-Zugänge	89	97	9,0 %
Antivirensoftware	91	96	5,5 %
Passwortschutz auf allen Geräten	83	94	13,3 %
eingeschränkte oder kontrollierte Nutzung externer Schnittstellen von PCs / Laptops	58	75	29,3 %
Intrusion Prevention / Detection Systems	50	58	16,0 %
Penetration-Tests	43	55	27,9 %
Zero-Trust-Umgebung (starke Einschränkungen der Zugänge zu int. Netzwerksegmenten)	k. A.	53	k. A.
hohe Standards (nach BSI-Grundschutz, ISO 27000) bei der IT-Sicherheit	68	52	– 23,5 %
abhörsichere Kommunikation (Telefon, E-Mail, Fax)	k. A.	31	k. A.
ISMS (Information Security Management System)	k. A.	30	k. A.
Zertifizierung nach BSI-Standard	24	24	0,0 %
Security Operation Center (SOC) eingerichtet	25	23	– 8,0 %
SIEM (Security Information and Event Management)	24	20	– 16,7 %
Sonstiges	k. A.	7	k. A.

*Mehrfachauswahl möglich. Quelle: EY

Alternativlos

Prozesstechnische Vorsichtsmaßnahmen im Unternehmen; Führungskräfte deutscher Unternehmen; in Prozent



*Mehrfachauswahl möglich. Quelle: EY

Nicht planlos

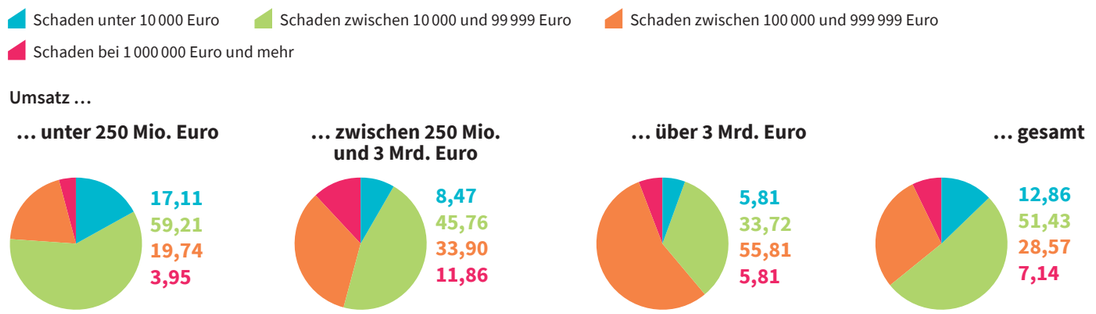
Versäumnisse bei der Reaktion auf Cyberangriffe; Mitarbeitende von repräsentativ ausgewählten Unternehmen; in Prozent *

	2015	2017	2019	2022	Veränderung 2015 – 2022
Es gab keine Versäumnisse bei der Reaktion.	75	64	66	54	– 28,0 %
unklare Informationslage	13	20	17	21	61,5 %
bei der Kommunikation der Vorkommnisse innerhalb des Unternehmens	9	16	14	19	111,1 %
unklare Verantwortlichkeiten bzw. Fehler in der Kommunikationskette	11	18	17	18	63,6 %
unzureichend definierte Sofortmaßnahmen	10	18	15	15	50,0 %
Dauer bis zur Umsetzung nötiger Sofortmaßnahmen	11	10	13	12	9,1 %
Kompetenzdefizite bei der Beweissicherung	7	7	8	8	14,3 %
bei der Kommunikation der Vorkommnisse außerhalb des Unternehmens	2	6	4	7	**250,0 %**
Kompetenzdefizite bei der Sicherung gefährdeter Vermögenswerte	3	7	5	7	133,3 %
zu späte Einbindung externer Fachleute	3	6	6	6	100,0 %
beim Umgang mit Tatbegehenden (intern oder extern)	6	7	5	4	– 33,3 %
bei der Sanktionierung	9	5	5	2	**– 77,8 %**
fehlende Einbindung einer Behörde bzw. der Polizei	4	4	4	2	– 50,0 %

* Aufgrund von Rundungsifferenzen ergibt die Summe nicht 100 Prozent. Quelle: KPMG

Uferlos

Gesamtschaden durch Cybercrime nach Unternehmensumsatz; Mitarbeitende von repräsentativ ausgewählten Unternehmen; Deutschland; 2021 – 2022; in Prozent *



* Aufgrund von Rundungsifferenzen ergibt die Summe nicht 100 Prozent. Quelle: KPMG

Schutzlos

Cyberversicherungen; Mitarbeitende von repräsentativ ausgewählten Unternehmen; in Prozent *

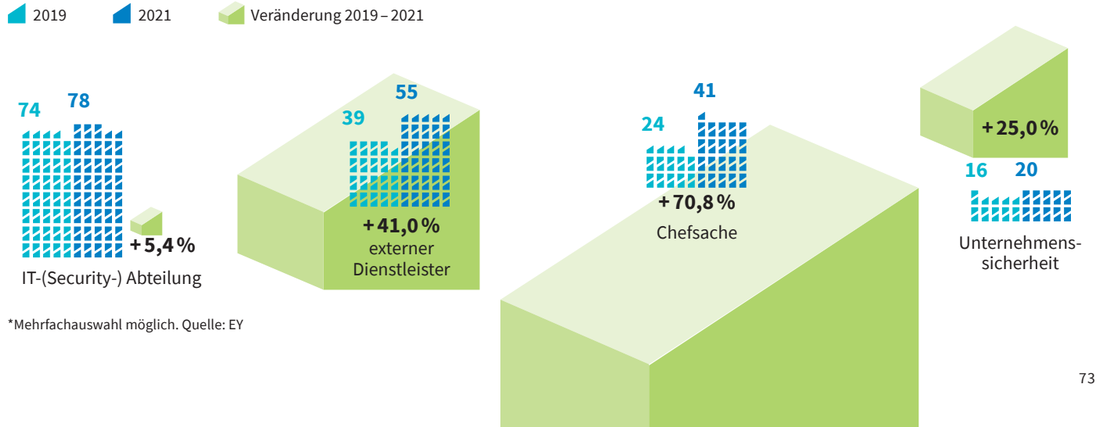
Bekanntheit von Cyberversicherungen	2017	2022	Veränderung 2017 – 2022
ja, ist bekannt	55	74	34,5 %
nein, bisher nicht bekannt	42	22	– 47,6 %
weiß nicht / keine Angabe	3	5	66,7 %

Abschluss einer Cyberversicherung	2017	2022	Veränderung 2017 – 2022
ja	22	39	77,3 %
Nein, aber wir prüfen oder planen den Abschluss.	27	23	– 14,8 %
Nein, und wir planen dies auch nicht.	37	21	– 43,2 %
weiß nicht / keine Angabe	14	17	21,4 %

* Aufgrund von Rundungsifferenzen ergibt die Summe nicht 100 Prozent. Quelle: KPMG

Nicht verantwortungslos

Verantwortliche des Schutzes sensitiver Informationen bzw. Daten im Unternehmen; Führungskräfte deutscher Unternehmen; in Prozent *

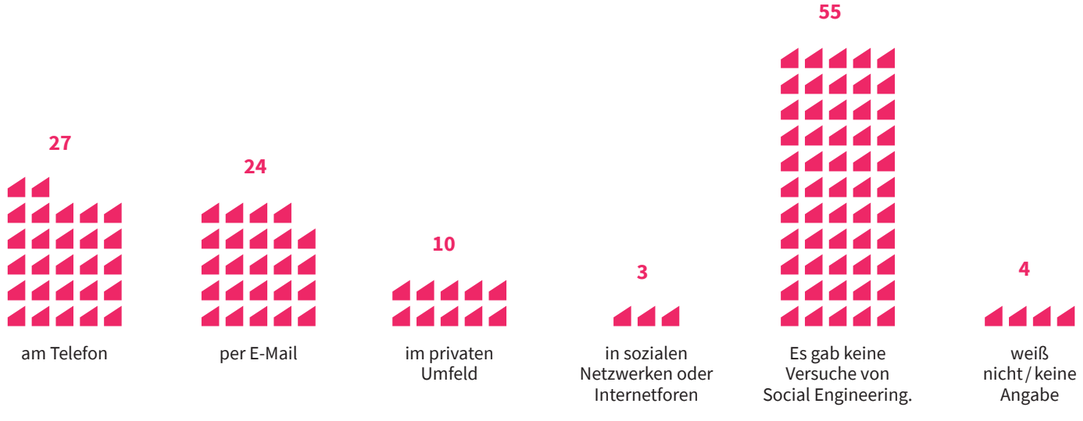


*Mehrfachauswahl möglich. Quelle: EY

Menschlich

Social Engineering als Cybercrime-Methode; Deutschland; 2021; in Prozent *

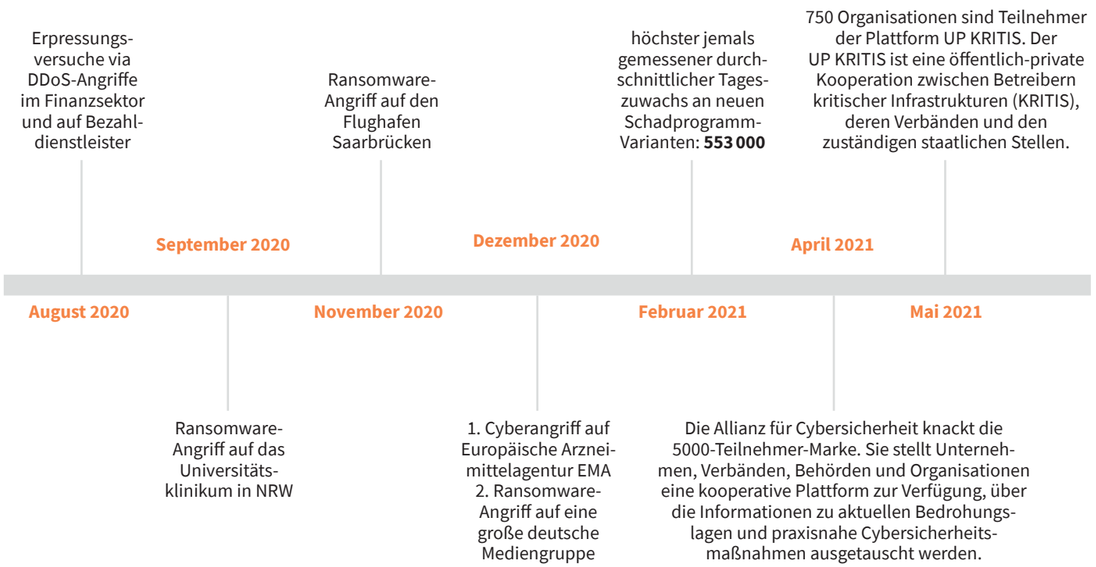
In welchen der folgenden Kontexte gab es innerhalb der vergangenen 12 Monate Versuche, Ihre Mitarbeitenden mittels Social Engineering zu beeinflussen?



*Mehrfachauswahl möglich. Quelle: Bitkom e. V.

Monatlich

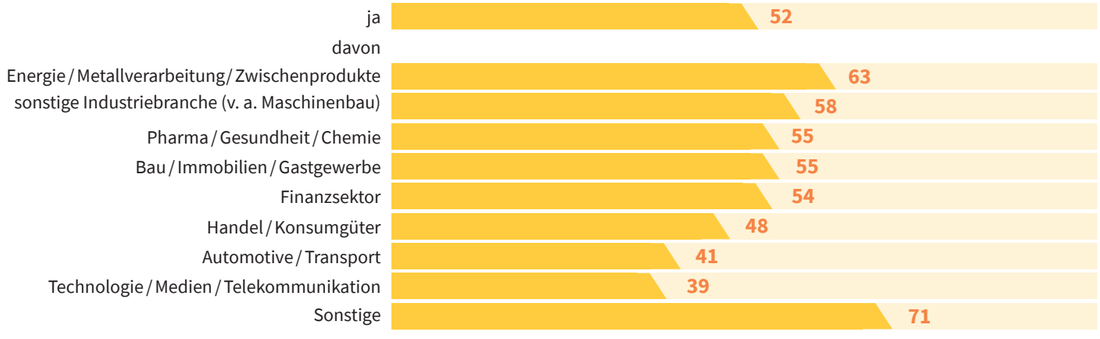
12 Monate Cybersicherheit (Juni 2020 – Mai 2021); ausgewählte Ereignisse



Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Kritisch

Krisenpläne zur Reaktion auf Datenklaufälle in Unternehmen; Führungskräfte deutscher Unternehmen; Anteil der Ja-Antworten nach Branchen; 2021; in Prozent



Quelle: EY

Optimistisch

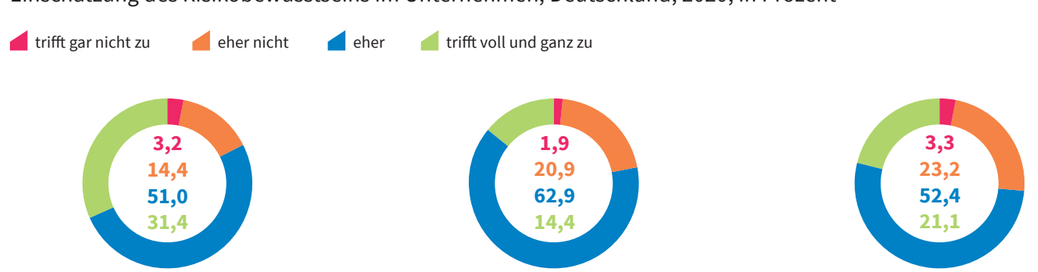
Selbsteinschätzung von Unternehmen zum Thema Cybersicherheit; Zustimmung zu der Aussage; Deutschland; 2021; in Prozent *

Wir schaden unserer Marke, wenn wir mit Kunden- und Partnerdaten nicht sicher umgehen.	71
Wir sind zuversichtlich, dass uns unsere IT-Technologie vor Cybervorfällen schützt.	68
Wir sind sehr zuversichtlich in Bezug auf unsere Bereitschaft zur Cybersicherheit.	68
Cybersicherheit ist für unsere Wettbewerbsfähigkeit auf unserem Markt / in unserer Branche von entscheidender Bedeutung.	65
Die Geschäftsführung / der Vorstand hat eine klare Vorstellung davon, wie die Cybersicherheit verwaltet wird.	63
Die Sicherstellung der Einhaltung lokaler cyberbezogener Vorschriften hat höchste Priorität.	62

* Mehrfachauswahl möglich. Quelle: Hiscox

Zuversichtlich

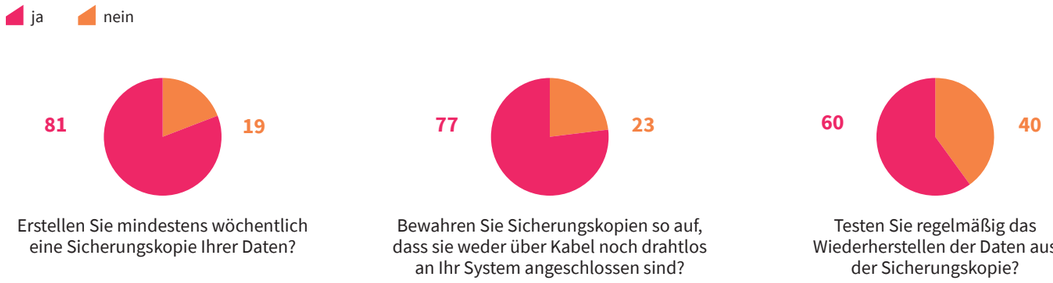
Einschätzung des Risikobewusstseins im Unternehmen; Deutschland; 2020; in Prozent



Quelle: Kriminologisches Forschungsinstitut Niedersachsen e. V.

Die Daten sind sicher?

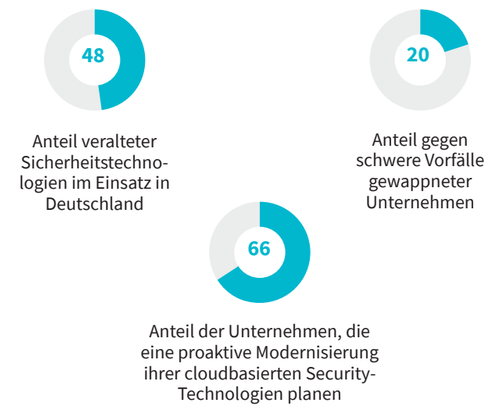
Datensicherung in kleinen und mittleren Unternehmen; Entscheiderinnen und Entscheider in kleinen und mittleren Unternehmen; Deutschland; 2021; in Prozent



Quelle: Gesamtverband der Deutschen Versicherungswirtschaft e. V.

Die Technologien sind alt

Schutz von Unternehmen in Deutschland; Sicherheits- und Datenschutz-Expertinnen und -Experten aus 27 Ländern; 2021; in Prozent



Quelle: Cisco

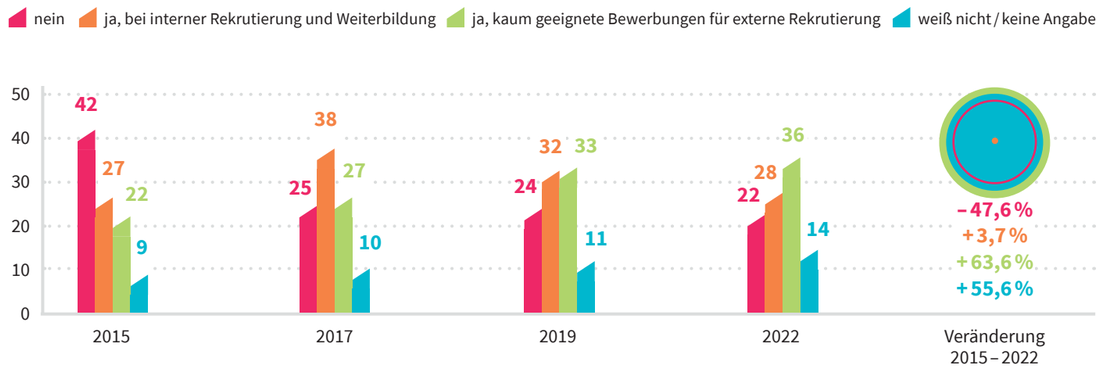
Die Investitionen sind sinnvoll

Bedeutung von Datenschutz für Unternehmen in Deutschland; Sicherheits- und Datenschutz-Expertinnen und -Experten aus 27 Ländern; 2021; in Prozent / Millionen Euro

Quelle: Cisco

Die Fachleute werden knapper

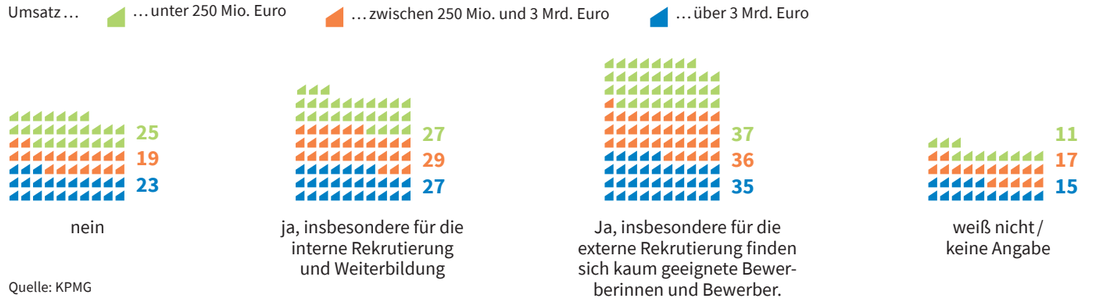
Vorhandensein von Problemen bei der Akquise qualifizierten Personals; Mitarbeitende von repräsentativ ausgewählten Unternehmen; in Prozent



Quelle: KPMG

Das Personal fehlt überall

Verfügbarkeit qualifizierten Personals nach Unternehmensumsatz; Mitarbeitende von repräsentativ ausgewählten Unternehmen; 2021 – 2022; in Prozent



Quelle: KPMG

Die Mühlen mahlen langsam

Sicherheitsvorkehrungen im Bereich Personal; Führungskräfte deutscher Unternehmen; in Prozent

	2019	2021	Veränderung 2019 – 2021
Geheimhaltungsverpflichtungen in Arbeitsverträgen	94	95	1,1 %
Sensibilisierung der Mitarbeitenden für die Gefahren von Spionage	81	85	4,9 %
personalfördernde Maßnahmen zur Steigerung der Verbundenheit	78	75	– 3,8 %
Background-Checks vor der Besetzung sensibler Positionen	38	34	**– 10,5 %**
Whistleblowing-System für Hinweise auf verdächtiges Verhalten	15	20	**33,3 %**
Integritätstests für neue Bewerberinnen und Bewerber	21	19	– 9,5 %
Pre-Employment Screening	15	14	– 6,7 %
Sonstiges	k. A.	4	k. A.

*Mehrfachauswahl möglich. Quelle: EY

Foto: Fraunhofer / SIT

Stress-Test für Abwehrkräfte

In der Cyber Range des Fraunhofer-Instituts für Sichere Informationstechnologie (SIT) kommen selbst ausgebuffte Sicherheitsleute ins Schwitzen. Das Darmstädter Trainingszentrum simuliert lebensecht tückische Hackerangriffe, die sich nur in Teamarbeit stoppen lassen.

Text: Ulf J. Froitzheim

• Mit Darmstadt verbinden viele Menschen vielleicht den 1997 verliehenen Titel „Wissenschaftsstadt“ oder das Jugendstil-Viertel Mathildenhöhe, das zum UNESCO-Welterbe gehört. Die hessische Stadt, in der Deutschlands erstes Hochschul-Rechenzentrum stand, ist aber auch eine Hochburg der IT-Sicherheitsforschung. Die wichtigste der Einrichtungen, die seit 2019 als „Nationales Forschungszentrum für angewandte Cybersicherheit Athene“ zusammenarbeiten, ist das Fraunhofer-Institut für Sichere Informationstechnologie (SIT). Es hat einen Simulator entwickelt, in dem Trainees Angriffe auf IT-Systeme von Unternehmen oder Behörden abwehren müssen – die sogenannte Cyber Range. In kleinen Teams werden die Verteidiger dort systematisch an ihre Grenzen geführt.

Die Frau hinter der Cyber Range ist Haya Shulman. Die 43-jährige israelische Informatik-Professorin entdeckte ihr Faible für IT-Sicherheit beim Militär: Als 18-jährige Wehrdienstleistende lernte sie, wie sich das kleine Land gegen die schon damals erkennbaren Gefahren aus dem Netz verteidigen muss. Auf ihrem Weg zur Habilitation verbrachte sie ein Forschungsjahr in Deutschland – und blieb.

Shulman sieht hierzulande großen Nachholbedarf darin, das verfügbare Wissen zur Cybersicherheit in die Praxis umzusetzen. In einem Interview gab sie Deutschland dafür zum heutigen Stand vier bis fünf von zehn Punkten. Das Problem sei, sagt sie, dass zu viel IT in Eigenregie betrieben werde. „In Israel ist das anders, da setzt nicht jeder selbst einen E-Mail- oder Webserver auf. Man überlässt das lieber denen, die die Expertise haben.“

Realistische Trainings sollen dabei helfen, die Praxis zu verbessern. Die Idee zur Cyber Range entstand vor der Corona-Pandemie, 2020 hätte es losgehen sollen. „Wir hatten zusammen mit Kollegen aus Israel eine vollständige Plattform für die Trainings aufgebaut“, sagt Shulman. „Der Plan war natürlich, das in Präsenz zu machen. Aber am Ende lief alles digital.“ ›

Foto: SIT / Farideh Diehl

Die Forscherin
Haya Shulman, 43, ist Informatikprofessorin an der Goethe-Universität Frankfurt und Gastprofessorin an der Hebräischen Universität Jerusalem. In Darmstadt leitet sie die Abteilung Cybersecurity Analytics and Defences des SIT und das Forschungsgebiet Analytics Based Cybersecurity bei Athene, in Jerusalem das Fraunhofer-Projektzentrum für Cybersicherheit.

Alle sind in Panik, keiner weiß, was tun.

Das SIT
Das Fraunhofer-Institut für Sichere Informationstechnologie (SIT) ging 2001 aus einem Institut der bundeseigenen Großforschungseinrichtung GMD (Gesellschaft für Mathematik und Datenverarbeitung) hervor. In Darmstadt und Birlinghoven forschen rund 240 Beschäftigte zur Sicherheit von IT-Infrastrukturen und zum Datenschutz. Das SIT unterhält Büros in Jerusalem und Singapur. Gemeinsam mit dem Fraunhofer-Institut für Graphische Datenverarbeitung (IGD), der Technischen Universität sowie der Hochschule Darmstadt bildet das SIT das „Nationale Forschungszentrum für angewandte Cybersicherheit Athene“. Es wird gefördert vom Bundesministerium für Bildung und Forschung (BMBF) sowie vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK).

Der frühe Teilnehmer: Patrick Zeitz, Allianz Cyber Defense Center, Unterföhring

Das Cyber-Abwehrzentrum der Allianz ist eine der personell bestausgestatteten Mannschaften ihrer Art. Sie ist international und arbeitsteilig aufgestellt: Das Ressort Threat Intelligence beobachtet vorausschauend Bedrohungslagen, ein anderes Team beschafft und wartet die für die Erkennung von verdächtigen Aktivitäten nötige Technik des „Security Information and Event Management“-Systems (SIEM). Die Sparte Detection kümmert sich um die laufende Überwachung des Datenverkehrs, Forensiker werten Spuren erkannter Angriffe aus.

Das Team hörte schon im Herbst 2020 von den offiziell noch gar nicht angekündigten Trainings, und so findet sich Patrick Zeitz im November des Jahres mit fünf Kollegen aus anderen Bereichen in einem Online-Meeting wieder – er ist stellvertretend für die Detektoren dabei.

Zeitz sitzt vor zwei Bildschirmen: einem für die Telekonferenz via „BigBlueButton“ und einem für das Cockpit des Simulators. Nach einer kurzen Einweisung durch den Moderator gibt ein Kollege, der den Chef spielt, den Blick auf die virtuellen Maschinen der Cyber Range frei. „Es begann mit einer leichten Mission, damit wir uns mit dem Tool vertraut machen konnten“, erinnert Zeitz. Der Markt für Sicherheitssoftware ist so vielfältig, dass das SIT nicht allen Teilnehmern ihre gewohnte IT-Umgebung bieten kann.

Auf Zeitz’ Zweitmonitor erscheinen erste „Indicators of Compromise“ – Anzeichen einer Kompromittierung. „Man sieht etwas Merkwürdiges und muss erkennen, was sich da tut und woran es liegt. Auf unserem Gateway verließen plötzlich sehr große E-Mails das Unternehmen.“ Es läuft eine Exfiltration: Kundendaten werden in Häppchen verpackt und verschlüsselt verschickt. Das Team spricht sich ab und verteilt die Aufgaben: Wie sind die Angreifer reingekommen? Wohin gehen die Nachrichten? Läuft das noch? Wenn ja, was ist besser: Weiter heimlich zuschauen, wie der Hacker arbeitet, oder dichtmachen und ihm so verraten, dass er entdeckt wurde? Und von welcher IP-Adresse kam der Zugriff? „Die Rekonstruktion des Angriffs funktioniert wie in einem Fernsehkrimi“, erklärt Zeitz: Ausgehend von der Tatzeit hangeln sich die Experten an den Logfiles entlang, von Datenspur zu Datenspur, die die Täter hinterlassen haben.

Die Szenarien werden von Mal zu Mal schwieriger. Und nach jedem erfahren die Teilnehmer, was ihnen durch die Lappen gegangen ist. Ein Szenario sei „knüppelhart“ gewesen, sagt Zeitz. „Die sind aber auch so aufgebaut, dass man sie nicht zu hundert Prozent erfüllen kann, damit man immer etwas daraus lernt.“

Am Ende des dreitägigen Seminars hat der Münchner ein beruhigendes Gefühl: Erstens hat sein Blue Team (Fachjargon für Verteidiger) nichts grundlegend Neues gesehen, ist also wissensmäßig auf dem aktuellen Stand. Und zweitens hat die Zusammenarbeit gut funktioniert, obwohl es sich nicht um ein eingespieltes Team handelte, sondern eine Gruppe von Kollegen, mit denen er sonst wenig zu tun hat. Außerdem hat ihm noch etwas gefallen: die „stressarmen Rahmenbedingungen“.

Die Einzelkämpferin: Melina Frowein, stellvertretende Informationssicherheitsbeauftragte, Hessischer Landtag

Nach dem offiziellen Start der Cyber Range im April 2021 spricht sich unter IT-Fachkräften in Hessens öffentlichem Dienst herum, dass das SIT eine neue Art von Trainings anbietet. Die Hessische Zentrale für Datenverarbeitung (HZD) nimmt den Behörden des Landes zwar viel Arbeit ab, aber es gibt auch überall hauseigene IT-Teams. So im Landtag in Wiesbaden: Um den technischen Schutz der rund 800 PCs, die in der Verwaltung und den Abgeordnetenbüros stehen, kümmert sich die junge Informatikerin Melina Frowein derzeit noch als Einzelkämpferin – der Informationssicherheitsbeauftragte, dessen Vize sie ist, betreut den organisatorischen Part.

Im Juni 2021 macht Frowein einen dreitägigen Einführungskurs online, im September nimmt sie an einem Vertiefungsseminar teil, das das SIT als coronakonforme Präsenzveranstaltung abhält. Während sie die erste Runde, ähnlich wie Patrick Zeitz, als eher entspannt beschreibt, kann sie das vom Fortgeschrittenenkurs nicht behaupten.

Natürlich ist der Schwierigkeitsgrad höher und die Teilnehmer müssen mit weniger Informationen klarkommen. Doch damit hat der aufkommende Stress nichts zu tun. Er wird mutwillig erzeugt: „Als wir morgens in den Schulungsraum kommen, ist es total warm. Ja, die Klimaanlage ist ausgefallen. Dann klingeln alle Telefone, ein Alarm geht los, das Licht geht aus. Wir bekommen Presseanfragen: Können Sie uns sagen, was los ist? Später kommt von nebenan Baulärm. Und der Empfang ruft an: Wer hat Pizza bestellt? Ein Teilnehmer wird sogar nach dem Schlüssel seines Autos gefragt, das gleich abgeschleppt würde. Die haben alles mit reingenommen, was geht.“

Das Stresstraining sei dem Feedback eines Trainers zu verdanken, erzählt SIT-Expertin Ranim Chakra, die mit ihrem Team die Trainings plant: „Wir haben mit verschiedenen Faktoren gespielt, damit die Atmosphäre und Umgebung für die Teilnehmer realistischer werden.“ Im Zeitalter von Internettelefonie und Smart Buildings mit computergesteuerter Beleuchtung und Klimatisierung ist es möglich, dass sich ein Hacker auch daran vergreift – falls er bemerkt wird, kann er seine Widersacher so ausbremsen.

„Bei einem Angriff hat man kein Telefon, keine E-Mail und kein Internet, aber ganz viele Handyanrufe vom Management“, erklärt Haya Shulman. „An wen wendet man sich dann? Ans BKA? Ans BSI? Wer ist zuständig? Alle sind in Panik, keiner weiß, was er tun soll. In vielen Organisationen gibt es keinen Plan für den Notfall. Und ein echter Cyberangriff ist kein guter Zeitpunkt, um das zu entdecken. Aber wenn Trainees das hier erleben, erkennen sie, wie schwierig es ist, richtig zu reagieren.“

Nach dem Tag, an dem Ranim Chakra sie buchstäblich ins Schwitzen gebracht hat, fühlt sich Melina Frowein „erst mal etwas geschlaucht“. Doch im Nachhinein lobt sie die IT-Übung: „Das war mal eine ganz andere Erfahrung. Sonst steht bei Schulungen immer jemand vorne und erzählt einem was. Das dagegen war richtig gut gemacht, wie im normalen Leben.“

Der Administrator: Daniel Weyrauch, Sachgebietsleiter in der IT, Hessisches Ministerium für Wissenschaft und Kunst (HMWK)

Kein Ministerium in Hessen ist näher dran an Athene und SIT als das HMWK. Also ist das Haus natürlich auch bei der Cyber Range dabei. Daniel Weyrauch administriert mit seinem kleinen Team ein System, an dem 270 Beamte und Angestellte hängen. Die IT-Sicherheit verantworten Kollegen. „Sonst würde man ja den Bock zum Gärtner machen“, sagt er. „Die technische Umsetzung liegt bei uns. Wir müssen wissen, wie Angreifer denken, um die Konzeption des Netzwerks entsprechend planen zu können.“

Um Hacker daran zu hindern, die IT-Infrastruktur Hessens anzugreifen, muss nicht nur die HZD wachsam sein, sondern auch die daran angeschlossenen Ministerien. Sicherheitstrainings für normale User, die oft eine Schwachstelle bilden, sind Weyrauch sehr wichtig: „Ich würde die Leute einmal im Jahr in eine Schulung schicken, bis es ihnen zu den Ohren rauskommt.“

Wie seine Kollegin vom Landtag absolviert Weyrauch beide Schulungen. Zunächst muss er sich mit dem Netz vertraut machen, das technisch nicht allzu komplex ist. Es gibt wie im HMWK mehrere getrennte Server, die vor allem mit Microsoft-Software laufen, aber nur eine Handvoll Clients. Einige simulierte Bedrohungslagen sind dynamisch, das heißt, der Angriff läuft: „Es wird schlimmer, während man dasitzt und schaut, was passiert. So kommt man unter Zeitdruck.“ Bei der Präsenzschulung im August muss Weyrauch wie Melina Frowein schwitzen und im Dunkeln sitzen, ohne sich aus der Ruhe bringen zu lassen.

Bei der Manöverkritik erfährt er, warum er und sein Team trotz aller Erfahrung und Routine ein paarmal auf der falschen Fährte waren und wie sie schneller zum Ziel gekommen wären. „Ich achte jetzt viel mehr auf Kleinigkeiten“, resümiert er. „Mir ist bewusst geworden, wie viele ungeschützte Systeme es allein dadurch gibt, dass nicht gepatcht wird.“ Auf die Aktualisierung von PCs bei sicherheitsrelevanten Updates hat er nur begrenzt Einfluss – wer alte, funktionierende Systeme ersetzen will, braucht dafür ein Budget. Auch deshalb sind die Geräte des Landes Hessen noch nicht so vereinheitlicht, dass die HZD per Mausklick alles aus der Ferne auf dem neuesten Stand halten könnte. Dass die User von Updates selten begeistert sind, kann Weyrauch nachvollziehen: „Ich habe mehr als einmal erlebt, dass wir einen Patch installieren und auf einmal das System nicht mehr funktioniert.“

Empfehlen würde der IT-Spezialist ein Training auf der Cyber Range nur Kollegen, die technisch ähnlich versiert sind wie er selbst. „Ich bin da mit vielen guten Ideen rausgekommen. Vorher wusste ich grob, wie es funktioniert, aber es ist etwas ganz anderes, wenn man den Angreifer live bei der Arbeit sieht.“ 〉

Der alte Hase: Antonio Jorba, Leiter Cybersecurity der Digitalstadt Darmstadt

„Statistisch sind Elektriker die häufigsten Opfer eines Stromschlags“, antwortet der 59-jährige Diplom-Informatiker Antonio Jorba auf die Frage, warum jemand mit seinem Background einen Kurs auf der Cyber Range besucht. Dem gebürtigen Nürnberger würde jeder sofort glauben, er sei ein Trainer: Er kümmert sich als Teamleiter bei Count + Care, der Abrechnungstochter des Energieversorgers Entega, sowie beim Projekt Digitalstadt Darmstadt um die IT-Sicherheit. Dieses kommunale Prestigeprojekt, mit dem sich die Universitätsstadt als Vorreiterin auf dem Weg zur Smart City positioniert, residiert sogar im SIT-Gebäude – Institutsleiter Michael Waidner ist im Nebenjob als Chief Digital Officer offizieller Vordenker der Digitalstadt.

Ja, er sei auch Dozent, bestätigt Jorba, aber in diesem Fall war er Teilnehmer. So hockt er im Mai 2022 für einen Online-Grundkurs vor dem Rechner, getrieben von einer Mischung aus Prophylaxe gegen Betriebsblindheit und beruflicher Neugier. Später versichert er: „Mich hat die Schulung verblüfft, wachgerüttelt, sensibilisiert. Ich kann noch ganz viel lernen.“

Freilich ging Jorba mit einer weiteren Motivation in den Kurs: „Ich wollte mir ansehen, ob das auch etwas für uns wäre.“ Mit „uns“ meint er nicht nur das vierköpfige Sicherheitsteam, dessen Chef er ist, sondern auch die Hälfte der rund 300 Beschäftigten von Count + Care, die im IT-Umfeld tätig sind.

Der Kurs stellte Jorba zunächst vor niedrige Hürden: „Wir konnten den Command and Control Server ausfindig machen und so den Hacker hacken. Dass Sie in dessen Datenbank den Schlüssel finden, wird Ihnen im echten Leben aber nicht passieren.“ Faszinierend findet Jorba, „dass das echte Trojaner waren, keine für die Cyber Range programmierten“. Einen bleibenden Eindruck hinterlässt auch der „ziemlich clevere“ Verschlüsselungstrojaner am dritten Tag. „Im echten Leben hätten ich und die anderen aus der Gruppe gesagt: Ist doch nix, alles gut. Da war aber nichts in Ordnung. Die heutigen Angriffe täuschen auch ein SIEM.“

Und noch eine Lektion hat Jorba gefallen – ein gezielter Fehlalarm als Ablenkungsmanöver, während an anderer Stelle der eigentliche Angriff beginnt. Sein Fazit lautet daher: „Solche Trainings sind ein Must-have für alle Sicherheitsbeauftragten.“

Zur Nachahmung empfohlen

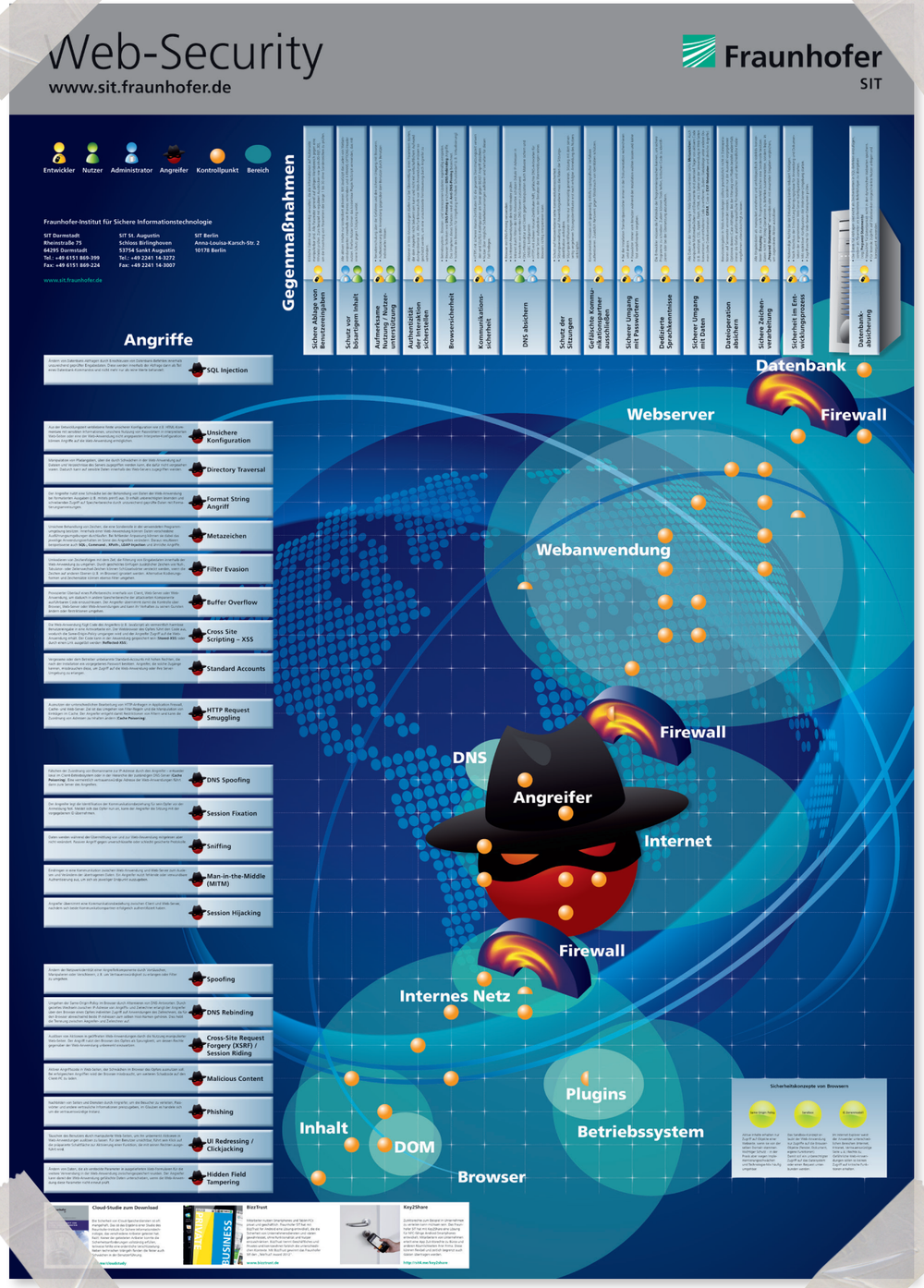
Das freut Haya Shulman natürlich ebenso wie das ihrer Ansicht nach gestiegene Bewusstsein für die Risiken von Cyberangriffen: „Die Awareness ist da. Dass sich durch Übungen die meisten Angriffe verhindern ließen, wissen die Leute aber nicht.“

Deshalb bietet das SIT nicht nur Kurse für IT-Sicherheitsprofis aus der Verwaltung an, sondern auch für deren Kollegen aus der industriellen Fertigung und sogar für nicht technische Kräfte, also normale Nutzer. Die Stress-Simulationen für Abwehr-Kräfte sind allerdings Höhepunkte. „Wir sind die Einzigen, die das in dieser Form machen“, sagt Shulman, „deshalb sind wir gut gebucht.“

Sie sucht bereits neue Mitarbeitende, hat aber nicht vor, die Cyber Range als exklusives Angebot vor Konkurrenz zu schützen. „Unser Ziel ist es, die Sicherheit in deutschen Netzen zu verbessern. Es ist für mich okay, wenn uns das andere nachmachen.“

SIEM
Systeme für das „Security Information and Event Management“ überwachen automatisch alle Datenzugriffe aus dem lokalen Netz und dem Internet. So fallen potenziell sicherheitsrelevante Aktivitäten („Events“) eher auf. Die Datenflut wäre ohne derartige Hilfsmittel, die genau an die Bedürfnisse und die Infrastruktur des Unternehmens angepasst werden können (und müssen), nicht zu bewältigen.

Der Ernstfall: Digitalstadt gehackt
Brandschutzübungen helfen, um im Brandfall richtig zu reagieren – aber sie verhindern keine Brände. Dasselbe gilt für Cybersicherheit: Nach Redaktionsschluss wurde der IT-Dienstleister Count + Care Opfer einer Ransomware-Attacke. In der Folge mussten die Websites mehrerer städtischer Unternehmen (Energieversorger, Stadtreinigung usw.) abgeschaltet werden. Mitarbeitende konnten keine E-Mails mehr senden und empfangen, auch „Digitalstadt Darmstadt“ war offline. Kritische Infrastrukturen waren nicht betroffen, weil sie gesondert geschützt werden, genauso wenig wie das SIT. Weitere Angaben zum Angriff wurden nicht gemacht, um die Ermittlungen nicht zu gefährden. Es ist allerdings nicht unwahrscheinlich, dass ein Mitarbeitender, der noch keine Cybersicherheits-Schulung hatte, auf den Link einer Phishing Mail geklickt hat …



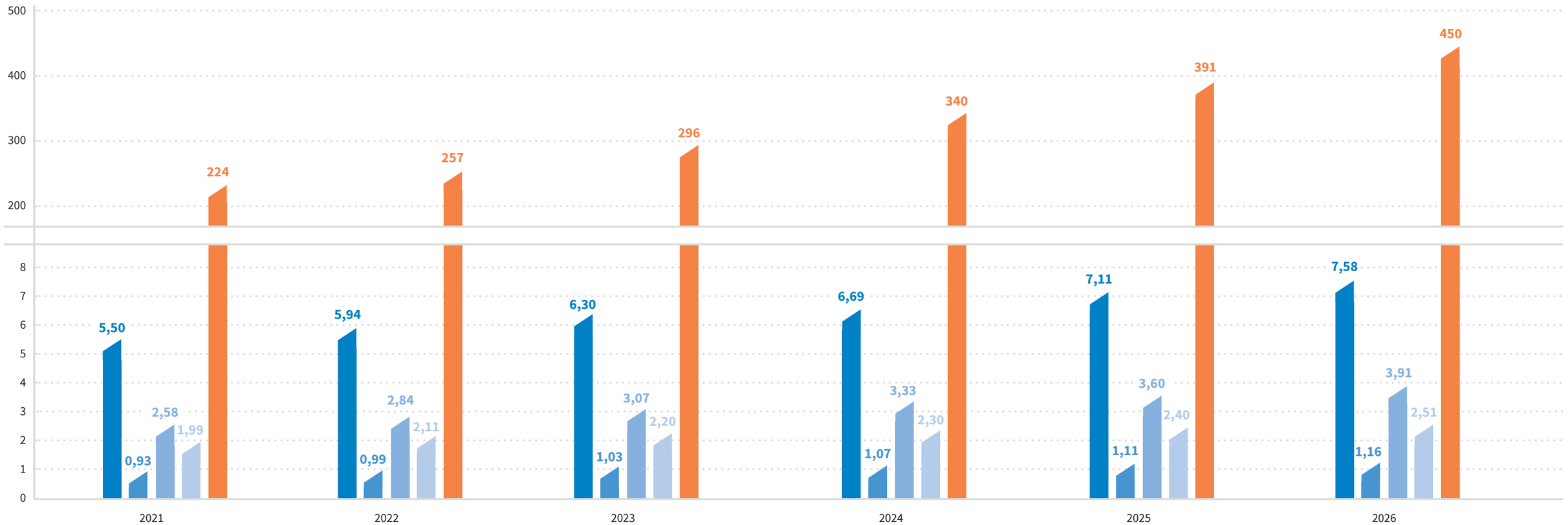
Poster: Fraunhofer SIT

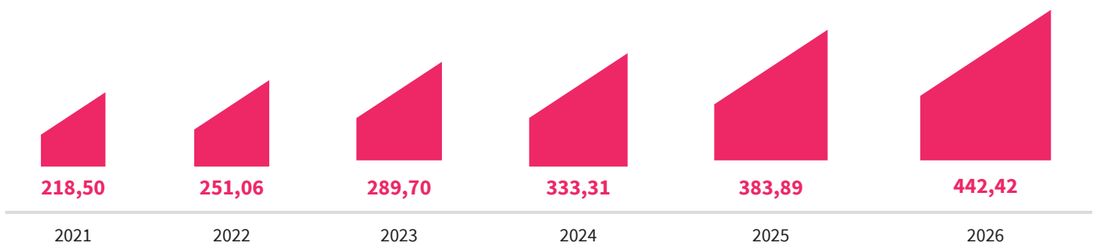
WIR

Auch im Privaten stellt Ransomware derzeit die größte Cybercrime-Bedrohung dar. Wie hoch sind die Fallzahlen? Welche Systeme sind besonders betroffen? Wie gut sind wir geschützt? Wo machen wir es den Angreifern leicht? Wo lauern im Alltag Gefahren? Und bei welchen Schutzmaßnahmen handeln wir stetig wider besseres Wissen?

Kein gutes Verhältnis

Schaden durch Cybercrime im Verhältnis zu Ausgaben für Cybersicherheit; Deutschland; Prognose; in Milliarden Euro





Entwicklung der Differenz zwischen den Ausgaben für Cybersicherheit und Schaden durch Cybercrime, in Milliarden Euro

Quellen: Bitkom, Statista, Embroker, Cybersecurity Ventures

Cyberbegriffe-Übersicht im Glossar auf Seite 100 – 103.

Erbeutet

Schadensdimensionen und Profit von Ransomware; weltweit / Deutschland; 2019 – 2021; in Euro

weltweit Deutschland

2020
148 351

2021
173 074

durchschnittliche Lösegeldforderungen bei Ransomware-Attacken

2019
5,3 Milliarden

2021
24,3 Milliarden

jährlicher Schaden durch Ransomware

2021
509 Milliarden

Profit durch Ransom-Gruppierungen

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Erpresst

Fallbeispiel: Ransomware-Angriff auf die Landkreisverwaltung Anhalt-Bitterfeld; Deutschland; 2021

Der Angriff

Der Ransomware-Angriff erfolgte am 5. Juli 2021 auf Netzwerke der LKV in Köthen, Bitterfeld und Zerbst. Die Systeme wurden vorsorglich heruntergefahren und kommunale Verwaltungsprozesse dadurch erheblich beeinträchtigt.

Die Täter

Die Tätergruppe „Grief“ nutzte Double Extortion und forderte Lösegeld in Form der Kryptowährung Monero. Als Reaktion wurde am 9. Juli 2021 der Katastrophenfall ausgerufen – das ermöglichte eine umfassende Abwehr und Eindämmung.

Die Folgen

Ein halbes Jahr später waren die Systeme noch immer nicht vollständig wiederhergestellt. Die Wiederherstellung wird noch 2022 andauern und etwa zwei Millionen Euro kosten.

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Ransomware war 2021 erneut die primäre, gesamtgesellschaftliche Bedrohung im Bereich des Cybercrime. Das Bedrohungs- und Schadenspotenzial ist nochmals spürbar angestiegen. 2021 war geprägt von Angriffen auf kritische Infrastrukturen, die öffentliche Verwaltung oder internationale Lieferketten. Neben monetären Schäden beeinträchtigen derartige Angriffe auch die Funktionsfähigkeit des Gemeinwesens. Es gibt drei wesentliche Modi Operandi:
Double Extortion: der Standard-Modus-Operandi (Datenverschlüsselung und -veröffentlichung)
Triple Extortion: Zusätzlich zur Datenverschlüsselung und -veröffentlichung erfolgen DDoS-Attacken beim Opfer.
Second-Stage-Extortion: Auch Kundinnen und Kunden der eigentlichen Opfer werden damit erpresst, dass ihre Daten veröffentlicht werden, sollte keine Zahlung erfolgen.

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Erwischt

Fallaufkommen von Cybercrime-Straftaten *; Deutschland

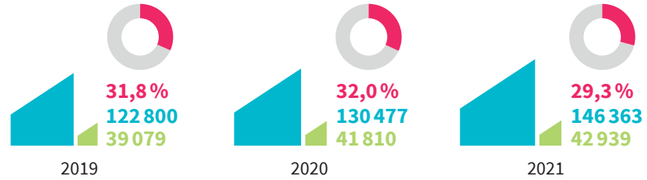
	2020	2021	Veränderung 2020 – 2021
Computerbetrug	105 049	113 002	7,6 %
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung	10 895	13 390	22,9 %
Datenveränderung, Computersabotage	3 770	5 053	34,0 %
Ausspähen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei	10 763	14 918	38,6 %
Cybercrime gesamt	130 477	146 363	12,2 %

* nach Definition des Bundeskriminalamtes. Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Erkannt

Zahl erfasster und aufgeklärter Fälle im Bereich Cybercrime (CC gesamt); Deutschland

erfasste Fälle aufgeklärte Fälle Anteil aufgeklärter Fälle



Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

CC gesamt umfasst alle erfassten Cybercrime-Fälle in Deutschland.

Bei **Cybercrime im engeren Sinne (CCieS)** handelt es sich um Delikte, die sich gegen das Internet und informationstechnische Systeme richten.

Quelle: BSI

Erfasst

Zahl erfasster und aufgeklärter Fälle im Bereich Cybercrime im engeren Sinne (CCieS); Deutschland

	2017	2018	2019	2020	2021
erfasste Fälle	85 960	87 106	100 514	108 474	124 137
aufgeklärte Fälle	34 658	33 862	32 489	35 390	37 124
Anteil aufgeklärter Fälle	40,3 %	38,9 %	32,3 %	32,6 %	29,9 %

Veränderung der erfassten Fällle von 2017 – 2021	44,4 %
Veränderung der aufgeklärten Fällle von 2017 – 2021	7,1 %

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

5. März 2021
Tatbestand: Die Website eines Impfzentrums sowie die Homepage des zugehörigen Landkreises wurden Ziele von DDoS-Attacken. Beide Internetseiten waren für einige Tage nicht erreichbar.
Angriffstyp: DDoS
Quelle: BSI

Im Untergrund

Beschaffungs- bzw. Nutzungskosten krimineller Services; Deutschland; 2021; in Euro

BankingTrojaner (Desktop-Version)	850 – 8 500	bei Kauf
BankingTrojaner (Mobile-Version)	850 – 8 500	bei Kauf
RAT (Remote Administration Tool)	50 – 450	pro Monat bei Miete
RAT (Remote Administration Tool)	ca. 2 500	bei Kauf
Mining Bots	40 – 130	pro Monat bei Miete
Crypting	0 – 85	bei Kauf von einem Crypt
Crypting	25 – 420	bei einem Wochen-Abo mit 50 Crypts pro Tag
DDoS-as-a-Service	70 – 1 270	pro Monat bei Miete
Bulletproof Hosting (Shared)	4 – 40	pro Monat bei Miete
Bulletproof Hosting (Dedicated)	40 – 590	pro Monat bei Miete
Counter-AV-Service	8	pro Monat und 300 Scans
Infection-on-Demand (Phishing-Services o. Ä.)	ab 85	pro Monat
Stealer Logs	4 – 13	pro Stück
Stealer Logs	340 – 760	pro Monat für Abonnement

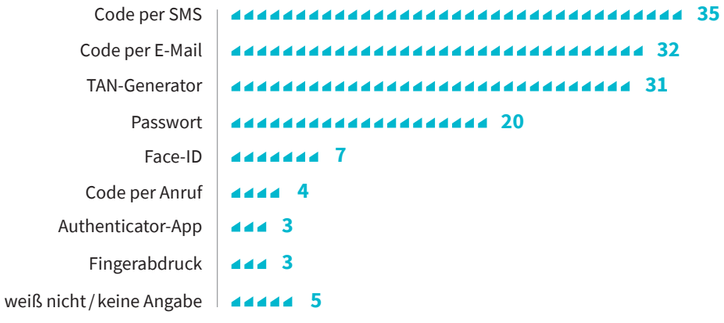
Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Im Kommen?

Verwendung von Zwei-Faktor-Authentifizierung; Internetnutzerinnen und -nutzer; Deutschland; in Prozent *

Nutzen Sie zumindest für einige Ihrer Online-Dienste eine Zwei-Faktor-Authentifizierung?

Welche Anmeldeoptionen nutzen Sie?

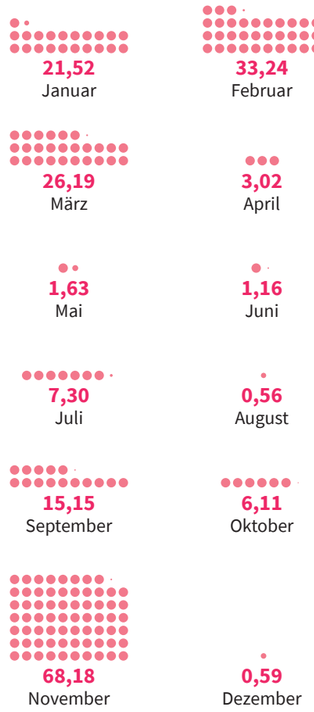


* Mehrfachnennung möglich. Quelle: Bitkom e. V.

8. Mai 2021
Tatbestand: Es kam zu einem Ransomware-Angriff auf die US-Firma Colonial Pipeline. Aufgrund des Angriffs musste eine der größten Ölpipelines der USA vom Netz genommen werden. Es kam zu Versorgungsengpässen und Lieferausfällen. Das FBI ordnete den Angriff der Ransomware bzw. Gruppierung DarkSide (CarbonSpider) zu.
Angriffstyp: Ransomware
Quelle: BSI

Im Verlauf

Zahl kompromittierter Nutzerkonten nach Monat; Deutschland; 2021; in Millionen



Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Im Gegenzug

Abwehr-Indizes 2021 des Bundesamtes für Sicherheit in der Informationstechnik; Deutschland; 2021

	neue Website-Sperrungen	abgewehrte Schadprogramm-Angriffe auf die Bundesverwaltung
Januar	102	48
Februar	91	42
März	159	135
April	135	45
Mai	128	50
Juni	97	54
Juli	128	45
August	163	49
September	95	57
Oktober	136	57
November	144	103
Dezember	138	50

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

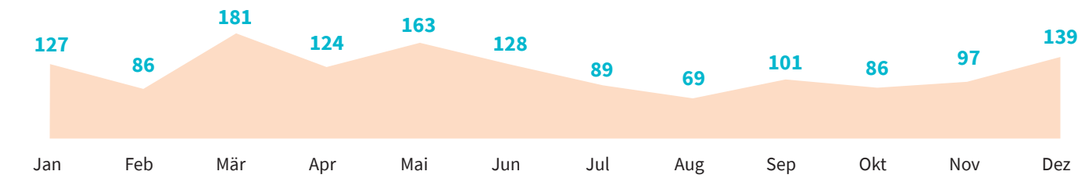
Abwehr-Indizes messen das Aufkommen und die Entwicklung von Malware-Angriffen per E-Mail auf die Netze des Bundes sowie die Menge präventiver Sperrungen von maliziösen Webseiten.

Der **Spam-Mail-Index** ist ein Maß für die in den Netzen des Bundes festgestellte Zahl der Spam-Mails.

Quelle: BSI

Im Überblick

Spam-Mail-Index 2021 des Bundesamtes für Sicherheit in der Informationstechnik; Deutschland; 2021



Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Attackiert
Fallbeispiel: DDoS-Angriff auf Server der Universität Mainz; Deutschland; 2021

Der DDoS-Angriff
Im Januar 2021 kam es zu mehreren DDoS-Angriffen auf Systeme der Universität Mainz. Ziel der Attacken waren Server, die die Universität im Zuge der pandemischen Lage dem Bildungsministerium zur Durchführung des Fernunterrichts an rheinland-pfälzischen Schulen zur Verfügung gestellt hatte. Ein erster Angriff begann am 4. Januar, dem ersten Schultag nach den Weihnachtsferien, und setzte sich bis zum Morgen des folgenden Tages fort. Ein weiterer davon unabhängiger Angriff erfolgte ab dem 19. Januar und hielt bis zum 21. Januar an. Ausgehend von elf Servern wurden während des zweiten DDoS-Angriffs 13 Millionen HTTP-Anfragen ausgeführt.

Die Auswirkungen
Auf dem Höhepunkt der DDoS-Attacke gingen 500 000 Anfragen pro Sekunde bei den angegriffenen Servern ein. Dadurch entstanden Schwierigkeiten bei der Erreichbarkeit der Lernplattform moodle@RLP, auf der Lernmaterialen für Schülerinnen und Schüler zur Verfügung gestellt wurden, und des Web-Konferenzsystems BigBlueButton. Von den Einschränkungen waren rund 900 Schulen in Rheinland-Pfalz betroffen.

Die Ermittlungen
Der Vorfall fand ein großes Medienecho und wurde mit Bezug auf die Notwendigkeit der Digitalisierung des Bildungssystems im Landtagswahlkampf 2021 aufgegriffen. Die Landeszentralstelle Cybercrime der Generalstaatsanwaltschaft Koblenz und das Dezernat Cybercrime des Landeskriminalamtes Rheinland-Pfalz nahmen Ermittlungen in diesem Fall auf. Für den zweiten Angriff konnte im Verlauf dieser Ermittlungen ein 14-jähriger Schüler als Tatverdächtiger identifiziert werden.

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Lahmgelegt
DDoS in Zahlen; Deutschland; 2021

2 335
durchschnittliche Zahl der Angriffe pro Monat

796,80 Mbps
durchschnittliche Bandbreite

1,5 Stunden
durchschnittliche Dauer eines Angriffs

41 %
Zuwachs der Angriffe verglichen mit 2020

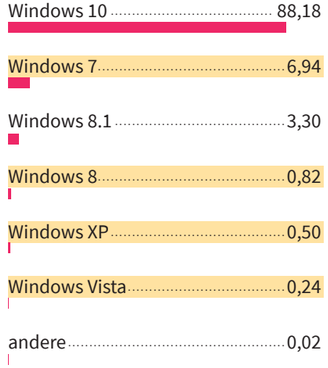
82 Tage
längste Angriffsdauer

3,04 Gbps
durchschnittlicher Bandbreitenpeak

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

14. Juni 2021
Tatbestand: Ein deutscher IT-Dienstleister für Banken wurde Ziel anhaltender DDoS-Angriffe. Teilweise waren Websites, Online-Banking und weitere Services nicht erreichbar oder nur eingeschränkt möglich.
Angriffstyp: DDoS
Quelle: BSI

Windows
Marktanteile der verschiedenen Windows-Versionen; Deutschland; 2021; in Prozent



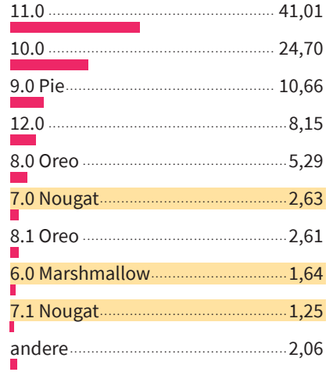
Quelle: Statcounter

Windows hat den Support von Windows 7 zum 14. Januar 2020 eingestellt. Davor wurden bereits der Support für Windows XP (am 8. April 2014) und der Support für Windows Vista (2017) eingestellt. Das bedeutet, dass etwa **7,7 % der Windows-PCs in Deutschland im Jahr 2021 nicht geschützt** waren.

Android ist das Google-Betriebssystem für Smartphones. Aktuelle Android-Versionen erhalten regelmäßige Updates. Eine Untersuchung aus England hat ergeben, dass die **Verwendung von Android-Versionen älter als 8.0 ein Sicherheitsrisiko** darstellt.

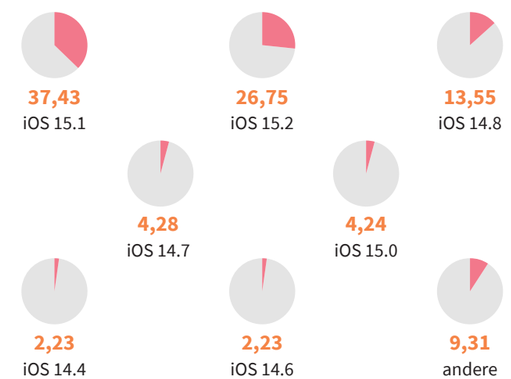
Quelle: Statcounter

Android
Verteilung der verschiedenen Android-Versionen (Mobile & Tablet); Deutschland; Januar 2022; in Prozent



Quelle: Statcounter

iOS
Verteilung der verschiedenen iOS-Versionen * (Mobile & Tablet); Deutschland; Januar 2022; in Prozent



* iOS ist das Betriebssystem für iPhones. Quelle: Statcounter

Programmiert
Schad-Apps für Android-Geräte; weltweit; 2021

mehr als **2,5** Millionen
Zahl der Schad-Apps für Android-Geräte

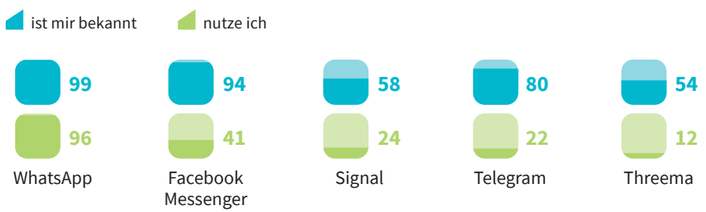
5 Zahl der pro Minute entwickelten schadhaften Android-Apps

Quelle: G DATA

2. Juli 2021
Tatbestand: Der amerikanische IT-Dienstleister Kaseya Ltd. gab einen Ransomware-Angriff auf eine von ihm angebotene Remote-Lösung bekannt. In der Folge kam es zu einem Supply-Chain-Angriff – das Unternehmen wurde als Distributor für die Ransomware REvil missbraucht. Über mehrere IT-Systemhäuser gelangte sie anschließend an eine Vielzahl Endkundinnen und Endkunden.
Angriffstyp: Ransomware
Quelle: BSI

Unterschiedlich

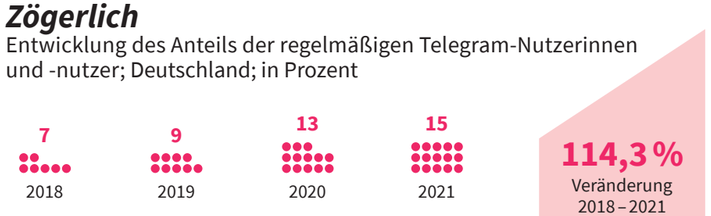
Nutzung und Kenntnis von verschiedenen Messenger-Apps für das Smartphone; Deutschland; 2021; in Prozent *



* Mehrfachnennung möglich. Quelle: Ad Allliance

Zögerlich

Entwicklung des Anteils der regelmäßigen Telegram-Nutzerinnen und -nutzer; Deutschland; in Prozent



Quelle: Statista

Sprachlich

Nutzungsanteile von Online-Kommunikationsdiensten; Deutschland; 2021; in Prozent *

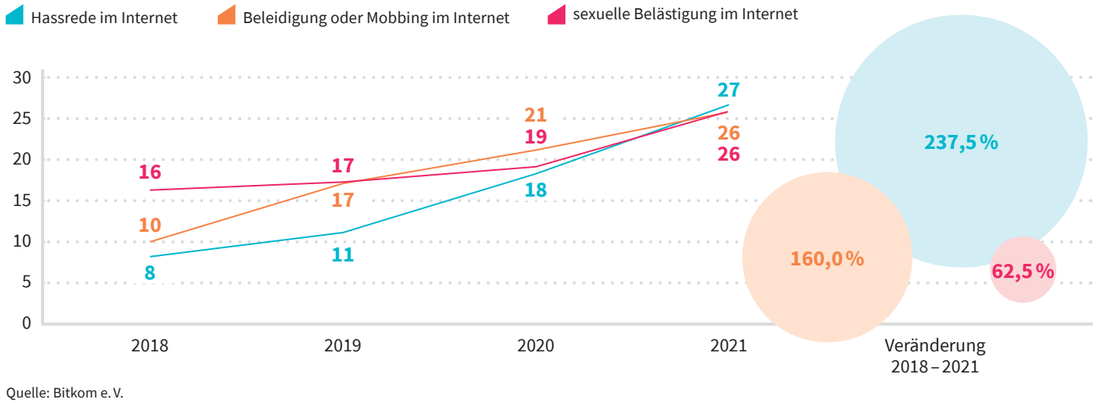
Ende zu Ende Verschlüsselung:
ja · zum Teil · nein

WhatsApp	93
Facebook Messenger	39
Instagram Direct Messages	25
Skype (for Business)	20
Zoom	18
Telegram	16
Microsoft Teams	14
Snapchat	14
Signal	13
Facetime	12
iMessage	10
Discord	8
Google Messages	7
Threema	5
Cisco WebEx	4

* Mehrfachnennung möglich.
Quellen: Bundesnetzagentur, tom's guide

Grässlich

Gefühlte Bedrohung durch Hatespeech und Belästigung; Internet-Nutzerinnen und -Nutzer; Deutschland; in Prozent

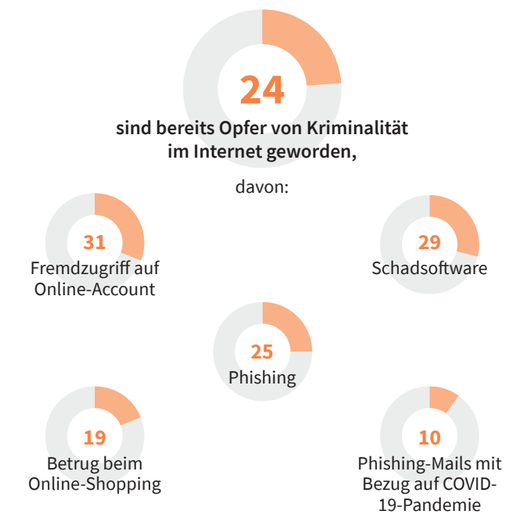


Quelle: Bitkom e. V.

5. Juli 2021
Tatbestand: Nach einem Ransomware-Angriff auf die Landkreisverwaltung Anhalt-Bitterfeld wurde erstmals der Cyber-Katastrophenfall in Deutschland festgestellt. Die Bereitstellung öffentlicher Dienstleistungen war nachhaltig eingeschränkt. Zwar war zwei Wochen nach dem Angrif eine Notinfrastruktur einsatzbereit. Allerdings war auch Monate nach dem Angriff noch kein normaler Regelbetrieb möglich.
Angriffstyp: Ransomware
Quelle: BSI

Bedauerlich

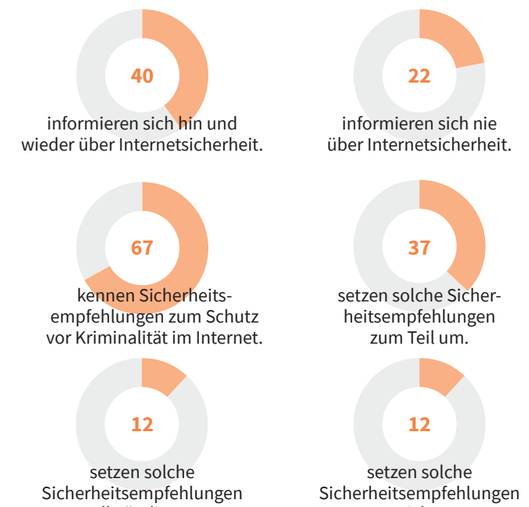
Opfer von Internetkriminalität: Art der Vorfälle; Deutschland; 2021; in Prozent



Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Sträflich

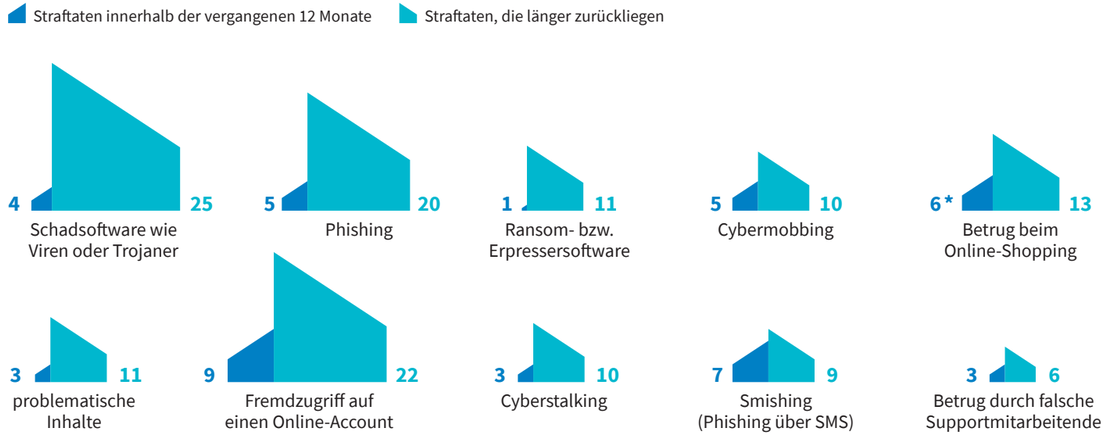
Umgang mit Sicherheitsempfehlungen zum Schutz vor Kriminalität im Internet; Deutschland; 2021; in Prozent



Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Zeitlich

Opfer von Internetkriminalität nach Art der Straftat; Befragte, die Opfer von Internetkriminalität geworden sind; Deutschland; 2021; in Prozent



* Kleine Fallzahl (insgesamt 94 Opfer beim Online-Shopping).
Quellen: Bundesamt für Sicherheit in der Informationstechnik (BSI) und Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK)

Kontinuierlich

Entwicklung der Zahl neuer Schadprogramm-Varianten; Deutschland; 2020 – 2021; in Millionen

06 / 2020	07 / 2020	08 / 2020	09 / 2020	10 / 2020	11 / 2020	12 / 2020	01 / 2021	02 / 2021	03 / 2021	04 / 2021	05 / 2021
7,6	9,4	11,1	11,1	6,4	9,5	12,6	14,5	15,5	17,0	15,2	13,9

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Gegensätzlich

Die häufigsten und seltensten IT-Sicherheitsvorfälle; Deutschland; in Prozent

2020 2021 Veränderung 2020 – 2021

die häufigsten IT-Sicherheitsvorfälle

Phishing-Versuch	Erhalt infizierter E-Mails / Anhänge / Weblinks	Betrug beim Online-Einkauf / bei Online-Buchungen	Mobbing / Belästigungen / Rufschädigung	Betrug beim Bezahlen im Internet (Zahlungsvorgang)	Ausspähen von Zugangsdaten zu Online-Plattformen
10,1 %	– 8,6 %	6,5 %	– 1,1 %	k.A.	+ 9,4 %
28,8	23,2	10,7	9,2	9,7	9,6
31,7	21,2	11,4	9,1	k.A.	8,7

die seltensten IT-Sicherheitsvorfälle

Betrug mit virtuellen Währungen (z. B. Bitcoin)	unbefugter Zugriff auf verlorenes oder gestohlenes Gerät	Vorfälle bei der Nutzung von Online-Angeboten der öffentlichen Hand	Manipulation von Hausvernetzung (Smart Home, z. B. Smart-TV)
– 23,0 %	– 31,3 %	– 21,5 %	– 31,1 %
7,4	6,7	6,5	6,1
5,7	4,6	5,1	4,2

Quelle: Deutschland sicher im Netz (DsiN)

Jugendlich

Nutzung von Cloud im Internet nach Altersgruppen; Deutschland; 2021 ; in Prozent

insgesamt	52,8
16 bis unter 25 Jahre	68,2
25 bis unter 45 Jahre	62,7
45 bis unter 65 Jahre	48,7
65 bis unter 75 Jahre	29,7

Quelle: Statistisches Bundesamt

Kürzlich

Nutzung von Cloud-Diensten; Online-Nutzerinnen und -Nutzer zwischen 18 und 64 Jahren; Deutschland; 2021 ; in Prozent *

Welche der folgenden Services haben Sie in den vergangenen 12 Monaten genutzt?

Online-Speicherung von Dateien und Bildern	38
Online-Anwendung zum Erstellen von Office-Dateien	28
Online-Back-up für Computer oder Smartphones	28
keine der obigen Möglichkeiten	40

* Mehrfachnennung möglich. Quelle: Statista

August 2021
Tatbestand: In einem Hacker-Forum wurde eine Datenbank mit Daten von angeblich 30 Millionen Nutzerinnen und Nutzern eines US-amerikanischen Mobilfunkanbieters angeboten. Der geforderte Preis belief sich auf 6 Bitcoin, damals etwa 240 000 Euro. Der Anbieter gab an, dass die Daten aus einem Angriff auf den Mobilfunkanbieter stammten.
Angriffstyp: Data-Leak
Quelle: BSI

Erheblich

Zahl der neu entdeckten Malware-Samples; Deutschland, Österreich, Schweiz; in Millionen

64 931
Bedrohungen pro Tag

45
Bedrohungen pro Minute

Quelle: G DATA

Bedenklich

Die Top 10 Malware: die häufigsten Angriffe; Deutschland, Österreich, Schweiz; 2021; in Prozent

Dridex (Information Stealer)	26,3
Emotet (Malware Distributor)	14,1
Tofsee (Bot)	11,0
Bodelph (Backdoor)	6,3
Trickbot (Malware Distributor)	6,0
Bladabindi (Remote Access Trojaner)	5,1
Shade (Ransomware)	5,1
BlackShades (Remote Access Trojaner)	5,0
AgentTesla (Information Stealer)	4,6
Pistolar (Dropper)	4,3

Quelle: G DATA

Ein **Information Stealer** ist ein Trojaner, der dazu designt ist, Informationen zu stehlen. Im Vordergrund stehen hier insbesondere Login-Daten.

Emotet war nur im Januar, November und Dezember 2021 aktiv.

Ein **Bot** ist ein Computerprogramm, das Aufgaben automatisiert abarbeitet.

Remote Access Trojaner sind Programme, die eine verdeckte Überwachung oder den unberechtigten Zugriff auf einen infizierten PC ermöglichen.

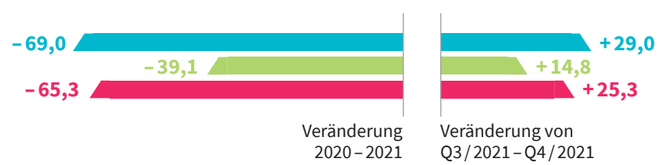
Primäre Funktionalität eines **Downloaders** ist das Herunterladen von Inhalten wie Konfigurations- oder Befehlsinformationen, verschiedene Dateien, andere Malware, irreführende Apps, sekundäre Komponenten des bestehenden Angriffs oder Upgrades für diesen.

Quelle: G DATA

Bedrohlich

Abgewehrte Cyberangriffe nach Zielgruppe im Quartalsvergleich und im Jahresvergleich; Deutschland, Österreich, Schweiz; in Prozent

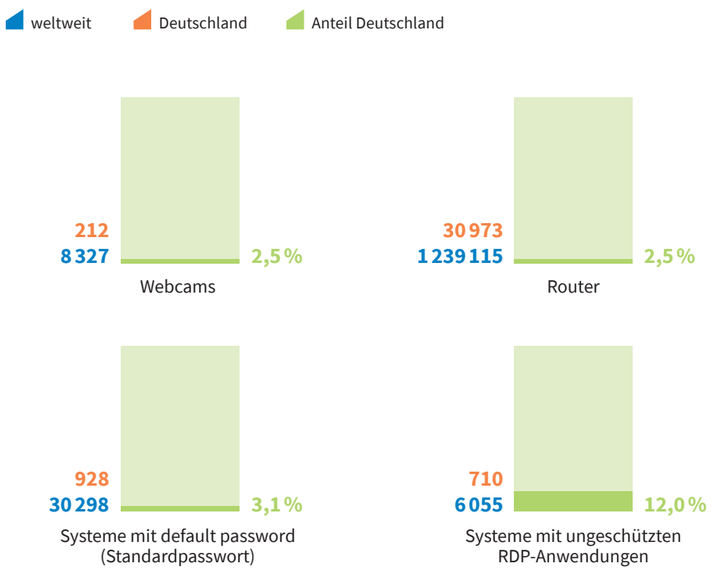
Consumer Business gesamt



Quelle: G DATA

Verletzlich

Zahl der über das Internet auffindbaren Geräte, Anwendungen oder Systeme; 2022 *; in Prozent



Shodan.io ist eine Suchmaschine, die ungeschützte Anwendungen oder Systeme (d. h. „Internet-connected devices“) mit nur geringen Sicherheitsvorkehrungen im Internet findet.

Geräte, Anwendungen oder Systeme, die über Shodan gefunden werden, bieten leichte Ziele für missbräuchliche Angriffe aus dem Bereich Cybercrime.

Quelle: Shodan.io

* Abgerufen am 18. Februar 2022. Quelle: Shodan.io

Öffentlich

Zahl der über das Internet auffindbaren Betriebssysteme; 2022 *; in Prozent

auffindbare Computer …	weltweit	Deutschland	Anteil Deutschland
… mit Windows 10	1 706 391	131 280	7,7 %
… mit Windows 8.1	1 037 927	38 468	3,7 %
… mit Windows 7	277 009	34 051	12,3 %
… mit Windows 8	45 082	1 905	4,2 %
… mit Windows 11	18 884	1 058	5,6 %
… mit Windows XP	1 465	12	0,8 %

* Abgerufen am 18. Februar 2022. Quelle: Shodan.io

30. September 2021
Tatbestand: Es wurde ein Cybersicherheitsvorfall von einem städtischen Klinikum in Sachsen-Anhalt gemeldet. Im Netzwerk des Klinikums wurde das unrechtmäßig eingesetzte Penetration-Testing-Tool Cobalt Strike entdeckt. Die Kommunikationssysteme sowie die Nutzung der IT waren nur eingeschränkt möglich. Zudem wurden täterseitig Daten ausgeleitet. Die medizinische Versorgung konnte durchgehend gewährleistet werden.
Angriffstyp: Malware
Quelle: BSI

Bekanntlich

Verbrauchersicht: Bekanntheitsgrad von Sicherheitsmaßnahmen; Internetnutzende über 16 Jahre; Deutschland; 2021; in Prozent *

die bekanntesten Sicherheitsmaßnahmen	
Schutz des Handys mit PIN o. Ä.	98,3
Sicherung der drahtlosen (Funk-) Netzwerkverbindung (WLAN) durch ein Passwort	98,2
Verwendung von Sonderzeichen in Passwörtern	98,2
regelmäßige Installation von Updates	98,0
Verwendung von langen Passwörtern (mind. 12 Zeichen)	97,9
die unbekanntesten Sicherheitsmaßnahmen	
Plug-ins zur Erhöhung der Datensicherheit (z. B. Skript-Blocker etc.)	82,9
Auslesen der E-Mail-Header	82,5
Inkognito-Funktion	81,7
Nutzung von VPN oder Proxy-Clients	81,3

* Mehrfachnennung möglich. Quelle: Deutschland sicher im Netz (DsiN)

Nützlich

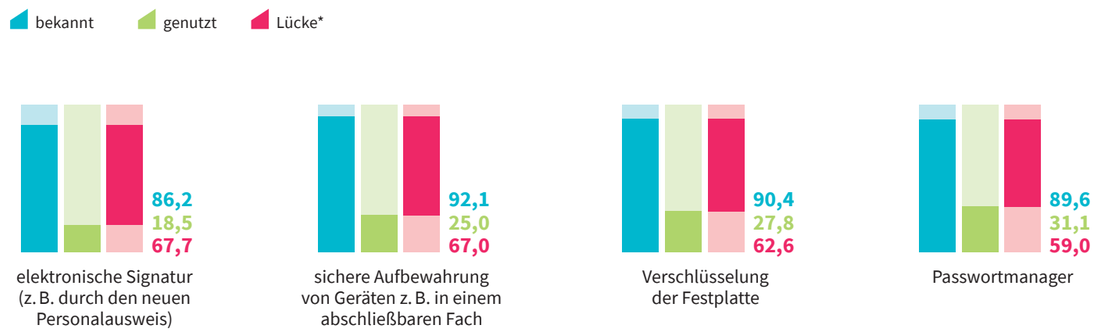
Verbrauchersicht: Meistgenutzte und am wenigsten genutzte Sicherheitsmaßnahmen; Internetnutzende über 16 Jahre; Deutschland; 2021; in Prozent *

die meistgenutzten Sicherheitsmaßnahmen	
Verwendung von Sonderzeichen in Passwörtern	80,1
Nutzung sicherer Zahlungssysteme	77,9
Schutz des Handys mit z. B. PIN	76,9
Verwendung unterschiedlicher Passwörter für unterschiedliche Zwecke	76,4
regelmäßiges Update des Betriebssystems	75,0
die am wenigsten genutzten Sicherheitsmaßnahmen	
Auslesen der E-Mail-Header	26,6
sichere Aufbewahrung der Geräte (z. B. in einem abschließbaren Fach)	25,0
Einsatz elektronischer Signaturen (z. B. durch den neuen Personalausweis)	18,5

* Mehrfachnennung möglich. Quelle: Deutschland sicher im Netz (DsiN)

Schmählich

Die größten Diskrepanzen zwischen Kenntnis und Nutzung bei Sicherheitsmaßnahmen; Internetnutzende über 16 Jahre; Deutschland; 2021; in Prozent *

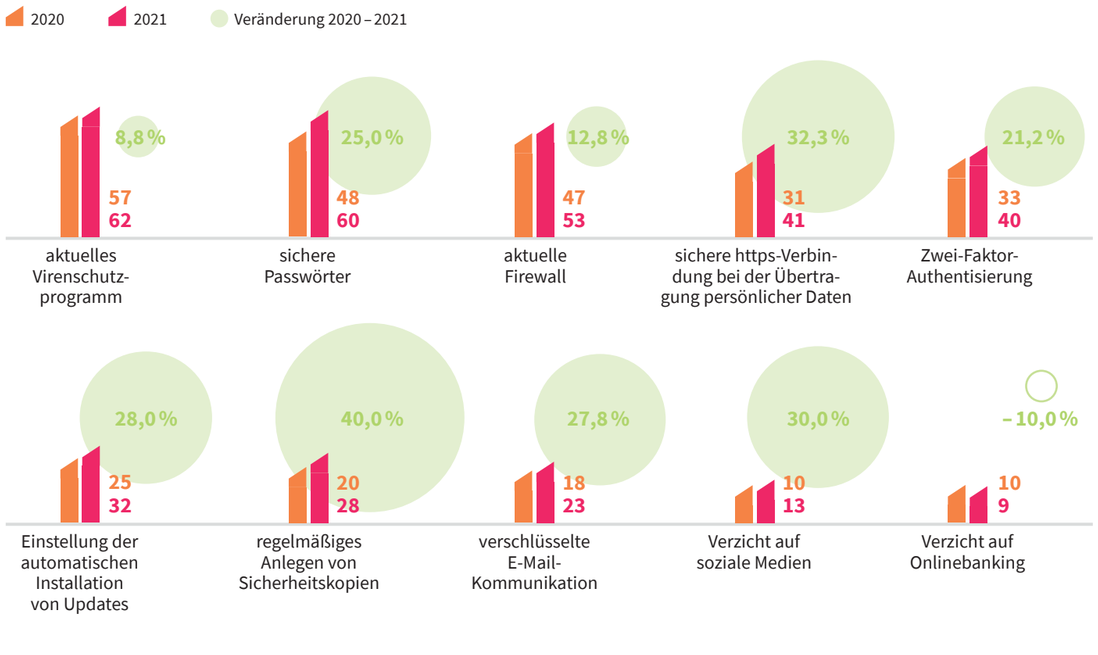


* Mehrfachnennung möglich. Quelle: Deutschland sicher im Netz (DsiN)

4. Oktober 2021
Tatbestand: Ein Softwareunternehmen, dessen Softwarelösungen in etwa einem Viertel der deutschen Arztpraxen eingesetzt werden, stellte die Verschlüsselung ihrer Server- und Netzwerkinfrastruktur fest und war ab diesem Zeitpunkt nicht mehr arbeitsfähig. Bei der eingesetzten Ransomware handelte es sich um Conti.
Angriffstyp: Ransomware
Quelle: BSI

Vorsorglich

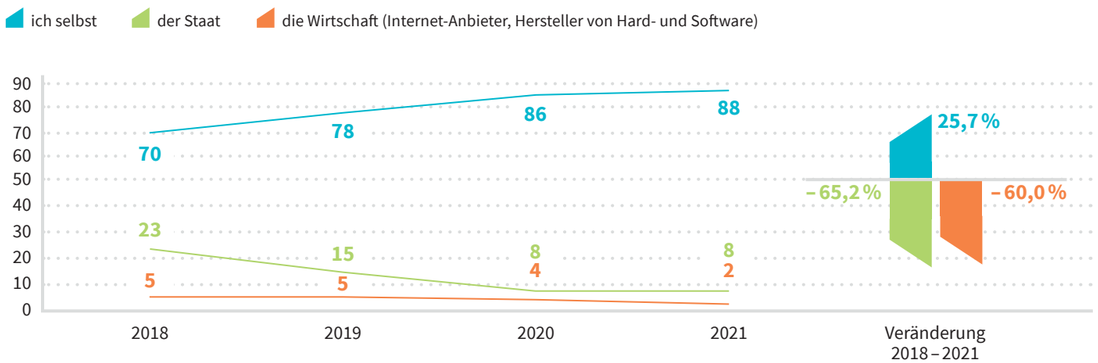
Verwendete Schutzmaßnahmen im Internet; deutschsprachige Bevölkerung im Alter von 14 bis 69 Jahren, die in einem Privathaushalt lebt und über einen Internetzugang verfügt; Deutschland; in Prozent *



* Mehrfachnennung möglich. Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI) und Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK)

Verantwortlich

Selbst- und Fremdverantwortung beim Thema Datenschutz; Internetnutzende; Deutschland; in Prozent



Quelle: Bitkom e. V.

Zugänglich

Verbrauchersicht: Verbesserungsvorschläge für das Sicherheitswissen; Internetnutzende über 16 Jahre; Deutschland; 2021; in Prozent *

Wie könnte Ihr Sicherheitswissen verbessert werden?

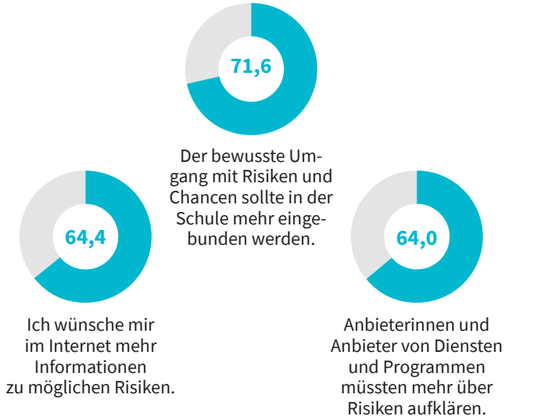
Die Informationen darüber, wie man sich im Internet besser schützen kann, müssten verständlicher sein.	62,7
Die Informationen darüber, wie man sich im Internet besser schützen kann, müssten stärker gebündelt werden (z. B. auf einer zentralen Website).	60,8
Es müsste mehr Aufklärungsangebote in beruflicher oder schulischer Aus- und Weiterbildung geben.	59,8
Ich wünsche mir im Internet mehr Informationen zu möglichen Risiken.	57,6
Es müsste mehr professionelle Ansprechpartner geben, die persönliche Hilfestellung bieten.	51,9

* Mehrfachnennung möglich. Quelle: Deutschland sicher im Netz (DsiN)

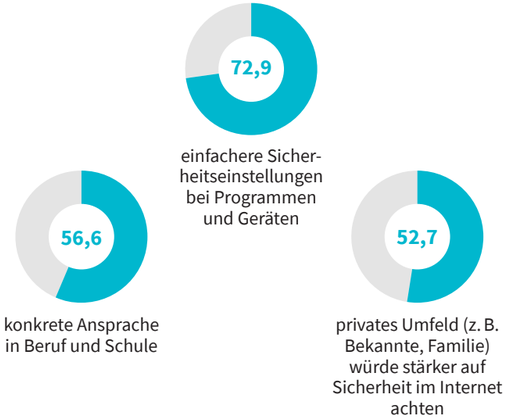
Inhaltlich

Vorschläge zur Stärkung des Risiko- und Sicherheitsbewusstseins; Internetnutzende über 16 Jahre; Deutschland; 2021; in Prozent *

Wie könnte das Risikobewusstsein gestärkt werden?



Was würde Sie zu einem sichereren Umgang mit Ihren Daten im Internet motivieren?



* Mehrfachnennung möglich. Quelle: Deutschland sicher im Netz (DsiN)

9. Dezember 2021
Tatbestand: Es wurde eine Zero-Day-Schwachstelle in der weitverbreiteten Protokollierungsbibliothek Log4j bekannt, die Bestandteil zahlreicher Open-Source- sowie kommerzieller Softwareprodukte ist. Die Schwachstelle ermöglicht die Installation von Schadsoftware und führt so zur Verwundbarkeit zahlreicher Unternehmen. Die langfristigen Folgen sind noch nicht absehbar.
Angriffstyp: Exploit / Schwachstelle
Quelle: BSI

GLOSSAR

Backdoor: Eine Backdoor ist ein üblicherweise durch Viren, Würmer oder Trojanische Pferde installiertes Programm, das Dritten einen unbefugten Zugang („Hintertür“) zum Computer verschafft, jedoch versteckt und unter Umgehung der üblichen Sicherheitseinrichtungen. Backdoors werden oft für Denial-of-Service-Angriffe benutzt.

Back-up: Ein Back-up ist eine Sicherung der Daten zum Schutz vor Datenverlust. Es werden dabei Kopien von vorhandenen Datenbeständen erstellt.

Bot: Der Begriff Bot ist vom englischen Begriff „robot“ (dt. Roboter) abgeleitet. Bots sind Computerprogramme, die nach ihrer Aktivierung ohne menschliches Zutun automatisiert im Internet agieren. Einen Zusammenschluss von Bots zu einem Kommunikationsverbund bezeichnet man als Botnetz.

Brute-Force-Angriff: Wählen Nutzer ein schwaches Passwort und ist der Benutzername (etwa die E-Mail-Adresse) bekannt, kann sich ein Angreifer unter Umständen auch durch wiederholtes Ausprobieren von Passwörtern (Brute-Force-Angriff) Zugang zu einem Benutzerkonto verschaffen. Mittels Brute-Force-Techniken kann der Angreifer zudem versuchen, kryptografisch geschützte Daten, zum Beispiel eine verschlüsselte Passwort-Datei, zu entschlüsseln.

Cache: Pufferspeicher, der Daten schneller zur Bearbeitung bereitstellt. Zum Beispiel: ein lokales Verzeichnis für beim Surfen im Internet besuchte Seiten, die so nicht neuerlich geladen werden müssen.

Cloaking: eine Methode zur Manipulation von Suchmaschinen. Dabei wird dem Robot eine Webseite als Ergebnis unterschoben, auf die die konkreten Suchbegriffe passen, die dem Suchenden jedoch nicht angezeigt wird. Sobald er auf den Link klickt, wird er automatisch auf eine andere Webseite umgeleitet.

Cloud / Cloud Computing: Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die im Rahmen von Cloud Computing angebotenen Dienstleistungen umfassen das komplette Spektrum der Informationstechnik und beinhalten Infrastrukturen (Rechenleistung, Speicherplatz), Plattformen und Software.

Cloudnative Technologien: Anwendungen, die speziell für das Cloud Computing entwickelt wurden.

Computer-Virus: Ein Computer-Virus ist eine nicht selbstständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an Programmen oder deren Umgebung vornimmt. (Zudem 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 es unter anderem, 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.

Cyberaktivisten: Angreifer, die durch einen Cyberangriff auf einen politischen, gesellschaftlichen, sozialen, wirtschaftlichen oder technischen Missstand aufmerksam machen oder eine diesbezügliche Forderung durchsetzen wollen („Hacktivismus“). Die Motivation hinter dem Angriff ist Einflussnahme. Der durch einen Cyberangriff entstandene Schaden wird in Kauf genommen bzw. forciert, um eine höhere Aufmerksamkeit zu erlangen. „Ethische Hacker“ begründen ihr Handeln mit gesellschaftlichen oder sozialen Themen.

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

Cyberkriminelle: Cyberkriminelle versuchen, mithilfe der Informationstechnik auf illegalen Wegen Geld zu verdienen. Die Bandbreite reicht von organisierter Cyberkriminalität bis hin zu einfacher Kriminalität mit geringen Schäden.
Organisierte Cyberkriminalität ist hochprofessionell und umfasst Identitätsdiebstahl mit Warenbetrug, Diebstahl von Geld durch Missbrauch von Bankdaten bis hin zur Erpressung. Dagegen sind einfache Cyberkriminelle meist Einzelpersonen oder kleine Gruppen, die sich durch geringere Professionalität auszeichnen. Von ihnen verursachte Schäden sind typischerweise geringer.

Cybersicherheit: Cybersicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld gilt für den gesamten Cyberraum – also für jede mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik sowie die darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeiteten Informationen.

Cyberterroristen: Terroristen können Cyberangriffe nutzen, um unterschiedliche Ziele anzugreifen, ihre Ideologie zu verbreiten und ihren Einfluss auszuweiten.

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. Es geschieht insbesondere in Beziehungen, zwischen aktuellen oder ehemaligen Partnern.

Data Miner: Programm zum Sammeln, Herausfiltern und Übermitteln von Informationen aus internen Unternehmensdatenbanken und externen Informationsquellen. In den gewonnenen Daten sucht der Data Miner nach Mustern und Zusammenhängen und gewinnt so neue Informationen. Auftraggeber sind Unternehmen, die die Daten zur Analyse und Vorhersage von Verhaltensweisen und Trends und als Entscheidungshilfe nutzen.

Datenleak: Bei einem Datenleak (leak = undichte Stelle) geraten Daten in falsche Hände. Cyberkriminelle können gezielt über eine kompromittierte Webseite an Daten kommen oder über eine Panne, wenn ein Unternehmen sensible Daten ungeschützt aufbewahrt. Oft werden die Daten dann auch veröffentlicht.

Datenschutz: Datenschutz soll den Einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Mit Datenschutz wird daher der Schutz personenbezogener Daten vor etwaigem Missbrauch durch Dritte bezeichnet (nicht zu verwechseln mit Datensicherheit).

Datensicherheit: Mit Datensicherheit wird der Schutz von Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität bezeichnet. Ein modernerer Begriff dafür ist Informationssicherheit.

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

Default password: Wenn ein Gerät zum Anmelden einen Benutzernamen und / oder ein Kennwort benötigt, wird normalerweise ein Standardkennwort bereitgestellt, mit dem auf das Gerät zugegriffen werden kann. Bleibt das ab Werk eingerichtete Standardpasswort unverändert, ist die Angriffsfläche groß.

DevSecOps ist ein Kunstwort, das sich aus jeweils drei Buchstaben der drei Begriffe Development, Security und Operations zusammensetzt. „Dev“ steht für Entwicklung, „Sec“ für Sicherheit und „Ops“ für Betrieb. Es handelt sich um ein Konzept, das den DevOps-Gedanken um die Aspekte der Software-Sicherheit erweitert.

Distributed Ledger Technology ist eine Technologie zur dezentralen Speicherung von Transaktionsdaten.

DOS / DDoS-Angriffe: Denial-of-Service (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.

E-Administration: Sammelbegriff für elektronische Dienstleistungen, die im Rahmen der öffentlichen Verwaltung eingesetzt werden. Häufiger verwendet wird der Begriff E-Government.

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

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 können mithilfe eines Exploits zum Beispiel 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 und dem externen Netzwerk kontrolliert. Alle Daten, die das Netz verlassen, können ebenso überprüft werden wie die, die hineinwollen.

Firmware: Als Firmware bezeichnet man Software, die in elektronische Geräte eingebettet ist. Je nach Gerät kann Firmware den Funktionsumfang von zum Beispiel BIOS, Betriebssystem oder Anwendungssoftware enthalten. Firmware ist speziell auf die jeweilige Hardware zugeschnitten und nicht beliebig austauschbar.

Hacker: Computerbenutzer mit einem überdurchschnittlichen 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, sie zu beseitigen. Hacker, die Sicherheitslücken suchen und ausnutzen, um illegalen Zugriff auf fremde Rechnersysteme zu erlangen und dort Schaden anrichten, werden innerhalb der Hackerszene als „Cracker“ tituliert.

Identitätsdiebstahl: Ein Benutzer identifiziert sich im Internet meist über eine Kombination aus Identifikations- und Authentisierungsdaten wie etwa Benutzername und Passwort, Bank- oder Kreditkarteninformationen. Verschafft sich ein unberechtigter Dritter Zugang zu solchen Daten, wird von Identitätsdiebstahl gesprochen.

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

IT-Sicherheitsbeauftragter: Person mit Fachkompetenz, die für Aspekte rund um die IT-Sicherheit zuständig ist, in enger Abstimmung mit dem IT-Betrieb. Die Rolle des Verantwortlichen für Informationssicherheit wird je nach Art und Ausrichtung der Institution

anders genannt. Im IT-Grundschutz wird die Bezeichnung Informationssicherheitsbeauftrager (ISB) verwendet.

Keylogger: Als Keylogger wird Hard- oder Software zum Mitschneiden von Tastatureingaben bezeichnet. Sie zeichnen alle Tastatureingaben auf, um sie möglichst unbemerkt an einen Angreifer zu übermitteln, der aus den Informationen Daten wie etwa Anmeldeinformationen oder Kreditkartennummern filtern kann.

Kritische Infrastrukturen (KRITIS): Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen einträten. In Deutschland werden folgende Sektoren (und Branchen) den Kritischen Infrastrukturen zugeordnet: Transport und Verkehr, Energie, Informationstechnik und Telekommunikation (Telekommunikation, Informationstechnik), Finanz- und Versicherungswesen, Staat und Verwaltung, Ernährung, Wasser, Gesundheit, Medien und Kultur.

Kryptografie ist die Wissenschaft der Verschlüsselung von Informationen in „Geheimschriften". Damit soll verhindert werden, dass Dritte Informationen einsehen können, die nicht für sie bestimmt sind. Im Internet werden verschiedene Verschlüsselungssysteme eingesetzt, um einen sicheren Datenaustausch zu gewährleisten und vertrauliche Informationen zu schützen. Kryptografische Verfahren kommen auch bei der digitalen Signatur zum Einsatz.

Krypto-Miner missbrauchen betroffene Systeme zur Errechnung von Krypto-Währungen.

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 meist schädliche Funktionen auszuführen. Beispiele sind Computer-Viren, Würmer und Trojanische Pferde. Schadsoftware ist üblicherweise für eine bestimmte Betriebssystemvariante konzipiert und wird daher meist für verbreitete Systeme und Anwendungen geschrieben.

Man-in-the-Middle-Angriff: Ziel bei einem Man-in-the-Middle-Angriff ist es, sich unbemerkt in eine Kommunikation zwischen zwei oder mehr Partnern einzuschleichen, etwa um Informationen mitzulesen oder zu manipulieren. Der Angreifer begibt sich „in die Mitte" der Kommunikation, indem er sich gegenüber dem Sender als Empfänger und gegenüber dem Empfänger als Sender ausgibt. Er leitet zunächst eine Verbindungsanfrage des Senders zu sich um und baut dann eine Verbindung zum eigentlichen Empfänger der Nachricht auf. Gelingt ihm das, kann der Angreifer im Zweifel alle Informationen, die der Sender an den vermeintlichen Empfänger sendet, einsehen oder manipulieren, bevor er sie an den richtigen Empfänger weiterleitet. Ohne entsprechende Schutzmaßnahmen kann er auch auf die Antworten des Empfängers zugreifen.

Manuelles Hacking: Manipulation von Soft- und Hardware ohne den Einsatz von Schadprogrammen.

Patch (= Flicken): kleines Programm, das Fehler in Anwendungsprogrammen oder Betriebssystemen behebt.

Penetrationstest: Ein Penetrationstest ist ein gezielter, in der Regel simulierter, Angriffsversuch auf ein IT-System. Er wird als Wirksamkeitsprüfung vorhandener Sicherheitsmaßnahmen eingesetzt.

Personal Firewall: Eine Personal Firewall ist ein 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. Beim Pharming allerdings wird die Infrastruktur so manipuliert, dass das Opfer auch dann auf einer gefälschten Webseite landet, wenn es die korrekte Adresse des Dienstes eingeben 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: Beim Phishing (eine Kombination aus „Password" und „Fishing", zu Deutsch „nach Passwörtern angeln") wird zum Beispiel mittels gefälschter E-Mails und/oder Webseiten versucht, Zugangsdaten für einen Dienst oder eine Webseite zu erlangen. Wird die Manipulation vom Opfer nicht erkannt und die Authentizität einer Nachricht oder Webseite nicht hinterfragt, gibt das Opfer seine Zugangsdaten 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, oder die Nutzer von E-Commerce-Anwendungen, etwa Onlineshops oder Online-Dienstleister. Angreifer setzen zunehmend Schadprogramme statt klassischem Phishing als Mittel zum Identitätsdiebstahl ein. Andere Varianten des Phishings setzen auf gefälschte Near Field Communication (NFC)-Tags oder Barcodes, die vom Opfer eingelesen werden und auf eine Phishing-Seite weiterleiten.

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 einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form digitaler Erpressung.

RDP-Anwendungen: Remote Desktop Protocol (RDP) ist eine Software mit dem sich über ein Netzwerk aus der Ferne auf einen Rechner mit Windows-Betriebssystem zugreifen lässt.

Rootkit: Ein Rootkit ist ein Schadprogramm, das manipulierte Versionen von Systemprogrammen enthält. Unter Unix sind dies typischerweise Programme wie login, ps, who, netstat etc. Die manipulierten Systemprogramme sollen es einem Angreifer ermöglichen, zu verbergen, dass er sich erfolgreich einen Zugriff mit Administratorenrechten verschafft hat, sodass er diesen Zugang später erneut benutzen kann.

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

Sicherheitsvorfall: Als Sicherheitsvorfall wird ein unerwünschtes Ereignis bezeichnet, das Auswirkungen auf die Informationssicherheit hat und in der Folge große Schäden nach sich ziehen kann. Typische Folgen von Sicherheitsvorfällen können die Ausspähung, Manipulation oder Zerstörung von Daten sein.

Skimming: bezeichnet das unbemerkte Auslesen von Zahlungskarten (Bank- und Kreditkarten) durch physikalische Manipulation von Geldautomaten oder Zahlungsterminals. Mit den ausgelesenen Daten werden in der Folge Karten-Kopien erstellt. Um auf das Konto des Opfers zugreifen zu können, wird meist auch die Eingabe der zugehörigen PIN aufgezeichnet, beispielsweise mithilfe einer kleinen, unauffälligen Kamera oder einer manipulierten Tastatur.

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.

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. Oft enthält Spam jedoch auch Schadprogramme im Anhang, Links zu verseuchten Webseiten oder wird für Phishing-Angriffe genutzt.

Spoofing: (von to spoof = manipulieren, verschleiern, vortäuschen) nennt man in der Informationstechnik verschiedene Täuschungsversuche zur Verschleierung der eigenen Identität und zum Fälschen übertragener Daten. Ziel ist es, die Integrität und Authentizität der Informationsverarbeitung zu untergraben.

Spyware: Als Spyware werden Programme bezeichnet, die heimlich, also ohne darauf hinzuweisen, Informationen über einen Benutzer bzw. die Nutzung eines Rechners sammeln und an den Urheber der Spyware weiterleiten. Spyware gilt häufig nur als lästig, dabei können auf diesem Weg auch sicherheitsrelevante Informationen wie Passwörter ausgeforscht werden.

Trojanisches Pferd: Ein Trojanisches Pferd, oft auch (fälschlicherweise) kurz Trojaner genannt, ist ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung. Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer.

Vendor Lock-in: Von einem Vendor Lock-in spricht man, wenn Kunden so sehr von einem Produkt oder einer Dienstleistung eines Anbieters abhängig sind, dass sich ein Wechsel zu einem Mitbewerber wirtschaftlich nicht lohnen würde.

Virenschutzprogramm: Es überprüft neue Dateien (zum Beispiel Anhänge von E-Mails) und den gesamten Computer auf Schadsoftware. Dazu vergleicht es in erster Linie die Daten auf dem Rechner mit den „Fingerabdrücken" bekannter Schadprogramme.

Virtuelle private Netze (VPN): VPN steht für Virtual Private Network. Es verschlüsselt die Datenkommunikation zwischen zwei Endpunkten – zum Beispiel zwischen einem Endgerät und einem VPN-Server. Auf diese Weise kann die Kommunikation nicht ohne Weiteres mitgelesen oder verändert werden.

Virus: Bezeichnung für Programmteile, die sich selbst vervielfältigen können, sich an andere Programme (oder Dateien) hängen und versuchen, den Ablauf des Computerbetriebs zu stören. Viren unterscheidet man nach Verbreitungswegen: Boot-Viren, Datei-Viren, Makro-Viren, Multipartite Viren. Während in der Medizin ein Virus ein Neutrum ist, wird in der Informationstechnologie ein Virus meist maskulin verwendet (der Virus).

Vishing: Kombination aus „Voice over Internet Protocol" (VoIP) und dem Namen der Betrugstechnik „Phishing". Die geringen Kosten der Internettelefonie (VoIP) 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 dem Entdecker bekannt ist, charakterisiert man mit dem Begriff Zero-Day-Exploit. Die Öffentlichkeit und insbesondere 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 den Hersteller existierte – also an einem fiktiven „Tag null". Der Hersteller hat somit keine Zeit, die Nutzer vor den ersten Angriffen zu schützen.

Zwei-Faktor-Authentisierung: Die Zwei-Faktor-Authentisierung bezeichnet die Kombination von zwei Faktoren aus den drei Bereichen Wissen (zum Beispiel Passwort), Besitz (zum Beispiel Chipkarte) und Biometrie (zum Beispiel Fingerabdruck).

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

QUELLENVERZEICHNIS

(ISC)²
Allianz
Bitkom e. V.
BlackFog
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Bundesministerium für Wirtschaft und Klimaschutz
Bundesnetzagentur
Cisco
CVE
CSIS
Cybersecurity Ventures
Destatis
Deutscher Gewerkschaftsbund
Deutschland sicher im Netz (DsiN)
DSGVO-Portal
Embroker
Europäische Kommission
Eurostat
EY
FBI
Foundry
Gartner
G DATA
Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GdV)
Hiscox
IBM Security
International Telecommuniction Union
Internet Crime Complaint Center
KPMG
Kriminologisches Forschungsinstitut Niedersachsen e. :V.
Marsh
Microsoft
Mimecast
Munich Re
Nutanics
Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK)
Ponemon Institute
PricewaterhouseCoopers
Shodan.io
Specops
Statcounter
Statista
Statistisches Bundesamt
Transforma Insights
UpGuard
Unternehmen Cybersicherheit – gemeinsame Initiative von VDMA und VSMA
US Departmen of Justice
Vanson Bourne

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, Julia Hasler, Dr. Daniela Kalkühler, Stefan Karpenstein, Joy Linders
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: Gesine Braun, Renate Hensel, Peter Lau, Kathrin Lilienthal
Autoren: Ulf J. Froitzheim, Christoph Koch, Andreas Molitor
Marktforschung, Recherche, Daten und Quellen:
Christian Cramer, Lukas Heiduk, Cindy Karwowski, Ana-Cristina Martus, Robin Rehfeldt,
Nina Reuschling, Daniel Tippel

brand eins G DATA statista