2021
CYBERSICHERHEIT IN ZAHLEN

2021

CYBERSICHERHEIT IN ZAHLEN

Lernen. Wissen. Handeln.

brandeins

G DATA

statista

So fing es an

Vor rund 35 Jahren, die Zeit der sogenannten Home-Computer, da habe ich mit meinen knapp zwanzig Jahren auch gern das eine oder andere Computerspiel gespielt. Eines Tages startete eines der Spiele nicht mehr. Dramatisch war das natürlich nicht – damals waren Unternehmen noch nicht existenziell auf eine funktionierende IT angewiesen und den Begriff „Privatanwender“ gab es noch gar nicht. Niemand hatte in den Achtzigerjahren umfangreiche Dateisammlungen mit Videos von den ersten Schritten seines Kindes oder den Unterlagen für die Steuererklärung auf diesen Home-Computern gespeichert.

Das Computerspiel habe ich wieder zum Laufen gebracht. Aber ich fand in der Startsequenz der damals weitverbreiteten Disketten Programmcode, der nicht zum Spiel gehörte. Viel Code war es nicht und er war schnell analysiert: ein kleines Programm, das nicht anderes tat, als sich auf weitere Disketten zu kopieren – ein Computervirus.

Und doch löste das bei mir ein ungutes Gefühl aus: Wie kam der Programmcode dahin, schließlich war ich „der Herr“ meines Computers, und wie kam es, dass auch fast alle anderen meiner Disketten „verseucht“ waren?

Mit einem kurzen Prüfprogramm war meine Diskettensammlung rasch „gesäubert“. Und ich konnte doch wohl kaum der Einzige sein, der ein solches Problem hatte. Diese Erkenntnis führte dazu, dass die damals junge Firma G DATA sich seither mit dem Thema IT-Sicherheit auseinandersetzt. Zunächst mit Lösungen vor allem für Privatpersonen – heute auch für Unternehmen und Behörden weltweit.

Seitdem hat sich die Bedrohungslage deutlich verschärft. Statt wie früher alle paar Monate ein Signatur-Update auf Diskette zu verschicken, arbeiten wir jetzt mit einem auf KI-Technologien basierenden Echtzeitschutz. Und statt einzelne Malwaresamples mühsam zu zerlegen, analysieren wir heute jeden Tag rund 600 000 verdächtige Dateien.

Der Themenbereich IT-Sicherheit ist für viele Menschen eine komplexe, undurchschaubare Materie, die hohe Anforderungen stellt: Unternehmen müssen ihre Technik im Griff haben und ihren Mitarbeitern den sicheren Umgang mit IT-Systemen vermitteln. Sie müssen einerseits ihre Verteidigung hochfahren, sich aber andererseits auch für den Notfall wappnen. Denn totale IT-Sicherheit gibt es nicht.

Dieses Heft will Sie mit Umfragen, Statistiken und Artikeln zu den wichtigsten Herausforderungen der IT-Sicherheit anregen, sich auf die Vielfalt des Themas einzulassen. Wir verzichten auf Schauergeschichten und erhobene Zeigefinger, denn Angst oder das Gefühl der Überforderung bringen niemanden weiter. Im Gegenteil: Sicherheit ist machbar – lassen Sie sich da nicht verunsichern!

Ich wünsche Ihnen viel Freude beim Lesen,

Ihr Andreas Lüning
Gründer und Vorstand G DATA

So geht es

Als wir die Idee für dieses Magazin entwickelten, war Corona noch kein Thema. Wir redeten vor allem über Digitalisierung: über ihre Chancen und Risiken, intelligente Tools und Prozesse, über Algorithmen, Strukturen, Geschäftsmodelle, künstliche Intelligenz, Vernetzung – und über die zahllosen Einfallstore für Kriminelle, die das alles schafft.

Mit dem massenhaften Umzug ins heimische Büro und dem Ausbau der technologischen Infrastrukturen ist auch die Sensibilität für das Thema Sicherheit gestiegen: Mit welchen Bedrohungen müssen wir rechnen? Welche Gefahren birgt die virtuelle Welt? Was wissen wir darüber, und was sollten wir eigentlich wissen, beruflich und privat?

Inzwischen ist es mehr als nur angeraten, sich mit diesen Themen zu beschäftigen und sich zumindest Grundkenntnisse für einen sicheren Umgang mit Rechner, Smartphone und digitalen Endgeräten anzueignen. IT-Know-how ist unverzichtbar geworden, für jeden von uns – im Job, im Privatleben und im Homeoffice, der neuen Zwischenwelt. Gerade dort ist ein Desinteresse an Virenscannern, Passwortschutz oder Cookie-Richtlinien gefährlich, im Zweifel sogar strafbar. Aber das Büro ist eben nur ein Ort von vielen, die uns heute zum Verhängnis werden können: Die Zahl der Cyberangriffe in Deutschland wächst, und das Risiko einer Bedrohung durch Manipulation von Konto- und Finanzinformationen oder das Ausspähen und Abfangen von Daten ist höher, als es den meisten von uns bewusst ist.

Grund genug für Statista und brand eins, dem Thema ein eigenes Heft zu widmen. Mit G DATA, dem Spezialisten für die Abwehr von Cyberattacken, haben wir dafür den idealen Partner gefunden. Gemeinsam wollen wir ab sofort die IT-Sicherheit ergründen: Zahlen, Daten und Fakten aus aller Welt aufbereiten, Unternehmen, Organisationen, Branchen und Industrien untersuchen, die Meinungen und Einschätzungen der deutschen Bevölkerung erfragen – und deren Sicherheitsgefühl jedes Jahr mit dem G DATA Index in einer eigenen Kennziffer abbilden.

In dieser ersten Ausgabe geht es um Vertrauen: um gefühlte und tatsächliche Sicherheiten, um echte und scheinbare Kompetenzen, um die Lücke zwischen Wissen und Tun. Denn natürlich ist uns allen inzwischen längst klar, dass wir uns gegen Hacker, Phisher und datenhungrige Digitalplattformen absichern müssten – und doch tun wir es nicht. Warum das so ist, und was wir besser machen sollten, lesen Sie in diesem Heft.

Susanne Risch
Chefredakteurin

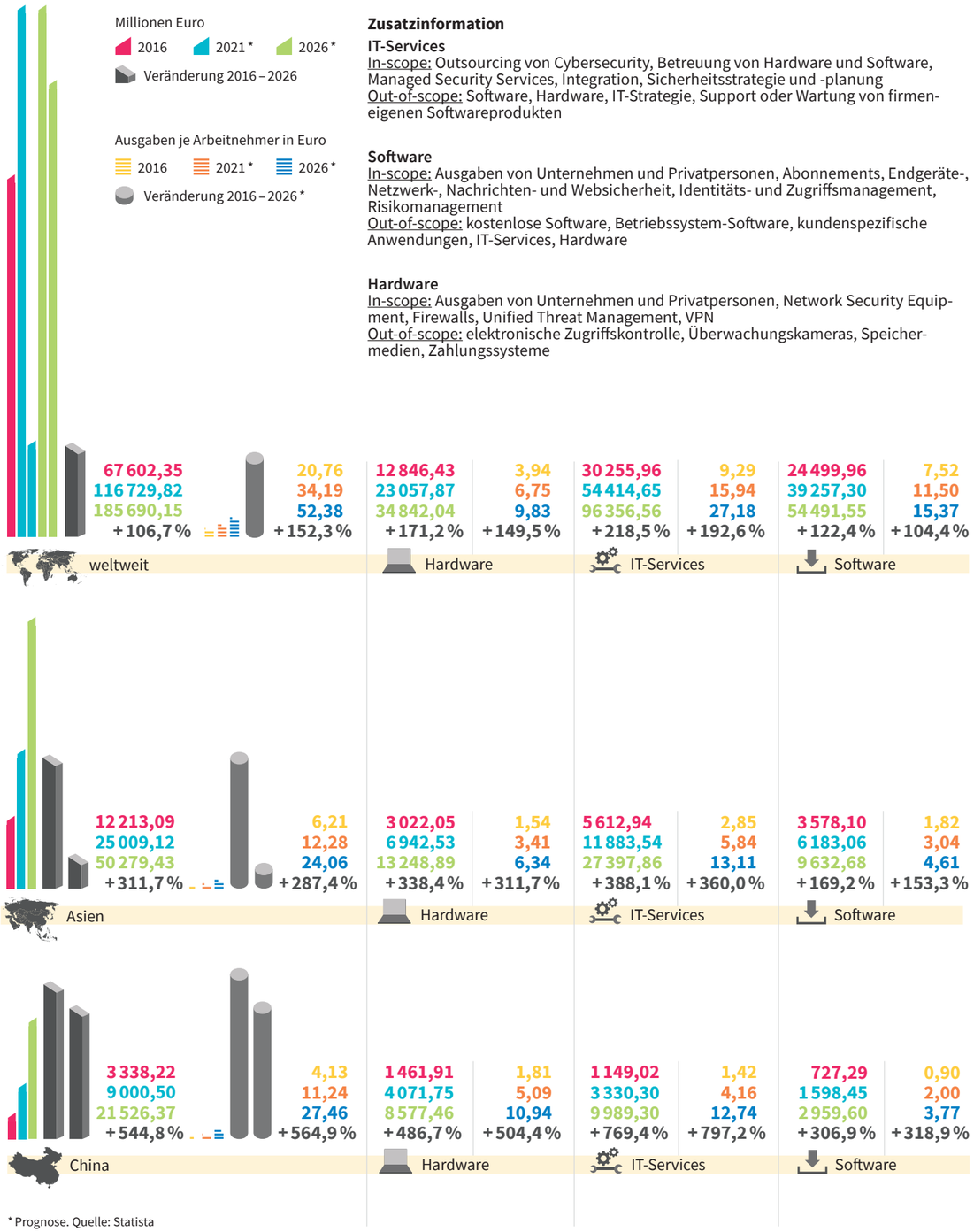
Inhalt

WELT

Digitalisierungsgrad und Bewusstsein für Datenschutz, Ausgaben für Cybersicherheit und Cyberversicherungen, Datenpannen und Datenlecks, Internetnutzer und IT-Experten, Schwachstellen und Arten von Cyberkriminalität, Public-Cloud-Services und künstliche Intelligenz, Bußgelder und entgangene Umsätze, Branchen und Privates.

Was ist uns unsere Sicherheit wert – gestern, heute, morgen?

Cybersecurity Market Outlook; ausgewählte Länder weltweit; in Millionen Euro und durchschnittliche Ausgaben je Arbeitnehmer; in Euro



Zusatzinformation

IT-Services
In-scope: Outsourcing von Cybersecurity, Betreuung von Hardware und Software, Managed Security Services, Integration, Sicherheitsstrategie und -planung
Out-of-scope: Software, Hardware, IT-Strategie, Support oder Wartung von firmeneigenen Softwareprodukten

Software
In-scope: Ausgaben von Unternehmen und Privatpersonen, Abonnements, Endgeräte-, Netzwerk-, Nachrichten- und Websicherheit, Identitäts- und Zugriffsmanagement, Risikomanagement
Out-of-scope: kostenlose Software, Betriebssystem-Software, kundenspezifische Anwendungen, IT-Services, Hardware

Hardware
In-scope: Ausgaben von Unternehmen und Privatpersonen, Network Security Equipment, Firewalls, Unified Threat Management, VPN
Out-of-scope: elektronische Zugriffskontrolle, Überwachungskameras, Speichermedien, Zahlungssysteme

* Prognose. Quelle: Statista

Passiert

Durchschnittliche Gesamtkosten von Datenpannen; 2019 / 2020; in Millionen Euro

7,71 USA
1,00 Brasilien
1,92 Australien
5,82 Mittlerer Osten
4,02 Kanada
2,79 Südkorea
3,97 Deutschland
1,50 Lateinamerika
3,58 Frankreich
3,48 Großbritannien
2,85 Italien
1,91 Südafrika
3,45 Durchschnitt weltweit
1,79 Indien
2,24 Skandinavien
1,58 Türkei
2,42 Asien
3,74 Japan

Quellen: Ponemon Institute, IBM Security

Engagiert

Länder mit dem höchsten Engagement in Cybersicherheit nach dem GCI-Index *; 2018; Index

Großbritannien	0,93
USA	0,93
Frankreich	0,92
Litauen	0,91
Estland	0,91
Singapur	0,90
Spanien	0,90
Malaysia	0,89
Norwegen	0,89
Kanada	0,89
Australien	0,89

* Global Cybersecurity Index. 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 Cybersicherheitsverpflichtungen. Quelle: International Telecommunication Union (ITU)

Investiert

Ausgaben für Cybersicherheit im Vergleich zum IT-Budget; ausgewählte Länder; 2019; in Millionen Euro

	Durchschnittl. IT-Budget	Durchschnittl. Ausgaben für Cybersicherheit	Anteil der Ausgaben für Cybersicherheit am IT-Budget
Frankreich	21,9	1,9	8,6 %
USA	14,5	1,3	9,2 %
Belgien	13,7	1,6	11,6 %
Deutschland	13,5	1,5	10,9 %
Niederlande	13,0	1,2	8,9 %
Durchschnitt	**13,1**	**1,3**	**9,9 %**
Spanien	11,1	1,0	8,9 %
Großbritannien	7,8	0,8	10,3 %

Quelle: Hiscox

Digitalisiert

Digitalisierungsgrad nach DESI-Index *; Europa; 2020; Index

Finnland	72,3
Schweden	69,7
Dänemark	69,1
Niederlande	67,7
Malta	62,7
Irland	61,8
Estland	61,1
Belgien	58,7
Luxemburg	57,9
Spanien	57,5
Deutschland	**56,1**
Österreich	54,3
Litauen	53,9
Europäische Union	**52,6**
Frankreich	52,2
Slowenien	51,2
Tschechien	50,8
Lettland	50,7
Portugal	49,6
Kroatien	47,6
Ungarn	47,5
Slowakei	45,2
Polen	45,0
Zypern	44,0
Italien	43,6
Rumänien	40,0
Griechenland	37,3
Bulgarien	36,4

* DESI = Digital Economy and Society Index. Der DESI-Gesamtindex berechnet als gewichteter Durchschnitt der fünf DESI-Hauptdimensionen: 1. Konnektivität (25 %), 2. Humankapital (25 %), 3. Nutzung des Internets (15 %), 4. Integration digitaler Technologie (20 %) und 5. digitale öffentliche Dienste (15 %). Quelle: Europäische Kommission

Identifiziert

Zahl kompromittierter Accounts; weltweit; abgerufen am 8.4.2021 vom Hasso-Plattner-Institut *

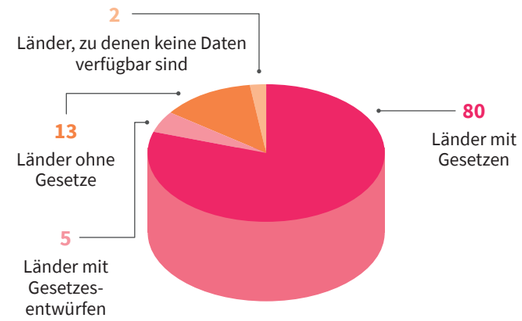
12 265 476 980
identifizierte kompromittierte Accounts

1 623 414
geleakte Accounts pro Tag

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

Reguliert

Gesetzgebungen zur Cyberkriminalität; weltweit; 2020; in Prozent



Quelle: UNCTAD

Attackiert

Die größten Datenlecks: Zahl gefährdeter Accounts; 2013 – 2020; weltweit; in Millionen

CAM4 * (März 2020)	10 880
Yahoo (August 2013 – aufgedeckt Dezember 2016; Update Oktober 2017)	3 000
River City (Februar 2016)	1 370
Adhaar System of the Unique Identification Authority of India (UIDAI) (Januar 2018)	1 000
Adhaar (Januar 2018)	1 000
First American Financial Corp. (Mai 2019)	885
Vertifications.io (Februar 2019)	763
Facebook (April 2019)	540
Yahoo (2014 – aufgedeckt August 2016)	500
Marriot / Starwood (November 2018)	500

* CAM4 ist der Name einer beliebten Plattform für Erwachsene mit „free live sex cams“. Quelle: UpGuard

Spioniert

Gefährdete Daten bei Datenpannen; ausgewählte Branchen und Länder weltweit; 2019 / 2020; in Prozent

Quellen: Ponemon Institute, IBM Security

Addiert

Durchschnittliche Gesamtkosten von Datenpannen in ausgewählten Branchen; weltweit; 2019 / 2020; in Millionen Euro

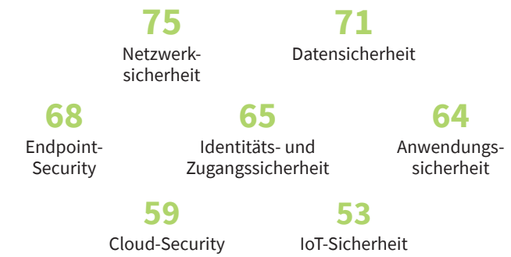
6,37 Gesundheit
5,71 Energie
5,22 Finanzen
4,52 Pharma
4,50 Technologie
4,46 Industrie
3,78 Dienstleistungen
3,64 Unterhaltung
3,48 Bildung
3,45 **Durchschnitt weltweit**
3,20 Transport
2,69 Kommunikation
2,31 Verbraucher
1,79 Einzelhandel
1,54 Gastgewerbe
1,47 Medien
1,37 Forschung
0,96 öffentlicher Sektor

Quellen: Ponemon Institute, IBM Security

Künstliche Intelligenz I

Nutzung von künstlicher Intelligenz nach Bereichen der Cybersicherheit; Befragung von Führungskräften in ausgewählten Ländern *; 2019; in Prozent

„In welchen der folgenden Bereiche nutzen Sie künstliche Intelligenz für die Cybersicherheit Ihres Unternehmens?“



* Frankreich, Deutschland, Großbritannien, USA, Australien, Niederlande, Indien, Italien, Spanien und Schweden. Quelle: Capgemini

Künstliche Intelligenz II

Nutzung von künstlicher Intelligenz zur Abwehr von Cyberattacken; Befragung von Führungskräften in ausgewählten Ländern; 2019; in Prozent

„Wir wären ohne künstliche Intelligenz nicht in der Lage, uns gegen Cyberattacken zu verteidigen.“

USA	83
Australien	73
Großbritannien	72
Spanien	71
Frankreich	70
Indien	69
Italien	69
Niederlande	68
Deutschland	62
Schweden	54

Quelle: Capgemini

IT-Infrastrukturen für alle

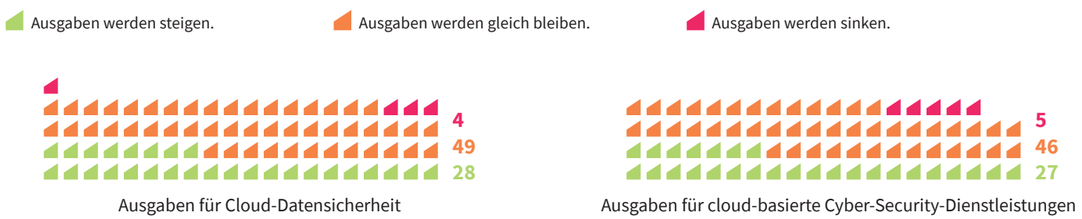
Prognose des Umsatzes für Public Cloud Services; weltweit; in Millionen Euro

	2019	2020	2021	2022	Veränderung 2019 – 2022
Cloud Application Services (SaaS)	91 128,6	91 817,5	106,1	123 358,8	35,4 %
Cloud Application Infrastructure Services (PaaS)	33 492,9	38 156,1	50,3	63 177,2	88,6 %
Cloud Business Process Services (BPaaS)	40 367,9	38 103,5	40 602,6	43 428,9	7,6 %
Cloud Management and Security Services	11 460,7	12 862,3	14,1	16 128,9	40,7 %
Cloud System Infrastructure Services (IaaS)	39 693,8	44 204,4	56,4	7 103,5	– 82,1 %
Desktop as a Service (DaaS)	550,0	1 055,3	1 711,4	2 223,7	304,3 %
Gesamtmarkt	**216 693,8**	**226 199,1**	**269 252,6**	**319 352,6**	**47,4 %**

Quelle: Gartner

Ausgaben für die Cloud

Einschätzung zur Entwicklung der Ausgaben für Cloud-Datensicherheit; Entscheider im Bereich IT- und Unternehmenssicherheit; weltweit; 2020; in Prozent



Quelle: IDG Research Services

Mehr Sicherheit

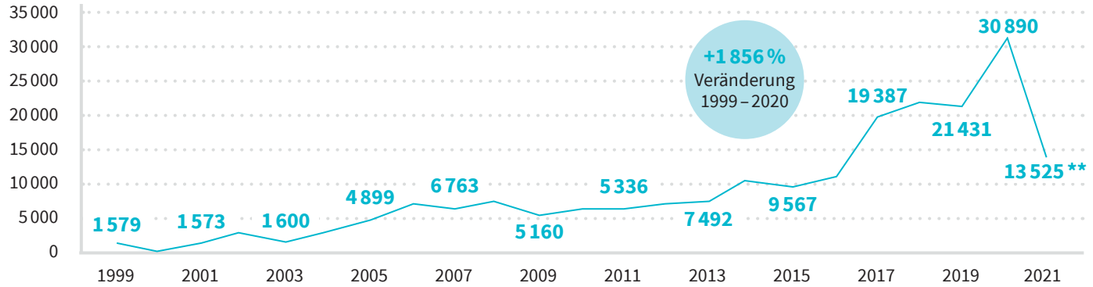
Ausgaben je Cybersicherheitssegment; weltweit; in Millionen Euro

	2019	2020	Veränderung 2019 – 2022
Sicherheitsdienstleistungen	55 338,4	56 377,2	3,7 %
Schutz der Infrastruktur	14 750,0	15 336,0	5,8 %
Ausstattung zur Netzwerksicherheit	11 952,7	10 257,9	– 12,6 %
Identitäts- und Zugangsmanagement	8 783,0	9 130,7	5,8 %
Sicherheitssoftware für Konsumenten	5 583,9	5 469,3	– 0,3 %
integriertes Risikomanagement	4 067,0	4 150,0	3,8 %
Anwendungssicherheit	2 763,4	2 883,3	6,2 %
Datensicherheit	2 376,8	2 501,8	7,2 %
andere Software zur Informationssicherheit	1 969,6	1 993,9	3,1 %
Cloud Security	392,0	513,2	33,3 %
gesamt	**107 976,8**	**108 612,3**	**2,4 %**

Quelle: Gartner

Erhebliche Schwachstellen

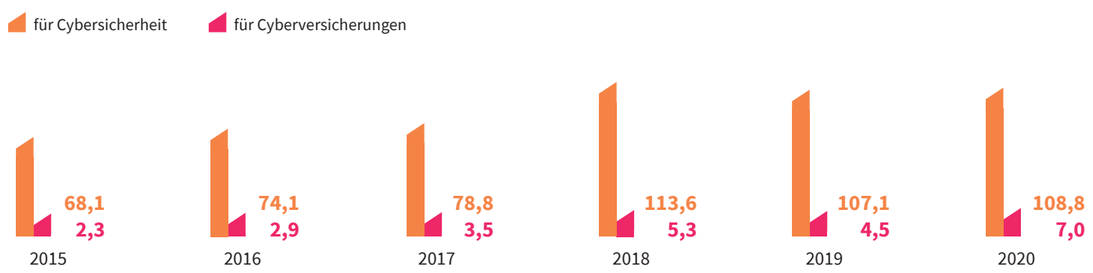
Entwicklung dokumentierter Schwachstellen in der IT-Sicherheit *; weltweit; Zahl



* Die Aufgabe des CVE®-Programms ist es, öffentlich bekannt gemachte Sicherheitslücken in der Cybersicherheit zu identifizieren, zu definieren und zu katalogisieren. Für jede Schwachstelle im Katalog gibt es einen CVE-Eintrag. Die Schwachstellen werden von Organisationen aus der ganzen Welt, die eine Partnerschaft mit dem CVE-Programm eingegangen sind, entdeckt, zugewiesen und veröffentlicht. Die Partner veröffentlichen CVE-Datensätze, um konsistente Beschreibungen von Sicherheitslücken zu kommunizieren. Fachleute aus den Bereichen Informationstechnologie und Cybersicherheit verwenden CVE-Datensätze, um sicherzustellen, dass sie über das gleiche Problem sprechen, und um ihre Bemühungen zu koordinieren, die Schwachstellen zu priorisieren und zu beheben. ** Stand 13.4.2021. Quelle: CVE (Common Vulnerabilities and Exposures

Steigende Ausgaben

Jährliche Ausgaben für Cybersicherheit und Cyberversicherung; weltweit; in Milliarden Euro



Quellen: Marsh, Microsoft, Gartner, Munich Re

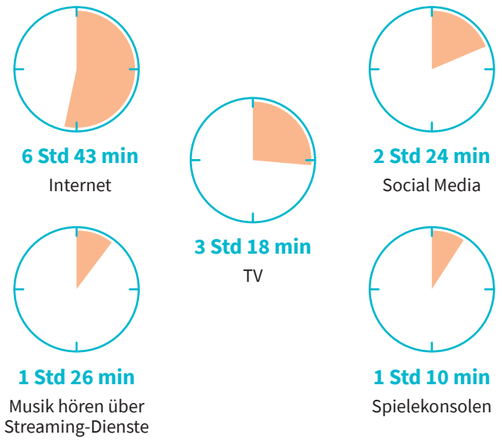
USA und Asien-Pazifik

Anteil der Besitzer von Smart-Home-Produkten nach Region; 16- bis 64-jährige Internetnutzer; weltweit; 2019; in Prozent

Quelle: Global Web Index

Stunden und Minuten

Durchschnittliche Nutzungszeit eines Mediums pro Tag; 16- bis 64-jährige Internetnutzer; weltweit; 2019; in Stunden und Minuten *



* In den einzelnen Kategorien kommt es zu Überschneidungen, da z. B. bei TV nicht nur Kabelfernsehen, sondern auch Streaming enthalten ist.
Quellen: DataReportal; We Are Social; Hootsuite; Global Web Index

Regional verschieden

Anteil der Internetnutzer an der Gesamtbevölkerung nach Region; weltweit; 2021; in Prozent

Nordeuropa	96
Westeuropa	93
Nordamerika	90
Südeuropa	86
Osteuropa	82
Südamerika	72
Westasien	74
Ozeanien	71
Südosteuropa	69
Zentralamerika	67
Ostasien	68
Südliches Afrika	62
Karibik	62
Welt	**60**
Zentralasien	57
Nordafrika	56
Südasien	42
Westafrika	42
Mittleres Afrika	26
Ostafrika	24

Quellen: DataReportal; We Are Social; Hootsuite

Weltweit verteilt

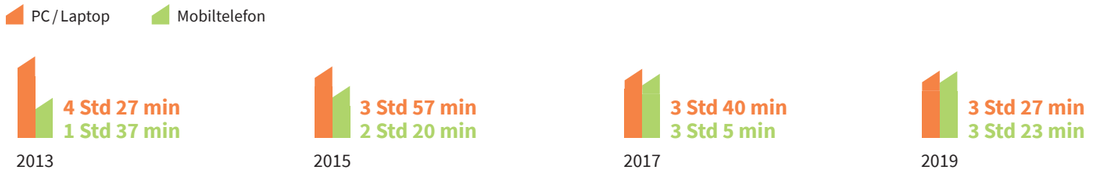
Überblick zur Internetnutzung; 16- bis 64-jährige Internetnutzer; weltweit; 2019 / 2020

Gesamtzahl weltweiter Internetnutzer	4,54 Milliarden
Anteil der Internetnutzer an der weltweiten Bevölkerung	59 %
jährliches Wachstum der weltweiten Internetnutzer	298 Millionen (+7 %)
durchschnittliche Zeit im Internet (pro Tag) je Internetnutzer	6 Std 43 min

Quellen: DataReportal; We Are Social; Hootsuite

Rechner und Mobiltelefon

Zeit der Internetnutzung nach Gerät am Tag; Internetnutzer; weltweit; in Stunden und Minuten

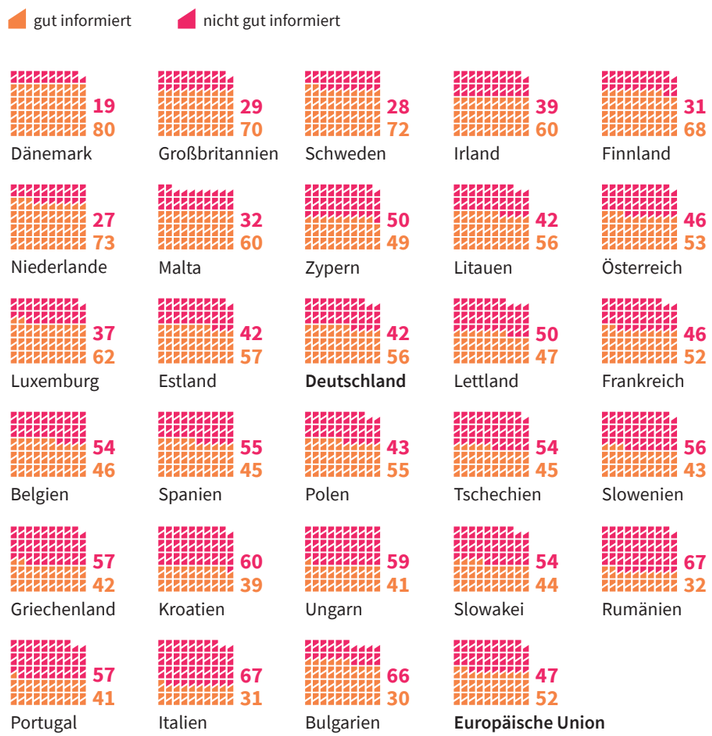


Quelle: Global Web Index

Informierte Dänen

Informationsstand von Internetnutzern zu Risiken von Cyberkriminalität; Europa; 2019; in Prozent

„Wie gut fühlen Sie sich über die Risiken durch Cyberkriminalität informiert?“



Quelle: Europäische Kommission

Glückliche Litauer

Erfahrung mit mindestens einem IT-Sicherheitsvorfall; Europa; 2019; in Prozent

Litauen	7
Polen	9
Lettland	10
Griechenland	13
Bulgarien	13
Slowenien	17
Kroatien	18
Ungarn	20
Irland	20
Zypern	21
Portugal	21
Slowakei	21
Tschechien	22
Italien	22
Spanien	28
Belgien	28
Estland	32
Europäische Union	**34**
Österreich	36
Luxemburg	37
Deutschland	**40**
Finnland	41
Niederlande	42
Malta	42
Schweden	45
Frankreich	46
Großbritannien	50
Dänemark	50
Rumänien	k. A.

Quelle: Eurostat

Betrogene Europäer

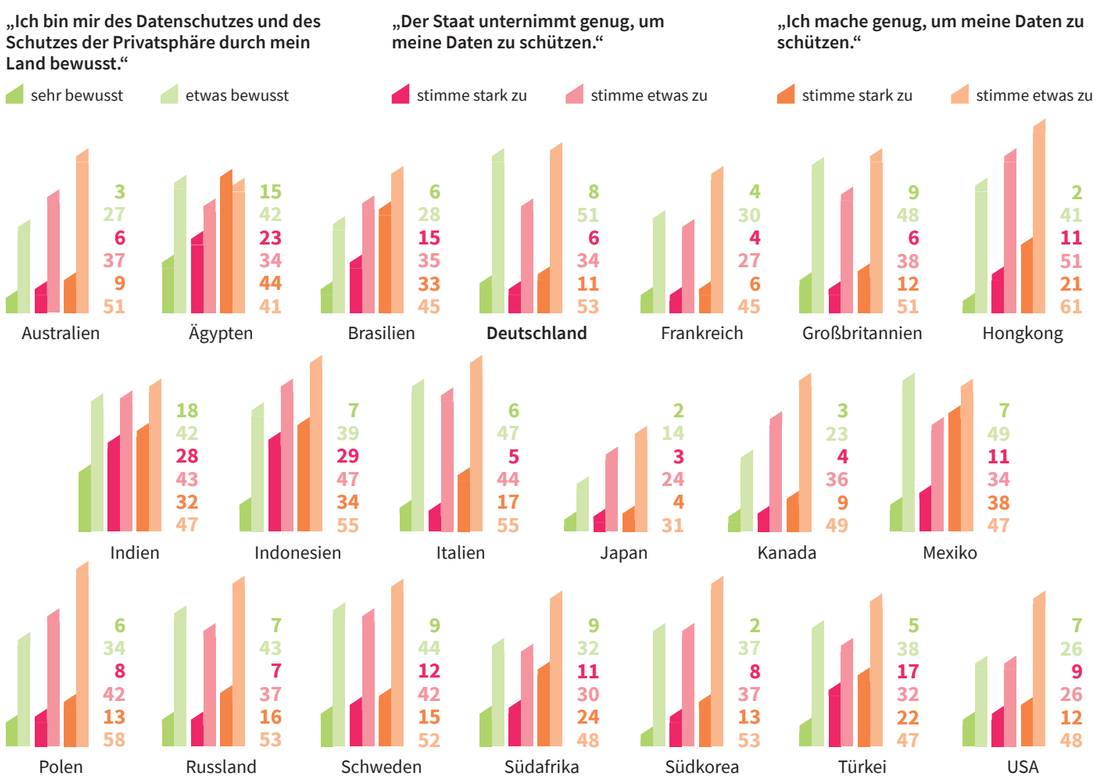
Erfahrungen von Internetnutzern mit betrügerischen E-Mails und Anrufen; Europa; 2019; in Prozent

„Wie oft haben Sie folgende Situation in den vergangenen drei Jahren erlebt oder sind Opfer davon geworden: Empfang von betrügerischen E-Mails oder Anrufen, die nach persönlichen Daten fragen (inkl. Zugang zu Ihrem Computer, Log-in Daten, Bank- und Zahlungsinformationen)?“

Quelle: Europäische Kommission

Hoffen, glauben, selber machen

Bewusstsein für Datenschutz und Privatsphäre, Datenschutz durch den Staat und Bewertung von Aktivitäten zum persönlichen Datenschutz nach ausgewählten Ländern; Internetnutzer; weltweit *; 2019; in Prozent



* Nicht berücksichtigte Länder: China, Kenia, Nigeria, Pakistan, Tunesien. Quelle: Ipsos; Centre for International Governance Innovation (CIGI)

Besorgt

Anteil der Internetnutzer, die sich Sorgen um ihre Online-Privatsphäre machen; weltweit; 2019; in Prozent

Lateinamerika	86
Mittlerer Osten / Afrika	85
BRICS *	82
Asien-Pazifik	82
Nordamerika	77
G-8-Länder	73
Europa	67

* Brasilien, Russland, Indien, China, Südafrika.
Quelle: Ipsos; Centre for International Governance Innovation (CIGI)

Beunruhigt

Institutionelle Gefahren für die Online-Privatsphäre; Internetnutzer; weltweit; 2018; in Prozent

„Welche Faktoren beunruhigen Sie am meisten in Bezug auf Ihre Online-Privatsphäre?“

Cyberkriminelle	81
Internet-Unternehmen	74
andere Internetnutzer	66
Staat / Regierung	63
Unternehmen allgemein	65
ausländische Regierungen	58
Arbeitgeber	48

Quelle: Ipsos; Centre for International Governance Innovation (CIGI)

Aus Schaden klug geworden?

Änderung des Verhaltens von Internetnutzern; weltweit; in Prozent

Was haben Sie an Ihrem Verhalten im Internet im Vergleich zum Vorjahr verändert?

	2017	2019	Veränderung 2017 – 2019
keine E-Mails von unbekannten E-Mail-Adressen öffnen	45	45	0,0 %
weniger persönliche Daten im Internet offenlegen	k. A.	41	k. A.
bestimmte Internetseiten vermeiden	37	40	8,1 %
Antivirus-Software benutzen	38	36	– 5,3 %
regelmäßig Passwort ändern	31	33	6,5 %
Vermeidung von bestimmten Webanwendungen	31	32	3,2 %
Verbreitung wichtiger biografischer Daten verringern	29	29	0,0 %
Selbstzensierung der eigenen Online-Kommunikation	22	21	– 4,5 %
Wechsel der Online-Kommunikationspartner	14	15	7,1 %
weniger finanzielle Transaktionen (online)	15	15	0,0 %
weniger Online-Käufe	13	12	– 7,7 %
von Social-Media-Kanälen wie Facebook usw. abmelden	10	11	10,0 %
weniger Internetnutzung	9	8	– 11,1 %
nichts davon	19	16	– 15,8 %

Was haben Sie zusätzlich an Ihrem Verhalten geändert?

	2017	2019	Veränderung 2017 – 2019
nicht auf unbekannte Links in Nachrichten klicken	45	46	2,2 %
mehr Einstellungen zur Privatsphäre nutzen	32	33	3,1 %
häufigere Updates der Software	28	29	3,6 %
Internet häufiger als Unterhaltungsmedium benutzt	23	25	8,7 %
Zwei-Faktor-Authentifizierung nutzen	14	20	42,9 %
Internet häufiger für soziale Interaktion genutzt	18	19	5,6 %
häufigere Nutzung des Internets fürs geschäftliche Arbeiten	16	17	6,3 %
mehr Online-Einkäufe	13	15	15,4 %
Nutzung von verschlüsselten Kommunikationsservices	14	14	0,0 %
Nutzung VPN	10	12	20,0 %
nichts davon	22	19	– 13,6 %

Quelle: Ipsos; Centre for International Governance Innovation (CIGI)

Aus Fehlern gelernt?

Passwortänderung für den Account-Zugang in den vergangenen 12 Wochen; Internetnutzer; EU; 2019; in Prozent

Quelle: Europäische Kommission

Findige Kriminelle

Arten von Cyberkriminalität nach Berichten an das Internet Crime Complaint Center (FBI); weltweit; 2019; Anzahl / Euro

	Zahl der Opfer
Phishing / Vishing / Smishing * / Pharming	114 702
Nicht-Zahlung / Nicht-Lieferung	61 832
Erpressung / Wucher	43 101
persönliche Datenpanne	38 218
Spoofing	25 789
BEC / EAC **	23 775
Vertrauens- / Liebesbetrug	19 473
Identitätsdiebstahl	16 053
Belästigung / Gewaltandrohung	15 502
Überzahlung	15 395
erweiterte Gebühren	14 608
Arbeit / Anstellung	14 493
Kreditkartenbetrug	14 378
betrügerische staatliche Imitation / Personifikation	13 873
technischer Support	13 633
Real Estate / Miete	11 677
andere	10 842
Lotterie, Wettspiel, Erbschaft	7 767
Falschdarstellung / Falschangaben	5 975
Investment / Vermögensanlage	3 999
IPR / Copyright und Fälschung	3 892
Malware / Scareware / Virus	2 373
Ransomware (Erpressungssoftware)	2 047
Datenpanne im Unternehmen	1 795
DoS / TDoS	1 353
Kriminalität gegen Kinder	1 312
Re-Shipping	929
Zivilangelegenheiten	908
Bezug zum Gesundheitswesen	657
Wohltätigkeitsstiftungen	407
Glücksspiel	262
Terrorismus	61
Hacktivist	39

	Verlust in Euro
Kompromittierung von E-Mails	1 586 205 079
Vertrauens- / Liebesbetrug	424 119 671
Spoofing	268 284 315
Investment / Vermögensanlage	198 380 531
Real Estate / Miete	197 648 135
Nicht-Zahlung / Nicht-Lieferung	175 503 122
Identitätsdiebstahl	143 130 169
betrügerische staatl. Imitation / Personifikation	110 975 541
persönliche Datenpanne	107 234 376
Kreditkartenbetrug	99 545 681
Erpressung / Wucher	95 981 211
erweiterte Gebühren	89 823 479
andere	59 127 821
Phishing / Vishing / Smishing * / Pharming	51 639 624
Überzahlung	49 839 475
technischer Support	48 250 940
Datenpanne im Unternehmen	47 677 034
Lotterie, Wettspiel, Erbschaft	43 430 654
Arbeit / Anstellung	38 052 415
Zivilangelegenheiten	18 073 988
Belästigung / Gewaltandrohung	17 738 084
Falschdarstellung / Falschangaben	11 046 047
IPR / Copyright und Fälschung	9 190 453
Ransomware (Erpressungssoftware)	8 005 221
DoS / TDoS	6 784 105
Wohltätigkeitsstiftungen	1 977 128
Malware / Scareware / Virus	1 793 856
Re-Shipping	1 582 761
Glücksspiel	1 301 891
Bezug zum Gesundheitswesen	1 007 891
Kriminalität gegen Kinder	870 813
Hacktivist	115 179
Terrorismus	44 276

* Phishing per SMS. ** Business E-Mail Compromise (BEC) und E-Mail Account Compromise (EAC). Quelle: FBI, Internet Crime Complaint Center, US Department of Justice

Vertrauliche Daten

Datengefährdung in Unternehmen nach Region; weltweit; 2019; in Prozent

* Exponierte Daten sind Dateien und Ordner, auf die jeder Mitarbeiter Zugriff hat. Quelle: Varonis

Steigende Ausgaben

Durchschnittliche Jahresausgaben für Cybersicherheit nach Unternehmensgröße; ausgewählte Länder*; 2019; in Euro

1 bis 9 Mitarbeiter	6 250
20 bis 49 Mitarbeiter	33 036
50 bis 99 Mitarbeiter	102 679
100 bis 249 Mitarbeiter	389 286
250 bis 499 Mitarbeiter	830 357
500 bis 999 Mitarbeiter	908 929
1 000 bis 4 999 Mitarbeiter	2 085 714
5 000 bis 19 999 Mitarbeiter	3 579 464
mehr als 20 000 Mitarbeiter	9 502 679

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

Gefährdete Banken

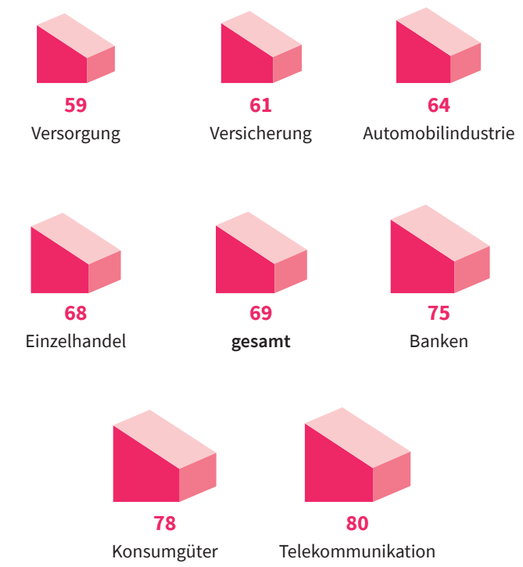
Datengefährdung in Unternehmen nach Industrien; weltweit; 2019; in Prozent

* Exponierte Daten sind Dateien und Ordner, auf die jeder Mitarbeiter Zugriff hat.
Quelle: Varonis

Nützliche Intelligenz

Nutzung von künstlicher Intelligenz zur Abwehr von Cyberattacken nach Branchen; Befragung von Führungskräften in ausgew. Ländern *; 2019; in Prozent

„Wir wären ohne künstliche Intelligenz nicht in der Lage, uns gegen Cyberattacken zu verteidigen."



* Frankreich, Deutschland, Großbritannien, USA, Australien, Niederlande, Indien, Italien, Spanien und Schweden. Quelle: Capgemini

Durchschnittliche Kosten

Durchschnittliche Kosten von Cyberattacken in Unternehmen; ausgewählte Länder; 2019; in Tausend Euro

	Kosten von allen Cyberattacken	Kosten der größten einzelnen Cyberattacken
Deutschland	809	441
Belgien	434	263
Niederlande	339	163
Großbritannien	217	120
Spanien	167	70
USA	106	65
Frankreich	98	44

Quelle: Hiscox

Klare Ziele

Prozentuale Verteilung von Cyberattacken auf Unternehmen nach Industrie *; weltweit; 2019; in Prozent

Professional **	23,3
unbekannt	21,8
öffentlicher Sektor	21,4
Information	17,1
Finanzen	4,7
Produktion / Herstellung	2,9
Bildung	2,6
Gesundheitswesen	2,5
Einzelhandel	0,9
Unterhaltung	0,6
Versorgung	0,5
Beherbergung	0,4
Transport	0,3
andere Dienstleistungen	0,3
Bergbauindustrie	0,1
Baugewerbe	0,1
Immobilien	0,1
Landwirtschaft	0,1
Management	0,1
Administration	0,1
Handel	0,1

* Die Branchen basieren auf NAICS-Codes. ** Für „Professional" gibt es kein deutsches Pendant. Darunter fallen Dienstleistungen von Juristen, Steuerberatern, Architekten sowie aus den Bereichen IT, Consulting, Marketing und Medien.
Quelle: Verizon

Entgangene Umsätze

Entgangener Umsatz durch Cyberangriffe nach Branchen; Schätzung auf Basis von 4 700 börsennotierten Unternehmen; weltweit; 2019; in Milliarden Euro

Hightech	672
Biowissenschaften	573
Automobilindustrie	451
Konsumgüter und Dienstleistungen	344
Banking	310
Gesundheit	310
Einzelhandel	304
Versicherung	272
Maschinenbau	253
Kommunikation und Medien	229
Natürliche Ressourcen	199
Versorgerunternehmen	196
Energie	184
Chemie	131
Transport	98
Reisen	63
Kapitalmärkte	42

Quelle: Accenture

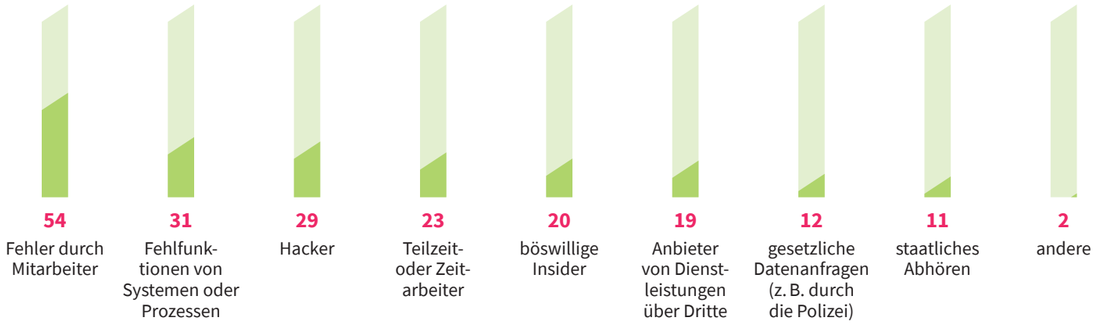
Betroffene Unternehmen

Anteil der Unternehmen mit mehr als 10 Mitarbeitern, die mindestens einmal Probleme aufgrund eines IKT-bezogenen Sicherheitsvorfalls * hatten; EU; 2019; in Prozent

* Nichtverfügbarkeit von Informations- und Kommunikationstechnik-Diensten (IKT), Zerstörung oder Beschädigung von Daten, Offenlegung von vertraulichen Daten.
Quelle: Eurostat

Häufigste Bedrohungen

Häufigste Bedrohungen für sensible oder vertrauliche Daten; IT-Experten; weltweit; 2019; in Prozent



Quellen: Ponemon Institut; Thales Group; nCipher Security

Verhängte Bußgelder

Die höchsten Bußgelder für Datenschutz-Verstöße; weltweit; 2019 / 2020 *; in Euro

4 536 999 350
USA
Facebook Inc.
24.7.2019
Verstoß gegen frühere FTC-Datenschutzanordnungen und Gesetz der Federal Trade Commission

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

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

67 487 768
USA
Capital One
6.8.2020
Fehlende Sicherheitsmaßnahmen ermöglichten Hackern Zugriff auf Daten von mehr als 106 Mio. Kreditkartenkunden.

60 000 000
Frankreich
Google LLC
9.12.2020
Einsatz von Tracking-Cookies zu Werbezwecken ohne Einwilligung der Betroffenen und fehlende Datenschutzhinweise

50 000 000
Frankreich
Google LLC
21.1.2019
Verstoß gegen zahlreichen Datenschutzgrundsätze (Transparenz, Zweckbindung …)

40 000 000
Frankreich
Google Ireland Limited
09.12.2020
Einsatz von Tracking-Cookies zu Werbezwecken ohne Einwilligung der Betroffenen und fehlende Datenschutzhinweise

35 258 708
Deutschland
H&M Online Shop
1.10.2020
Bespitzelung Hunderter Mitarbeiter des Service Centers Nürnberg

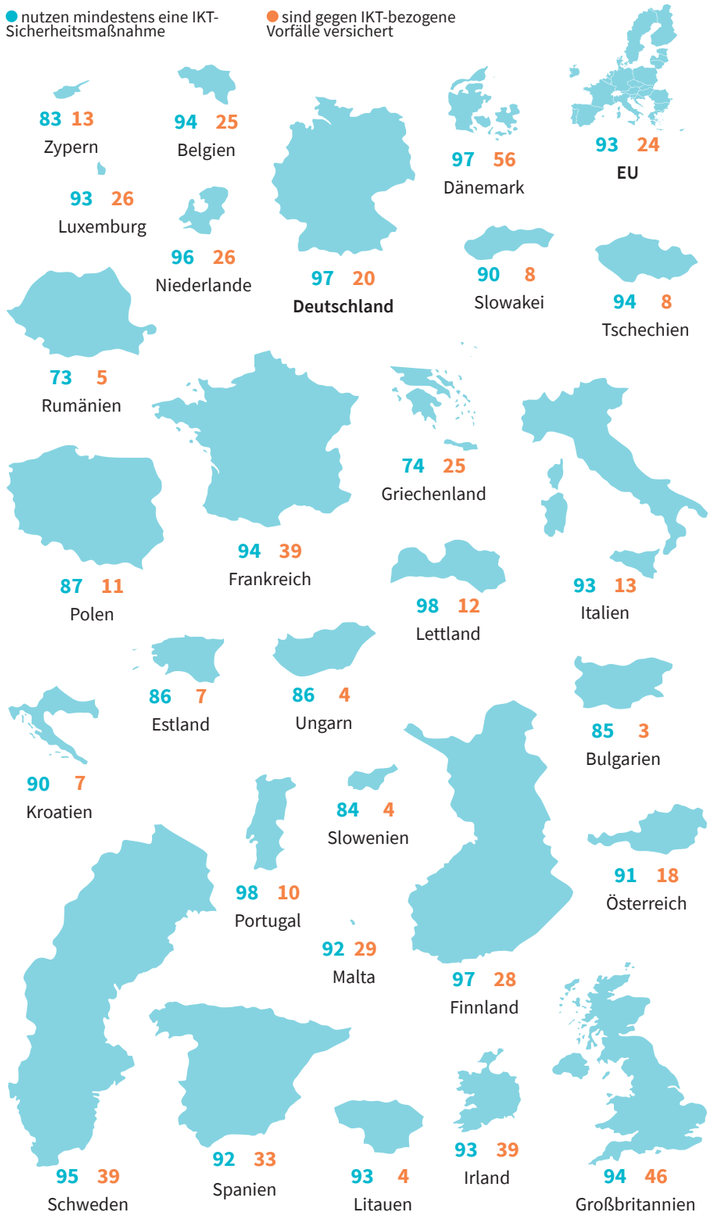
35 000 000
Frankreich
Amazon Europe Core
9.12.2020
Einsatz von Tracking-Cookies zu Werbezwecken ohne Einwilligung der Betroffenen und fehlende Datenschutzhinweise

27 802 946
Italien
TIM SpA
15.1.2020
Mehrere Millionen Werbeanrufe ohne Einwilligung, Informationsmängel in Apps und unzureichende TOMs (technische u. organisatorische Maßnahmen)

* Datenabruf am 2.8.2021. Quelle: DSGVO-Portal

Selten versichert

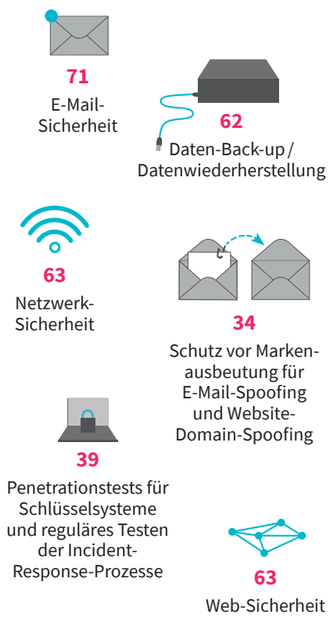
IKT-Sicherheit * in Unternehmen mit mindestens 10 Beschäftigten; EU; 2019; in Prozent



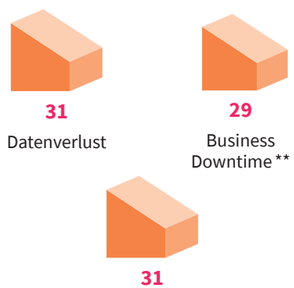
* IKT = Informations- und Kommunikationstechnik. IKT-Sicherheit umfasst Maßnahmen, Kontrollen und Verfahren, die auf IKT-Systeme angewandt werden, um die Integrität, Authentizität, Verfügbarkeit und Vertraulichkeit von Daten und Systemen zu gewährleisten. Quelle: Eurostat

Typisch aufgestellt

Übliche Bestandteile einer Cyber-Resilienz-Strategie; Entscheider aus der IT; ausgewählte Länder *; 2020; in Prozent



Folgen bei mangelnder Vorbereitung im Bereich Cyber-Resilienz



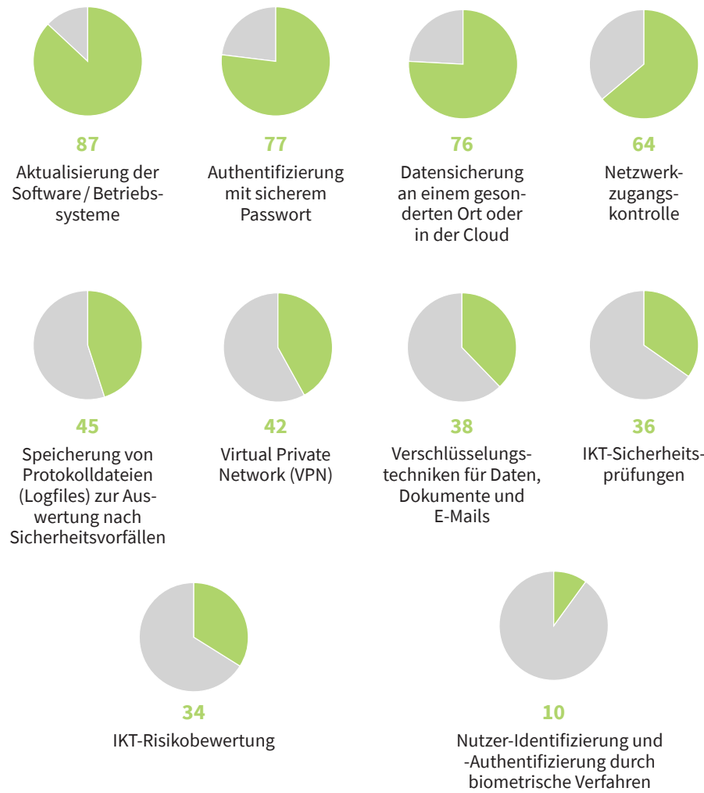
* USA, Großbritannien, Deutschland, Niederlande, Australien, Südafrika, Vereinigte Arabische Emirate und Saudi-Arabien. ** Die Business Downtime gibt die Zeit an, in der ein System während einer Umstellung für den produktiven Geschäftsbetrieb nicht zur Verfügung steht. Quelle: Mimecast

Mäßig vorbereitet

IKT-Sicherheit * in Unternehmen mit mindestens 10 Beschäftigten; EU; 2019; in Prozent

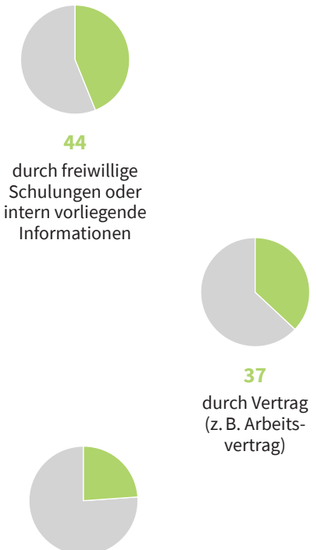
Ähnlich strukturiert

Nutzung von IKT-Sicherheitsmaßnahmen * in Unternehmen mit mindestens 10 Beschäftigten; EU; 2019; in Prozent



Kaum informiert

Unternehmen mit mindestens 10 Beschäftigten, die ihre Beschäftigten auf Verpflichtungen bzgl. IKT-Sicherheit * hinweisen; EU; 2019; in Prozent

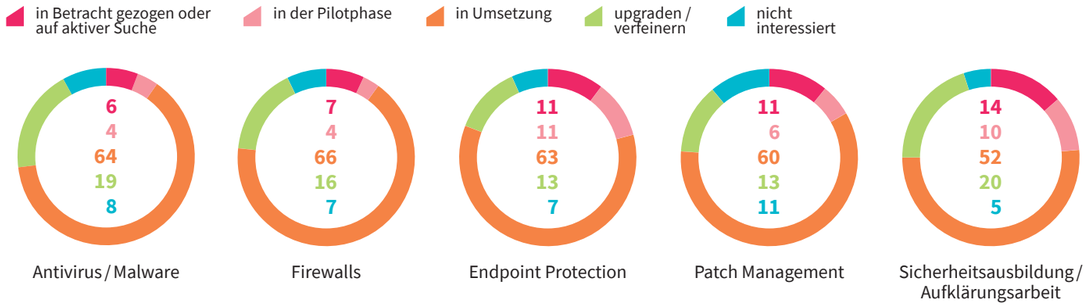


* IKT = Informations- und Kommunikationstechnik. IKT-Sicherheit umfasst Maßnahmen, Kontrollen und Verfahren, die auf IKT-Systeme angewandt werden, um die Integrität, Authentizität, Verfügbarkeit und Vertraulichkeit von Daten und Systemen zu gewährleisten. Quelle: Eurostat

Wie IT-Experten ihre Unternehmen schützen

Nutzung von Sicherheitslösungen in Unternehmen; Entscheider im Bereich IT und Unternehmenssicherheit; weltweit; 2019; in Prozent

„Welche Option beschreibt Ihre derzeitige Aktivität für jede der folgenden Sicherheitslösungen?“



Quelle: IDG Research Services

Was IT-Experten in ihren Unternehmen planen

Entwicklung der Ausgaben für Sicherheitsaufklärung und -bewertung; Entscheider im Bereich IT- und Unternehmenssicherheit; weltweit; 2019; in Prozent

„Beschreiben Sie, wie sich die Ausgaben für die folgenden Bereiche in den nächsten 12 Monaten ändern werden.“

	steigen	bleiben gleich	sinken	Das ist eine neue Kategorie für uns	potenzieller zukünftiger Bereich für Investments
Sicherheitsausbildung / Aufklärungsarbeit	38	54	3	2	3
Dienstleistungen zur Sicherheitsbewertung	38	50	4	4	3
cloud-basierte Cyber-Security-Dienstleistungen	38	40	2	10	10
Authentifizierung	36	53	3	4	4
Zugangskontrollen (Netzwerk, Daten)	36	57	2	1	4
Cloud-Datenschutz	33	41	1	11	14
Verhaltens-Monitoring & Analysen	33	40	2	11	14
Endgeräteerkennung und -reaktion	31	57	2	4	5
Big Data Analytik	30	39	2	11	17
Identitätsmanagementsysteme	29	56	2	5	8
Managed Security Service Providers (MSSPs)	29	52	4	6	10

Quelle: IDG Research Services

Kommt vielleicht

Entwicklung der Nutzung von Security „as a Service“ Lösungen; IT-Entscheider; Europa und Nordamerika; 2019; in Prozent

	wird derzeit genutzt	wird möglicherweise innerhalb der nächsten zwei Jahre genutzt
Endpoint Protection	28	17
Gefährdungsschutz	19	20
Angriffserkennung und -schutz	12	23
Schutz vor Datenverlust	11	22
Identitäts- und Zugangsmanagement	9	19
Verschlüsselung	8	15
Schwachstellenmanagement	6	22
Security Information Event Management	4	18
Security Operations Center	4	16

Quelle: Spiceworks

Kostet im Schnitt

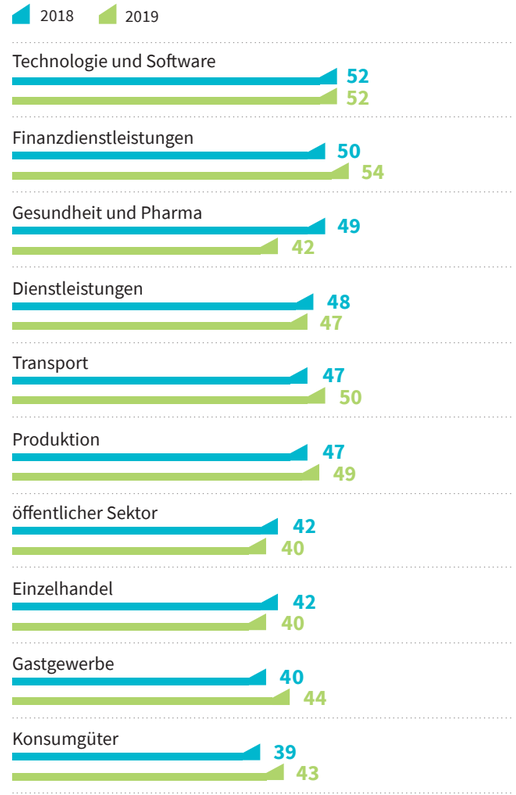
Anteile der verschiedenen Bereiche am IT-Sicherheits-Budget; Entscheider im Bereich IT und Unternehmenssicherheit; weltweit; 2020; in Prozent

ausgebildete Mitarbeiter	23
On-Premises Infrastruktur und Ausstattung (Hardware)	19
On-Premises Tools und Software (Software)	17
Cloud-basierte Sicherheitslösungen	12
Beratungsdienstleistungen	8
cloud-basierte Sicherheitsüberwachungslösungen	7
vertraglich vereinbarte Bewertungsdienstleistungen	6
externe Dienstleister zur Reaktion auf Zwischenfälle	5
andere (Reisen, Konferenzen usw.)	3

Quelle: IDG Research Services

Verschlüsselt

Unternehmensweite Nutzung von Verschlüsselungslösungen nach Branche; IT-Experten; weltweit; in Prozent



Quellen: Ponemon Institute, Thales Group, nCipher Security

Treibt

Treiber für die Nutzung von Verschlüsselungslösungen in Unternehmen; IT-Experten; weltweit; in Prozent

	2018	2019	Veränderung 2018 – 2019
zum Schutz des geistigen Eigentums	54	52	– 3,7 %
zum Schutz von persönlichen Kundeninformationen	54	54	0,0 %
zum Schutz von Informationen gegen spezifische, identifizierte Bedrohungen	51	51	0,0 %
um die externe Privatsphäre oder Datensicherheits-Regularien und -Anforderungen zu erfüllen	46	47	2,2 %
um den Umfang von Compliance Audits zu reduzieren	31	29	– 6,5 %
um die Verantwortlichkeit nach Datenpannen und unbeabsichtigter Datenoffenlegung zu reduzieren	29	28	– 3,4 %
um die internen Richtlinien zu erfüllen	21	23	9,5 %
um die Veröffentlichung von Daten nach einer Datenpanne zu verhindern	14	15	7,1 %
unsicher	–	1	k. A.

Quellen: Ponemon Institute, Thales Group, nCipher Security

computer-jennifer 12345678-baseball-computer-trustno1-Mehr-als football-sunshine-corvette-1234-ein-technisches qwertyuiop-superman-baseball-Problem worldcup-1qaz2wsx-starwars 1234567890-iloveyou-jennifer 1111111-geheim-meinpasswort-beatles baseball-startrek-football-987654321 iloveyou-michelle-trustno1-qwertyuiop-sunshine

Viele Menschen wissen inzwischen, wie IT-Sicherheit geht.
Und ignorieren es.
Warum eigentlich?

Text: Sarah Sommer

123456.

Ja, eigentlich wissen wir, dass das kein kluges Passwort ist. Trotzdem wählen sehr, sehr viele Menschen immer noch so eine simple Lösung, um ihre digitalen Konten und Profile zu schützen. Das zeigen auch alljährlich die Listen der beliebtesten Passwörter: Zahlenreihen, „hallo“, „password“ oder „passwort“ und „iloveyou“ oder „ichliebedich“ sind ähnlich beliebt wie Namen oder einfache englische Begriffe wie „killer“ oder „dragon“. Und das, obwohl wir uns das Augenrollen der IT- und Datenschutz-Experten, ihr entnervtes Kopfschütteln genau vorstellen können.

Das ungute Gefühl, unser digitales Arbeits- und Privatleben nicht im Griff zu haben, stellt sich aber ebenso ein, wenn wir es eigentlich richtig machen wollten, dann aber mal wieder Anmeldedaten mit einem supersicheren zehnstelligen Passwort mit Sonderzeichen, Zahlen sowie groß- und kleingeschriebenen Buchstaben vergessen haben. Oder wenn wir innerhalb von Sekunden gleich fünf nervige Cookie-Nachfragen wegklicken oder auf dem unsicheren Messenger über allzu Privates schreiben.

Natürlich ist uns klar, dass wir uns gegen Hacker, Phisher und datenhungrige Digitalplattformen absichern müssten – aber wir tun es oft nicht. Das geht so weit, dass viele Menschen Webseiten und digitale Services nicht mehr nutzen, wenn sie ihr Passwort vergessen haben. „Password Anxiety“ oder „Password Fatigue“ nennt sich das.

Doch woher stammt die Blockade? Warum bekommen wir oft keinen vernünftigen Umgang mit Cyber-Risiken hin? Wo liegt der Kern des Problems? Zu diesen Fragen forschen längst nicht nur IT-Experten. Auch Psychologinnen, Neurowissenschaftler, Technik-Ethikerinnen und Pädagogen fragen sich, was da los ist.

1. Die Entzauberin

Wie gehen wir mit den Risiken neuer Technologien sinnvoll um? Indem wir einsehen, dass wir mit unserer Risikoeinschätzung oft danebenliegen, sagt Rafaela Hillerbrand, Professorin für Technikethik und Wissenschaftsphilosophie am Karlsruher Institut für Technologie (KIT). Vor allem aber müssen wir damit aufhören, Technik als etwas Geheimnisvolles, Magisches zu betrachten.

Frau Hillerbrand, Sie erforschen, welche Folgen und Risiken Technologien mit sich bringen und wie die ethisch zu beurteilen sind. Können wir die Risiken der neuen digitalen Technologien, die wir im Alltag anwenden, überhaupt richtig einschätzen?
Ich fürchte, vielen Menschen fehlen die Voraussetzungen, um die aktuelle technische Entwicklung und ihre Folgen in ihrer ganzen Komplexität wirklich zu verstehen. Das Tempo der Veränderung ist gerade sehr hoch: Künstliche Intelligenz, Cloud-Technologie, neue digitale Plattformen für Kommunikation und Zusammenarbeit – all das gestaltet unser Leben spürbar um. Eigentlich müsste unser Bildungswesen und die Politik den Menschen die nötigen Kompetenzen und Rahmenbedingungen vermitteln, um damit umzugehen, aber die kommen bei dem Tempo nicht hinterher.

Welche Risiken entstehen dadurch?
Wenn wir die Technik und damit die Maschinen, mit denen wir interagieren und die unseren Alltag bestimmen, nicht verstehen, sind sie für uns letztlich pure Magie. Technik darf aber nichts Magisches, Geheimnisvolles sein. Das ist gefährlich, denn es führt dazu, dass wir Risiken und Chancen falsch einschätzen und uns inkonsistent verhalten. In der Risikoforschung sprechen wir von Heuristics and Biases, also von kognitiven Verzerrungen, von Voreingenommenheiten, die vor allem dann auftreten, wenn wir wissen: Es gibt ein Risiko, eine Gefahr – die aber nicht mit Sicherheit eintritt.

Wo verschätzen wir uns denn bei den Risikoanalysen?
Ein Beispiel: Eine Person weiß, dass es Passwort-Hacks gibt und die Folgen gravierend sein können – aber sie treten selten auf. Also fängt sie an abzuwägen: Wie viel Zeit und Energie wende ich auf, um mich zu schützen?

Da gibt es typischerweise so etwas wie einen Ankereffekt: Ich orientiere mich daran, was andere in meinem Umfeld tun. Oder ich gehe davon aus, dass die Zukunft der Vergangenheit ähnelt: Es ist noch nie etwas passiert – also wird das auch in Zukunft so sein. Mit einer rationalen Risikoanalyse hat das wenig zu tun.

Wie geht man mit so einem irrationalen Verhalten um, wenn man neue Technologien entwickelt oder einsetzt?
In der technischen Risikofolgenabschätzung arbeitet man zum Beispiel mit Szenarien, denn eine Technologie ist nicht allein dadurch sicher, dass es Sicherungsmechanismen gibt. Es gilt, Szenarien durchzuspielen, in denen Menschen diese Sicherungsmechanismen nicht oder falsch nutzen.

Ein Teil der Aufgabe ist es also, prospektiv auch anderes oder irrationales Verhalten einzubeziehen: Was könnte man falsch machen? Das muss ich als Unternehmen, das eine Technologie einsetzen will, ebenso in meine Überlegungen einbeziehen wie als Politiker, der den Umgang mit einer Technologie regulieren will.

Strenge Sicherheitsmaßnahmen, die digitalen Risiken vorbeugen, sind in der Regel nicht sehr beliebt: In Unternehmen wird oft über die strenge IT-Sicherheit geschimpft. Und die DSGVO, die uns Sicherheitsmaßnahmen wie etwa die Cookie-Hinweise beschert hat, ist für viele auch ein rotes Tuch.
Letztlich zeigt sich immer wieder, dass rein technische Lösungen ihre Grenzen haben. Am Ende stecken systemische, gesellschaftliche Fragen dahinter.

Man muss sich fragen, wie die Randbedingungen unseres Verhaltens aussehen. Kann ich zum Beispiel in unserer schnell getakteten Gesellschaft und Arbeitswelt wirklich verlangen, Cookie-Richtlinien bis zum Ende zu lesen? Oder dass man einen umständlichen, aber sicheren E-Mail-Client nutzt statt des komfortablen Angebots eines Tech-Konzerns?

Dafür bräuchte es wohl eine deutlich entschleunigte Gesellschaft. Solange wir die nicht haben, braucht es rechtliche Regelungen, die für mehr Sicherheit für „gewöhnliche User“ im IT-Bereich sorgen.

Foto: privat

2. Der Profiler

Christian Montag ist Professor für Molekulare Psychologie. Er forscht im Bereich der Psychoinformatik und Neuroökonomie. An der Universität Ulm untersucht er, wie sich Genetik und Umwelt auf die Persönlichkeit auswirken und wie die Persönlichkeit das Verhalten in der digitalen Welt beeinflusst.

Einen grundsätzlichen Zusammenhang zwischen den Persönlichkeitsprofilen von Menschen und ihrem Digitalverhalten gibt es auf jeden Fall, sagt er: „Zeig mir deine digitalen Spuren, und ich sage dir, wer du bist. Zeig mir dein Persönlichkeitsprofil, und ich sage dir, wie du mit digitalen Medien umgehst, welche Risiken du online eingehst oder ob du Tendenzen zu suchtartigem Verhalten im Umgang mit Social Media entwickelst.“

Persönlichkeit ist dabei eine von vielen Variablen, die das Digitalverhalten beeinflussen, und die Vorhersagen der Forscher sind noch fern ab von perfekt. Montag ist allerdings überzeugt: „Die Tech-Konzerne sind längst viel besser darin, unsere digitalen Spuren zu deuten, unser Verhalten vorherzusagen und unsere Persönlichkeit zu bewerten, als viele unabhängige Forscher.“ Das liege daran, dass die Tech-Kozerne auf gigantische Datenmengen zugreifen können und nahezu unbemerkt mit unserem Online-Verhalten experimentieren.

Analysen per Knopfdruck

Forscher wie Montag wollen auch deshalb verstehen, wie Persönlichkeit und Digitalverhalten zusammenhängen, weil uns diese Verbindung manipulierbar macht. Eine große Studie US-amerikanischer Forscher wertete etwa das Verhalten von mehreren Hunderttausend Facebook-Nutzerinnen aus, deren Daten in der insgesamt mehrere Millionen Datensätze umfassenden Datenbank des MyPersonality-Projektes erfasst sind. Die Wissenschaftler schätzten deren Persönlichkeitsstruktur ein, je nachdem, welchen Beiträgen sie ein Like gaben. Danach schickten sie ihnen Werbung, die an ihre aus dem Digitalverhalten abgeleitete Persönlichkeit angepasst war: Extrovertierte erhielten etwa Anzeigen mit fröhlich tanzenden Menschen, Introvertierte dagegen ruhige, nachdenkliche Werbebotschaften.

Die Klick- und Kaufraten erhöhten sich signifikant, berichtet Montag: „Das war eine der ersten wissenschaftlichen Studien, die den Effekt solch eines persönlichkeitsgetriebenen Microtargetings nachgewiesen hat.“ Und die Plattformen müssten so eine Studie nicht über Monate durchführen – die testen das per Knopfdruck. Anlässe und Motive für digitale Persönlichkeitsanalysen gibt es viele: Werbetreibende wollen Produkte verkaufen, Online-Plattformen oder -Medien dafür sorgen, dass sich Nutzer möglichst lange mit ihren Angeboten beschäftigen.

Auch Cyberkriminelle interessieren sich für unsere Persönlichkeitsstruktur. Denn die kann sich auch darauf auswirken, wie stark wir bei der Nutzung digitaler Dienste auf Sicherheit achten. Wann klicken wir auf einen Link in einer Mail oder ein Bild in unserem Social-Media-Stream? „Studien zeigen, dass unser Wissen über bestimmte Risiken und Schutzmöglichkeiten unser Verhalten nur in geringem Umfang beeinflusst“, sagt Montag. Theoretisch zu wissen, wie ein starkes Passwort aussieht und wozu Cookie-Hinweise gut sind, schützt nicht vor Fehlverhalten.

Einen Effekt scheint die Persönlichkeitsstruktur zu haben. „Wir arbeiten mit sogenannten OCEAN-Persönlichkeitsprofilen“, sagt Montag. Dabei schätzen sich Menschen mit Blick auf fünf Persönlichkeitsmerkmale ein: Offenheit, Gewissenhaftigkeit, Extraversion, Verträglichkeit und Neurotizismus. In einer Fragebogen-Studie zeigte sich, welche Merkmale mit einem bestimmten Verhalten einhergehen. „Man kann zum Beispiel sehen, dass unter anderem Menschen mit höheren Offenheitswerten eher einen sicheren Messenger wie Signal nutzen, weil ihnen Whatsapp zu unsicher ist“, sagt Montag. Dagegen machen Menschen, die vor allem „verträglich“ sind, eher Kompromisse und nutzen mehrere Messenger gleichzeitig, um allen gerecht zu werden.

„Wie konsequent ich auf Sicherheit und Datenschutz achte, hat letztlich auch damit zu tun, wie gut ich mit meiner kognitiven Dissonanz umgehen kann“, sagt Montag. Das heißt: Ich weiß eigentlich, wie riskant ein Verhalten ist, und kann es ändern, tue es aber nicht, etwa weil der Digitaldienst so praktisch ist. Und ja schließlich auch viele andere auf der Plattform unterwegs sind. Das Problem so kleinzureden ist eine Möglichkeit, die kognitive Dissonanz zu reduzieren. „Andere wiederum tun das durch den Wechsel zu einem anderen Messenger und nehmen bewusst in Kauf, dass sie dort vielleicht noch nicht mit so vielen anderen Menschen verbunden sein können.“

Am Ende sollte es aber keine Frage der Persönlichkeit sein, wie gut sich jemand im digitalen Alltag schützen kann, meint Montag: „Das Kernproblem ist und bleibt, dass Menschen allzu oft mit ihren Daten für die Nutzung digitaler Dienste zahlen. Je mehr dieser Daten im Umlauf sind, desto besser können interessierte Akteure uns manipulieren.“

3. Der Begleiter

Kai Schmidt ist Schulleiter der Oberschule Uelsen in Niedersachsen. Als Mathelehrer kennt er sich damit aus, wie man Schüler zu etwas motiviert, das ihnen kompliziert erscheint und auf das sie keine Lust haben. Ihm gelingt das mit einfachen Erklärvideos, die er bei Youtube einstellt – so wurde er zum „Mathe-Influencer". Sein Kanal Lehrerschmidt hat mehr als eine Million Abonnenten.

Foto: privat

Herr Schmidt, auf Ihrem Kanal schaffen Sie es, das unbeliebte Thema Mathe unterhaltsam aufzubereiten. Das geht schon bei den Titeln los: „streng geheime Tricks der Mathelehrer", „superschnell – genialer Rechentrick!" oder „Geheim!!! Multiplizieren – die Lehrervariante". Könnte man Schüler so auch dazu bewegen, sich mit anderen trockenen und mühsamen Themen zu beschäftigen wie etwa mit digitalen Sicherheitsregeln?

Es ist immer gut, wenn wir uns gemeinsam mit den Schülerinnen und Schülern in der digitalen Welt aufhalten. Natürlich kommen auch Expertinnen in die Schule und erzählen Kindern und Jugendlichen etwas über Datenschutz, Fake News auf digitalen Plattformen oder darüber, wie gute Passwörter funktionieren. Im Unterricht, in Deutsch oder Politik zum Beispiel, ist das auch ein Thema.

Aber vieles lernen die Schülerinnen und Schüler viel eindrücklicher, wenn etwa der Instagram-Account eines Klassenkameraden gehackt wird. Oder zuletzt durch die Diskussionen darüber, welche Videokonferenz-Software sie während der Pandemie in der Schule nutzen durften.

Wobei ich sagen muss: Obwohl sie gut gemeint waren, waren die IT-Sicherheits-Regeln, die wir in den Schulen zu Beginn der Pandemie hatten, oft ziemlich unrealistisch.

An vielen Schulen darf wegen Datenschutzbedenken keine Software von Anbietern wie Microsoft verwendet werden. Sie dagegen stellen Ihre Videos auf Youtube und diskutieren dort auch mit Schülern. Gibt das keinen Ärger?

Nein, die Videos sind ein freiwilliges Angebot. Und die Schüler halten sich ohnehin dort auf, sie verbringen einen großen Teil ihrer Freizeit auf solchen digitalen Plattformen. Da ist es besser, man ist dort auch ansprechbar und zeigt den Schülerinnen und Schülern, dass man diese Medien auch zum Lernen nutzen kann.

Ich denke generell, dass man mit Aufklärung weiter kommt als mit einem Verbot aus Sicherheitsgründen. Der Bedarf, Datenschutz und digitale Sicherheit an der Schule zum Thema zu machen, ist ganz klar da – aber Zeit, Ressourcen und entsprechende Fortbildungen sind es bisher leider nicht in ausreichendem Maße.

Sind denn die Lehrerinnen und Lehrer bereit, sich mit diesen Fragen auseinanderzusetzen?

Das ist sehr unterschiedlich, es sind sicher nicht alle digital-affin. Und oft gibt es wirklich berechtigte Unsicherheiten, weil die Rechtslage unklar ist: Was darf ich und was nicht? Insgesamt habe ich aber das Gefühl, die Bereitschaft, digital zu arbeiten, wird größer. Und dabei lernen alle dazu.

Vor ein paar Jahren mussten wir noch fünf- bis sechsmal pro Woche ein Lehrer-Passwort für die Schul-Server zurücksetzen – jetzt passiert das immer seltener, weil sich alle viel selbstverständlicher und regelmäßiger im digitalen Schulumfeld bewegen. Jeder kann jetzt eine Videokonferenz starten, PDFs erstellen und verschicken – das gehört einfach zum Alltag.

Für die Schüler ist das super: Wenn sie erwachsene Vorbilder haben, die ihnen vorleben, wie man selbstbewusst und sicher digital unterwegs ist, bewirkt das mehr als jede IT-Sicherheit-Aufklärungsstunde.

4. Die Befähigerin

Martina Sasse forscht und lehrt als Professorin am University College London und an der Ruhr-Universität Bochum zum Thema Human-Centred Security. Der Begriff der menschlichen Sicherheitslücke, sagt sie, bringt sie auf die Palme.

„Sagen Sie mal, Sie als Psychologin verstehen doch was von Menschen! Machen Sie doch mal eine Studie, warum unsere Mitarbeiter sich nie ihre Passwörter merken können! So fing das an, damals in den Neunzigern. Und am Ende musste ich dem Unternehmen erklären, dass sich kein Mensch achtstellige Passwörter und sechsstellige Kennwörter für mindestens 16 verschiedene IT-Systeme merken kann, die jeden Monat gewechselt werden. Nein, sorry, das ist absurd! Selbst Gedächtniskünstler müssten täglich eine halbe Stunde trainieren, um alle Zahlen parat zu haben. Werden die Mitarbeiter dafür bezahlt oder freigestellt? Nein, ich denke nicht. Leider gibt es diese Art überkomplexer Sicherheitssysteme heute immer noch in ganz vielen Unternehmen. Über Jahre oder Jahrzehnte gewachsene IT-Systeme werden oft mit der Zeit immer komplexer. Wer sich da nicht traut, ganz grundsätzlich ranzugehen und Systeme neu aufzusetzen, muss ständig an allen Ecken und Enden Sicherheitslücken schließen.

Das Problem ist: Wenn Sicherheit für Menschen nicht anwendbar ist, bringt sie nichts. Es ist Unsinn, zu sagen: Die Schwachstelle Mensch killt unser schönes Sicherheitssystem. Das regt mich wirklich auf, diese Phrase von der menschlichen Schwachstelle gehört verboten! Seit den Neunzigern sage ich: Leute, die Nutzer sind keine Feinde. Und Institute wie das National Cyber Security Centre in Großbritannien und die Agentur der Europäischen Union für Cybersicherheit, ENISA, betonen seit Jahren, dass dieses Denken viel Schaden anrichtet. Aber die Command-and-Control-Sicht, die Sicherheitstechnik einsetzt, um „das System" zu schützen, und dann den einzelnen Mitarbeitern ihre Aufgaben bei dieser Mission zuteilt, ist immer noch sehr verbreitet. Wer dann die ihm zugewiesene Aufgabe nicht erfüllt, hat die Anweisungen nicht richtig befolgt und somit versagt. Diese Sichtweise ist auch deshalb so verbreitet, weil die IT-Teams in Unternehmen bis heute nicht sehr divers besetzt sind. Das sind häufig sehr homogene Gruppen, die bisweilen so etwas wie eine Stammes-Mentalität entwickeln: Wer hat die meisten, stärksten, drakonischsten Sicherheitsmaßnahmen?

Ich fürchte, so viele Menschen verbinden mit IT-Sicherheit inzwischen Angst, Stress und Überforderung, dass wir dringend ein Re-Branding, einen Imagewechsel brauchen. In Unternehmen könnte das gelingen, wenn die IT enger zusammenarbeitet mit den Personalabteilungen, den Kommunikatoren und dem Management. Die sind ohnehin damit beschäftigt, bestimmte Werte und Verhaltensweisen ins Unternehmen zu tragen. Gerade die Kommunikationsleute arbeiten dabei mit Bildern und Storys, die vielleicht eher verstanden werden als eine klassische Rundmail aus der IT in hochtechnologischer Fachsprache.

Und die Sicherheitsleute müssen lernen, sich in den Austausch über Werte und erwünschtes Verhalten einzuklinken und in einen echten Dialog mit den einzelnen Mitarbeitern und Teams zu treten. Wenn dann jemand sagt: ‚Sorry, aber eure Sicherheitsprozesse kosten uns jeden Tag eine Stunde Arbeitszeit, das ist zu viel!' – muss man darüber ernsthaft reden und die Prozesse anpassen. Wenn das nicht geht, ist im IT-System etwas falsch, nicht bei den Mitarbeitern. Dieser Gedanke ist leider immer noch wenig verbreitet. Aber ein Umdenken ist notwendig: Die Angreifer sind innovativ und klug, sie finden Schwachstellen vor allem durch Social Engineering, also indem sie bei menschlichen Schwächen ansetzen, zum Beispiel bei Vermeidungsstrategien, die Mitarbeiter entwickeln, wenn ihnen die IT unrealistische Vorgaben macht.

Wirklich schützen können sich Unternehmen langfristig nur, wenn sie das nicht als rein technisches Problem sehen. Sie müssen ihre Mitarbeiter aus einer oftmals erlernten Hilflosigkeit und Tech-Angst holen. Es muss zur Corporate-Citizen-Kultur gehören, im Alltag regelmäßig darüber zu sprechen, wie man sich und das Unternehmen schützen kann. Interesse daran haben meiner Erfahrung nach alle Mitarbeiter. Wer lässt sich schon gern von irgendwelchen Cyber-Kriminellen manipulieren? Na eben: keiner!"

WIRTSCHAFT

Vom Mitarbeiter bis zum Geschäftsführer, vom Kleinstunternehmen bis zum Konzern: IT-Lösungen, IT-Budgets, Sicherheitsanalysen, Schutzmaßnahmen, Trainings, Zuständigkeiten, Schwachstellen, Risiko-Einschätzungen, Sensibilisierungsmaßnahmen, Infrastrukturen, Gefahren, Sicherheitslücken, Cyberangriffe, Kosten und Schäden.

Wie gut sind wir für den Ernstfall gerüstet?

Befragung von Unternehmen, Organisationen und Verbänden der Wirtschaft aller Branchen mit mindestens 3 Beschäftigten, die Homeoffice angeboten haben (n = 1 000); Deutschland; 2020; in Prozent

Umsetzung organisatorischer Sicherheitsmaßnahmen während der Corona-Krise *

2 / 11 / 7 / 17 / 64 — Mitarbeiter-sensibilisierung

7 / 20 / 13 / 13 / 47 — Notfall-management

7 / 20 / 14 / 7 / 52 — IT-Sicherheits-strategie

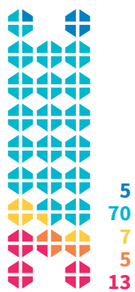
11 / 29 / 9 / 7 / 44 — Leitgedanke: Cybersicherheit ist Chefsache

7 / 47 / 11 / 6 / 29 — Beauftragung externer Informa-tionssicherheits-Dienstleister

9 / 49 / 12 / 7 / 24 — Etablierung eines Informations-sicherheits-Beauf-tragten

25 / 32 / 12 / 5 / 25 — ISMS (Informations-sicherheits-Managementsystem)

6 / 56 / 14 / 6 / 18 — regelmäßige Notfallübungen

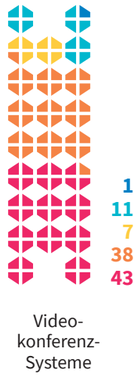


5 / 70 / 7 / 5 / 13 — Aufbau einer Abteilung „IT-Sicherheit“

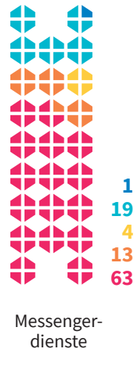
7 / 69 / 9 / 4 / 12 — Neueinstellung von Personal im IT-Sicherheits-bereich

bereits vor der Corona-Krise umgesetzt oder genutzt
in der Corona-Krise umgesetzt oder genutzt
Umsetzung oder Nutzung geplant
Umsetzung oder Nutzung bisher nicht geplant
weiß nicht

Eingesetzte IT-Lösungen während Corona mit Homeoffice-Bezug *



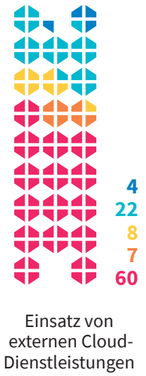
1 / 11 / 7 / 38 / 43 — Video-konferenz-Systeme



1 / 19 / 4 / 13 / 63 — Messenger-dienste

3 / 18 / 6 / 17 / 57 — Einsatz von Remote-Desktop-Tools

3 / 19 / 7 / 17 / 54 — Fernzugriff auf Unternehmens-ressourcen



4 / 22 / 8 / 7 / 60 — Einsatz von externen Cloud-Dienstleistungen

18 / 41 / 9 / 10 / 22 — Kollaborations-Tools für die dezentrale com-putergestützte Zusammenarbeit

Umsetzung technischer Sicherheitsmaßnahmen mit besonderer Relevanz für das Homeoffice *

5 / 21 / 8 / 11 / 55 — VPN (Virtual Private Network)

4 / 24 / 9 / 5 / 59 — Verschlüsselung von Datenträgern

8 / 28 / 12 / 10 / 42 — Mehr-Faktor-Authentisierung

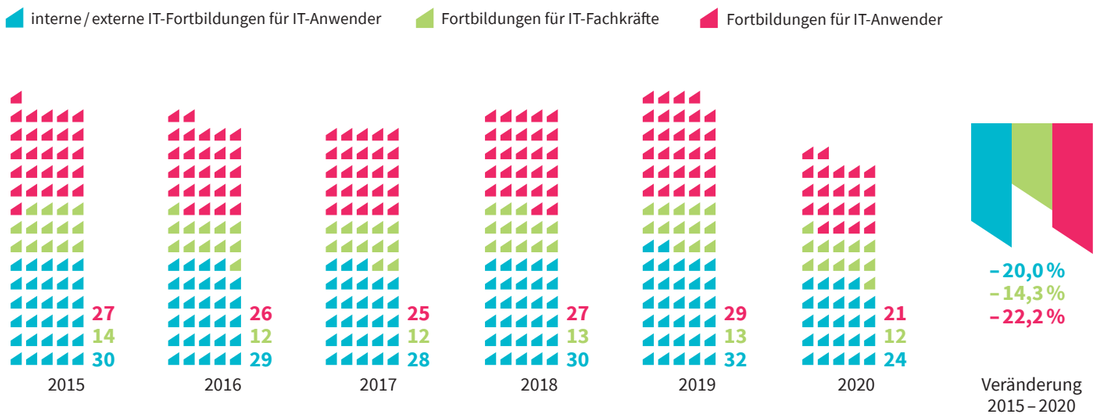
14 / 30 / 7 / 8 / 43 — Segmentierung und Absicherung von Netzen

19 / 31 / 12 / 9 / 29 — Mobile-Device-Management

* Gewichtung nach Branchen und Unternehmensgrößen. Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Schrumpft

IT-Fortbildungen in Unternehmen in Deutschland; in Prozent



Quelle: Statistisches Bundesamt

Beruhigt

Erledigung von IT-Aufgaben in Unternehmen in Deutschland; in Prozent

	2015	2016	2017	2018	2019	2020
Erledigung von IT-Aufgaben hauptsächlich durch externe Anbieter	53	53	k. A.	56	k. A.	42
Erledigung von IT-Aufgaben durch interne und externe Fachkräfte	19	19	k. A.	19	k. A.	33
Beschäftigung eigener IT-Fachkräfte	21	22	19	20	19	19
Erledigung von IT-Aufgaben hauptsächlich firmenintern	23	23	k. A.	19	k. A.	17

Quelle: Statistisches Bundesamt

Steigt

Zahl der Meldungen von KRITIS-Unternehmen *; Deutschland

2018	2019	2020
145	252	419

Veränderung 2018 – 2020: 189 %

* Kritische Infrastrukturen (KRITIS) sind Organisationen oder 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 eintreten würden. Im BSI-Lagebericht wird von rund 1700 registrierten KRITIS Anlagen gesprochen. Die dargestellten KRITIS-Meldungen beziehen sich nicht ausschließlich auf IT-Sicherheitsattacken, sondern beinhalten auch gemeldete IT-Störungen. Im Allgemeinen beurteilt das BSI die Situation als eine Gefährdungslage auf einem hohen Niveau. Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Ängstigt

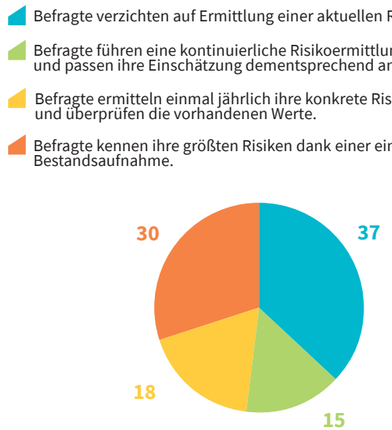
Zahl der Meldungen von KRITIS-Unternehmen nach Sektoren; Deutschland; 2020

Gesundheit	134
Information & Kommunikationstechnik	75
Energie	73
Finanzen und Versicherungen	65
Transport & Verkehr	56
Ernährung	9
Wasser	7
kerntechnische Anlagen	0

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Wir fühlen uns zu sicher …

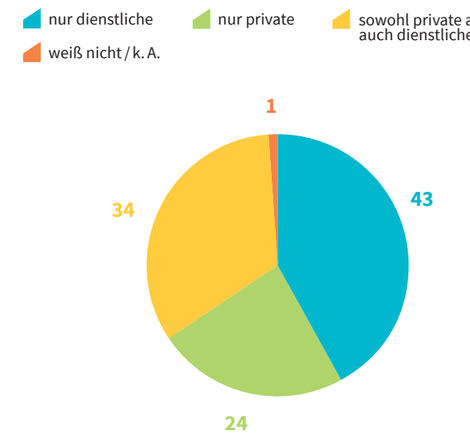
Ermittlung der aktuellen Risikosituation für den Bereich IT-Sicherheit; Befragung von Mitarbeitern und leitenden Angestellten in kleinen und mittleren Unternehmen * (n = 1 038); 2019 / 2020; in Prozent



* Kleinunternehmen: bis zu 50 Beschäftigte; mittlere Unternehmen: bis zu 500 Beschäftigte. Quelle: Deutschland sicher im Netz (DsiN)

… vermischen Job und Privat

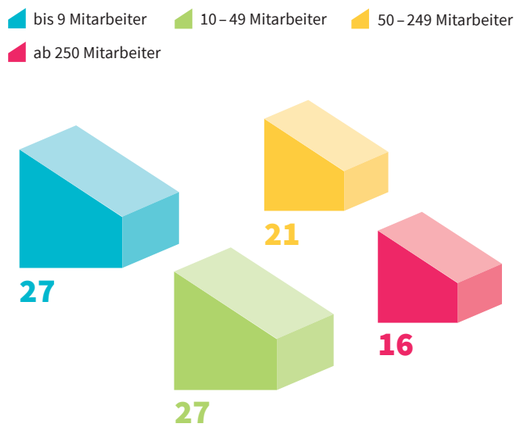
Nutzung von dienstlichen und privaten IT-Geräten im Homeoffice (während Corona); Befragte im Homeoffice (n = 891); Deutschland; 2020; in Prozent *



* Aufgrund von Rundungen können sich bei Summenbildungen geringfügige Abweichungen ergeben.
Quelle: Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GdV)

… geben unsere Daten preis

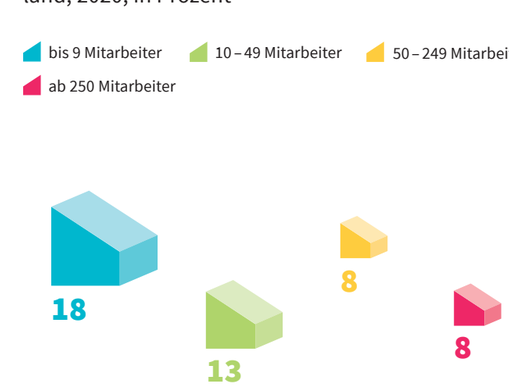
Nutzung von Whatsapp für die berufliche Kommunikation (während Corona); Befragte im Homeoffice (n = 891); Deutschland; 2020; in Prozent *



* Aufgrund von Rundungen können sich bei Summenbildungen geringfügige Abweichungen ergeben.
Quelle: Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GdV)

…und laden zu Missbrauch ein

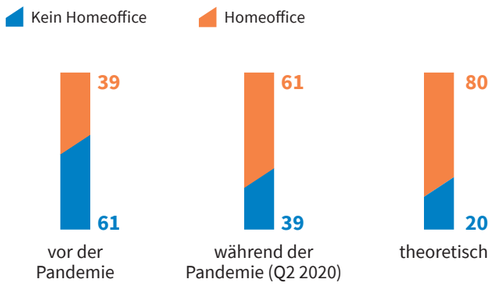
Nutzung der privaten E-Mail Adresse für dienstliche Dokumente und Mails (während Corona); Befragung von deutschen Arbeitnehmern (n = 2 011); Deutschland; 2020; in Prozent *



* Aufgrund von Rundungen können sich bei Summenbildungen geringfügige Abweichungen ergeben.
Quelle: Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GdV)

Im Homeoffice

Anteil der Belegschaft, die im Homeoffice arbeitet oder theoretisch arbeiten könnte; Befragung von deutschen Personalleitern (n = ca. 800); Deutschland; 2020; in Prozent



Quellen: Randstad, ifo Institut

Auf Tour

Verbreitung mobiler Arbeit in Deutschland (vor Corona) *; Befragung von zufällig ausgewählten abhängig Beschäftigten (n = 6 297); Deutschland; Januar – Mai 2020; in Prozent

mobile Arbeit	36
fester Arbeitsplatz	64

* Nicht berücksichtigt wurden Tätigkeiten, deren Zweck der Transport von Personen oder Gütern ist. Zusätzlich wurden die Teilnehmer gebeten, die Veränderungen durch Corona bei ihren Antworten nicht zu berücksichtigen.

Quelle: Deutscher Gewerkschaftsbund

Im Unternehmen

Hindernisse für das Arbeiten im Homeoffice (vor Corona) *; Befragung von zufällig ausgewählten abhängig Beschäftigten (n = 6 297); Deutschland; Januar – Mai 2020; in Prozent

Art der Arbeit lässt das nicht zu	61
betriebliche Regelung verhindert das	47
fehlende räumliche oder technische Voraussetzungen	43
Vorgesetzter möchte das nicht	37
Nachteile im Betrieb befürchtet	13

* Nicht berücksichtigt wurden Tätigkeiten, deren Zweck der Transport von Personen oder Gütern ist. Zusätzlich wurden die Teilnehmer gebeten, die Veränderungen durch Corona bei ihren Antworten nicht zu berücksichtigen.

Quelle: Deutscher Gewerkschaftsbund

Im Job

Nutzung von privaten Geräten als Arbeitsmittel (vor Corona) *; Befragung von zufällig ausgewählten abhängig Beschäftigten (n = 6 297); Deutschland; Januar – Mai 2020; in Prozent

* Nicht berücksichtigt wurden Tätigkeiten, deren Zweck der Transport von Personen oder Gütern ist. Zusätzlich wurden die Teilnehmer gebeten, die Veränderungen durch Corona bei ihren Antworten nicht zu berücksichtigen.

Quelle: Deutscher Gewerkschaftsbund

Im Ausnahmezustand

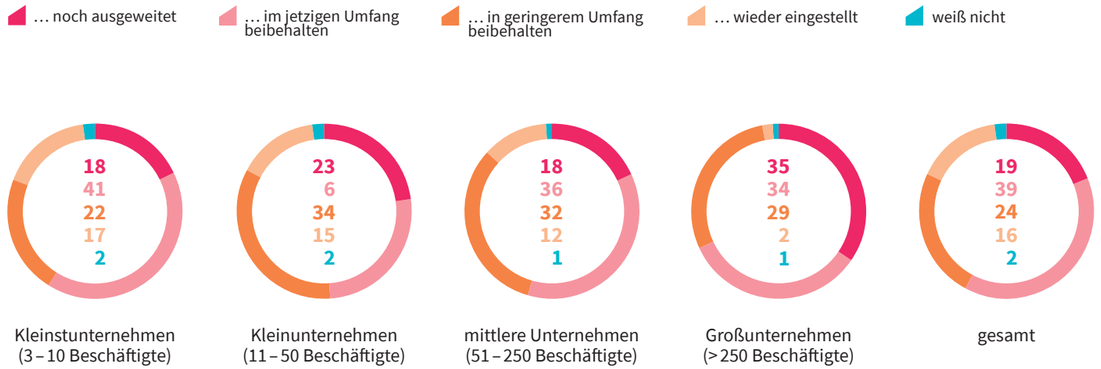
Mitarbeiter im Homeoffice wegen Corona-Pandemie nach Beschäftigtengrößenklassen; Befragung von Unternehmen, Organisationen und Verbänden der Wirtschaft aller Branchen mit mindestens 3 Beschäftigten, die Homeoffice angeboten haben (n = 1 000); Deutschland; 2020; in Prozent

	Beschäftigte im HO Gesamt	Beschäftigte im HO wegen Corona-Pandemie
Kleinstunternehmen (3 – 10 Beschäftigte)	68	41
Kleinunternehmen (11 – 50 Beschäftigte)	51	31
mittlere Unternehmen (51 – 250 Beschäftigte)	46	28
Großunternehmen (> 250 Beschäftigte)	48	26
gesamt	**64**	**39**

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Wie werden wir künftig arbeiten?

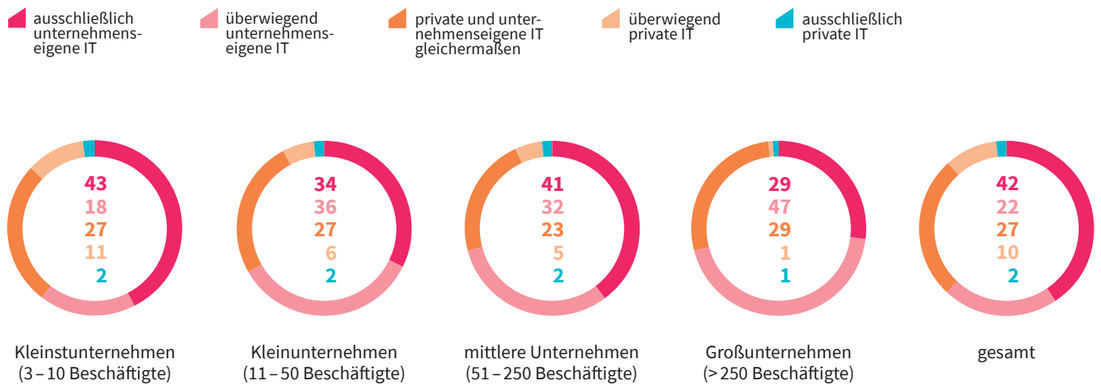
Perspektive von Homeoffice, Telearbeit und mobilem Arbeiten; Befragung von Unternehmen, Organisationen und Verbänden der Wirtschaft aller Branchen mit mindestens 3 Beschäftigten, die Homeoffice angeboten haben (n = 1 000); Deutschland; 2020; in Prozent



Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Wie werden wir uns künftig ausstatten?

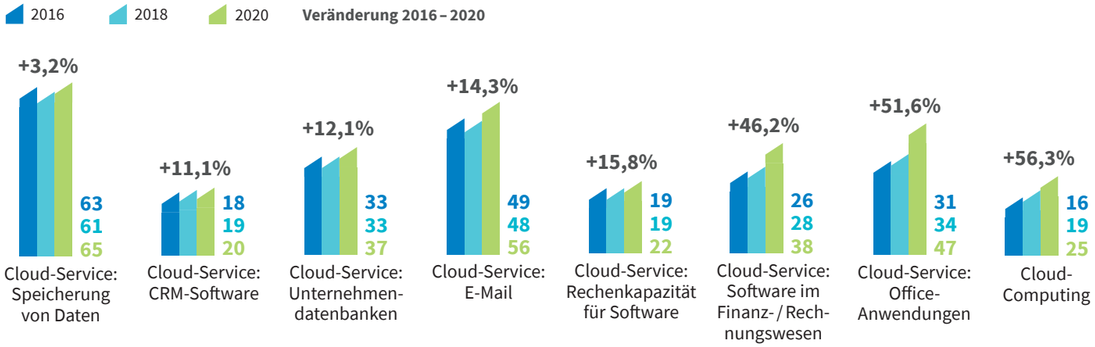
IT-Ausstattung im Homeoffice; Befragung von Unternehmen, Organisationen und Verbänden der Wirtschaft aller Branchen mit mindestens 3 Beschäftigten, die Homeoffice angeboten haben (n = 1 000); Deutschland; 2020; in Prozent



Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

In den Clouds

Nutzung von Cloud-Services in Unternehmen *; Deutschland; in Prozent



* Die Erhebung unter mehr als 20 000 registrierten Unternehmen basiert auf den Hauptbranchen von Destatis. Quelle: Destatis

In den Köpfen

Wahrnehmung der Digitalisierung im Arbeitsleben; repräsentative Befragung unter Erwerbstätigen (n = 2 088); Deutschland; 2019; in Prozent *

Meine Kollegen bzw. mein Arbeitsumfeld sind sehr aufgeschlossen gegenüber digitalen Arbeitsweisen und Technologien.	65
Die Technologien, die in meinem Unternehmen eingesetzt werden, sind modern und digital.	63
Die Digitalisierung bringt mehr positive Veränderungen in mein Arbeitsleben als negative.	61
Mein Unternehmen verfügt über eine Digitalisierungsstrategie und setzt diese aktiv um.	54
Die Digitalisierung erleichtert mir die Vereinbarkeit von Beruf und Arbeitsleben.	51
In meinem Unternehmen arbeiten wir räumlich und zeitlich flexibel, z. B. mobiles Arbeiten, Homeoffice, virtuelle / standortübergreifende Teams etc.	47
Ich würde mir in meinem Unternehmen ein moderneres und digitaleres Arbeitsumfeld wünschen.	42

* Befragte, die den Aussagen voll und ganz zustimmen oder eher zustimmen. Quellen: Bertelsmann Stiftung, Kantar

In den Strukturen

Auswirkung der Digitalisierung auf die Komplexität der IT-Landschaft; Befragung von Entscheidungsträgern (2019: n = 76; 2018: n = 77) in Deutschland, Österreich und der Schweiz; in Prozent

Die Komplexität der IT-Landschaft ist aufgrund der Digitalisierung …

	2018	2019	Veränderung 2018 – 2019
… stark gestiegen	24,5	25,0	2,0 %
… gestiegen	57,1	63,2	10,7 %
… unverändert	11,2	7,9	– 29,5 %
… gefallen	4,1	3,9	– 4,9 %
weiß nicht	2,0	k. A.	k. A.
keine Angaben	1,0	k. A.	k. A.

Quelle: Capgemini

In den Prozessen

Datenaustausch mit anderen Unternehmen; Befragung von Entscheidungsträgern (n = 74) in Deutschland, Österreich und der Schweiz; 2019; in Prozent

mit Teilnehmern Supply Chain (Lieferanten, Kunden)	60,8
mit Aufsichtsbehörden	54,1
mit Partnern außerhalb meiner Supply Chain	25,7
mit kommerziellen Datenanbietern (PoS-, Bonitäts-, demografische Daten etc.)	24,3
mit Wettbewerbern	9,5
weiß nicht	6,8
keine Angaben	12,2

Quelle: Capgemini

Darstellung und Verkauf?

Nutzung von digitalen Auftritten und Vertriebskanälen in Unternehmen *; Deutschland; in Prozent

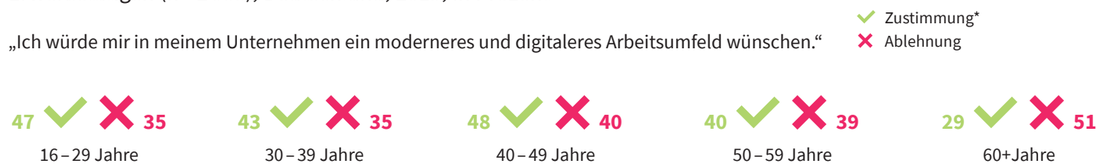
	2015	2018	2020	Veränderung 2015 – 2020
Website	58	66	62	6,9 %
Umsatz über Website / App	15	17	18	20,0 %
Verkäufe über eine Website oder App B2C	71	82	86	21,1 %
Verkäufe über Website oder App B2B und / oder B2G	82	79	58	– 29,3 %
Verkäufe über Online-Marktplätze	k. A.	50	63	k. A.

* Die Erhebung unter mehr als 20 000 registrierten Unternehmen basiert auf den Hauptbranchen von Destatis. Quelle: Destatis

Modern und digital?

Demografische Bereitschaft für ein modernes und digitaleres Arbeitsumfeld; repräsentative Befragung unter Erwerbstätigen (n = 2 088); Deutschland; 2019; in Prozent

„Ich würde mir in meinem Unternehmen ein moderneres und digitaleres Arbeitsumfeld wünschen."



* Zustimmung: Befragte, die der Aussage voll und ganz zustimmen oder eher zustimmen. Ablehnung: Befragte, die der Aussage eher nicht zustimmen oder überhaupt nicht zustimmen. Quellen: Bertelsmann Stiftung, Kantar

Hacker und Spione?

Größte Hemmnisse beim Thema IoT * für Unternehmen; Befragung der obersten IT-Verantwortlichen von Unternehmen (n = 444) in Deutschland, Österreich und der Schweiz; 2019; in Prozent **

„Security / Safety gilt als eines der Hemmnisse beim Thema IoT: Was fürchten Sie für Ihr Unternehmen am meisten?"

Hacker-Angriffe / DDos-Angriffe	36,5
Industriespionage	32,7
juristische Probleme	29,5
Produktionseinbußen / Produktionsausfälle	19,6
ungeklärte Compliance-Fragen	14,9
Havarie der Maschinen / Produktionsanlagen	5,6
Reputationsverlust / Vertrauensschaden bei Kunden und Stakeholdern	5,6
Verlust der Wettbewerbsfähigkeit durch Spionage / Datenklau	5,6
Erpressung durch Cyberattacken (z. B. Ransomware)	5,6

* Das Internet der Dinge (IoT) ist ein Sammelbegriff für Technologien einer globalen Infrastruktur der Informationsgesellschaften, die es ermöglicht, physische und virtuelle Objekte miteinander zu vernetzen und sie durch Informations- und Kommunikationstechniken zusammenarbeiten zu lassen. ** Mehrfachnennungen möglich (maximal 3 Antworten). Quelle: IDG Research Services

Datenschutz und Sicherheit?

Bedenken gegen IoT-Aktivitäten *; Befragung der obersten IT-Verantwortlichen von Unternehmen (n = 444) in Deutschland, Österreich und der Schweiz; 2019; in Prozent **

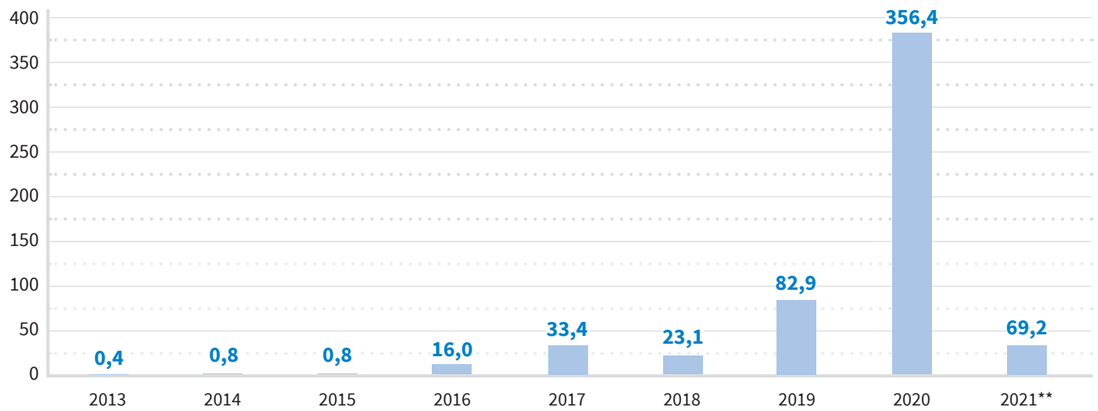
„Was sind in Ihren Augen ganz allgemein belastbare Argumente gegen breit angelegte IoT-Aktivitäten?"

Datenschutzbedenken	36,5
Sicherheitsbedenken	32,7
knappes Budget	29,5
Fachkräftemangel	27,3
fehlende Anwendungsfelder	20,7
fehlender ROI bei bestehenden IoT-Anwendungen	19,6
mangelnde Akzeptanz bei Mitarbeitern	14,9
mangelnde Akzeptanz bei Kunden	12,4
mangelnde Akzeptanz bei Geschäftspartnern und Dienstleistern	5,6
Es gibt keine belastbaren Argumente gegen IoT-Aktivitäten	4,3

* Das Internet der Dinge (IoT) ist ein Sammelbegriff für Technologien einer globalen Infrastruktur der Informationsgesellschaften, die es ermöglicht, physische und virtuelle Objekte miteinander zu vernetzen und sie durch Informations- und Kommunikationstechniken zusammenarbeiten zu lassen. ** Mehrfachnennungen möglich. Quelle: IDG Research Services

Lösegeld-Zahlungen

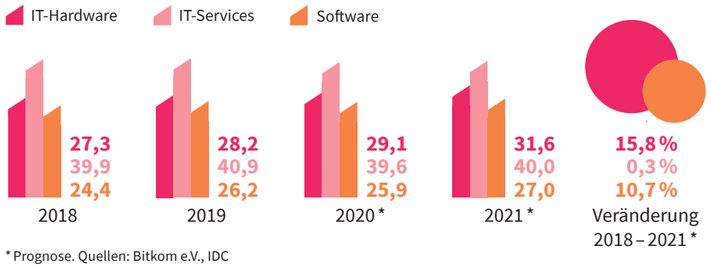
Ransomware-Angriffe: Lösegeld, gezahlt mit Kryptowährungen *; weltweit; in Millionen Euro



* Bitcoin Cash, Bitcoin, Ethereum, Theter. ** Stand 10. Mai 2021. Quelle: Chainalysis.com

IT-Märkte

Marktvolumen von Informationstechnik; Deutschland; in Milliarden Euro



* Prognose. Quellen: Bitkom e.V., IDC

IT-Sicherheitsinvestitionen

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

	2018	2019	2020 *	2021 *
Hardware	0,6	0,7	0,7	0,8
Services	2,3	2,6	2,8	3,1
Software	1,3	1,5	1,6	1,7
gesamt	4,2	4,8	5,1	5,6

* Prognose. Quellen: Bitkom e.V., IDC

IT-Budgets

Entwicklung des IT-Budgets in Unternehmen; Befragung von Entscheidungsträgern (n = 128) in Deutschland, Österreich und der Schweiz; 2020; in Prozent

27,3
bleibt gleich

48,4
steigt

14,9
sinkt

9,4
weiß nicht / keine Angabe

Quelle: Capgemini

Wie steht es um IT-Entwicklung und Digitalisierung?

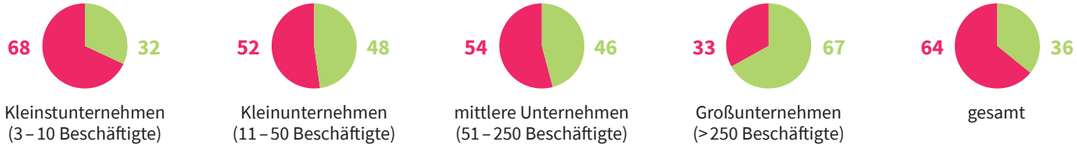
Befragung von Unternehmen, Organisationen und Verbänden der Wirtschaft aller Branchen * mit mindestens 3 Beschäftigten, die Homeoffice angeboten haben (n = 1 000); Deutschland; 2020; in Prozent

	sehr gut (1)	(2)	(3)	(4)	(5)	sehr schlecht (6)
Kleinstunternehmen (3 – 10 Beschäftigte)	11	38	38	9	3	1
Kleinunternehmen (11 – 50 Beschäftigte)	12	43	32	10	2	1
mittlere Unternehmen (51 – 250 Beschäftigte)	14	42	30	12	2	0
Großunternehmen (> 250 Beschäftigte)	18	45	32	1	3	0
gesamt	12	39	37	9	3	1

* Gewichtung nach Branchen und Unternehmensgrößen. Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Ist die Pandemie ein Digitalisierungsturbo?

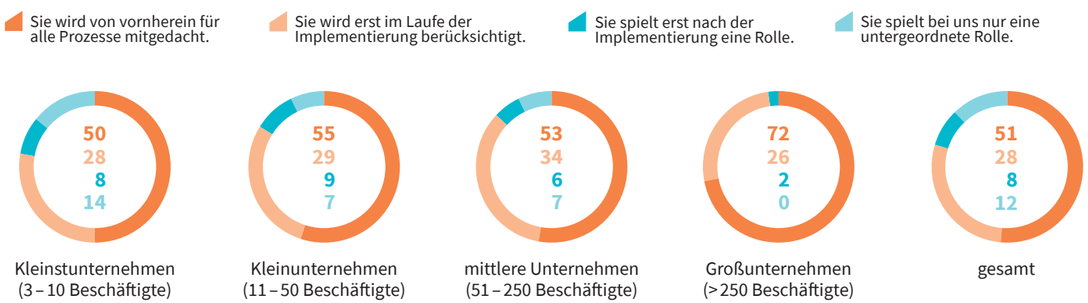
Befragung von Unternehmen, Organisationen und Verbänden der Wirtschaft aller Branchen * mit mindestens 3 Beschäftigten, die Homeoffice angeboten haben (n = 1 000); Deutschland; 2020; in Prozent



* Gewichtung nach Branchen und Unternehmensgrößen. Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Ist Informationssicherheit im Zuge der Digitalisierung ein Thema?

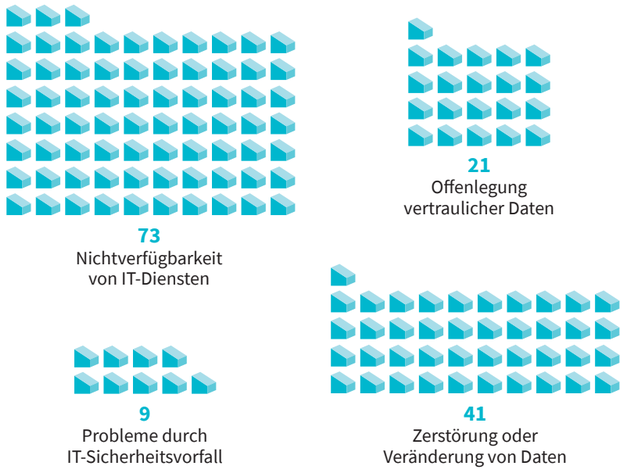
Befragung von Unternehmen, Organisationen und Verbänden der Wirtschaft aller Branchen * mit mindestens 3 Beschäftigten, die Homeoffice angeboten haben (n = 1 000); Deutschland; 2020; in Prozent



* Gewichtung nach Branchen und Unternehmensgrößen. Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Was passiert?

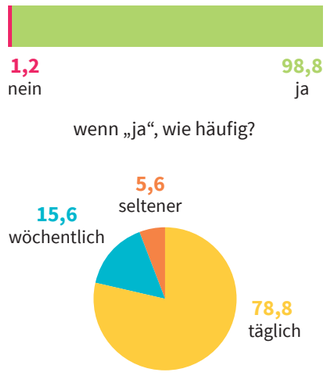
IT-Sicherheitsvorfälle in Unternehmen *; Deutschland; 2019; in Prozent



* Die Erhebung unter mehr als 20 000 registrierten Unternehmen basiert auf den Hauptbranchen von Destatis.
Quelle: Destatis

Wer sorgt vor?

Durchführung regelmäßiger Back-ups & Updates in Unternehmen; Befragung von Entscheidungsträgern; Deutschland; 2018 / 19; in Prozent



Quelle: Kriminologisches Forschungsinstitut Niedersachsen

Welche Unternehmen trifft es?

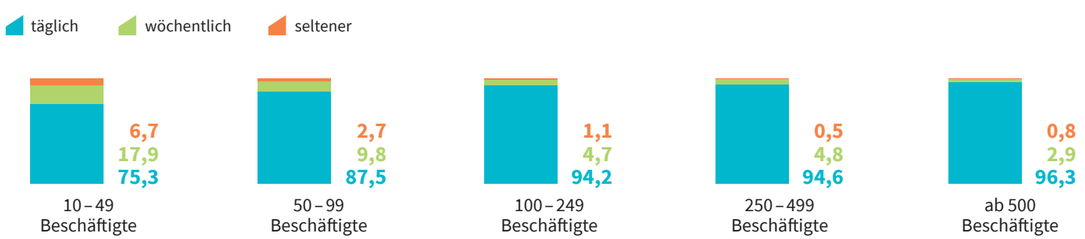
IT-Sicherheitsvorfälle in Unternehmen nach Beschäftigtengrößenklassen *; Deutschland; 2019; in Prozent

	1 – 9 Beschäftigte	10 – 49 Beschäftigte	50 – 249 Beschäftigte	250 und mehr Beschäftigte
Probleme durch IT-Sicherheitsvorfall	9	10	15	18
Nichtverfügbarkeit von IT-Diensten	74	71	75	71
Zerstörung oder Veränderung von Daten	39	50	45	41
Offenlegung vertraulicher Daten	23	13	10	15

* Die Erhebung unter mehr als 20 000 registrierten Unternehmen basiert auf den Hauptbranchen von Destatis. Quelle: Destatis

Wer ist eher lässig?

Durchführung regelmäßiger Back-ups & Updates in Unternehmen nach Beschäftigtengrößenklassen; Befragung von Entscheidungsträgern in Unternehmen; Deutschland; 2018 / 2019; in Prozent



Quelle: Kriminologisches Forschungsinstitut Niedersachsen

Klar geregelt

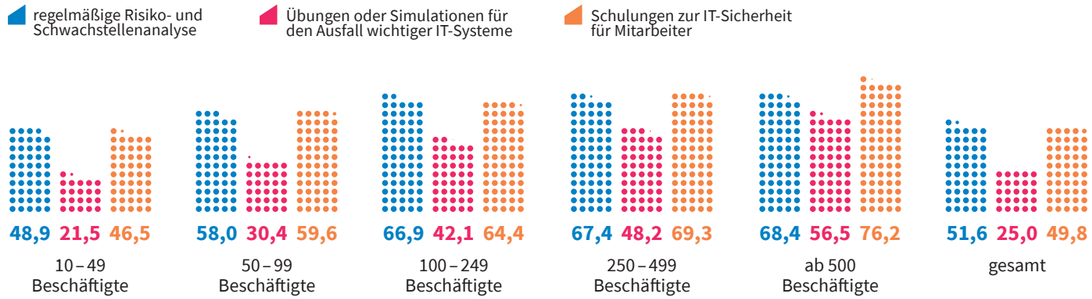
Richtlinien & Zertifizierungen nach Beschäftigtengrößenklassen; Befragung von Entscheidungsträgern in Unternehmen; Deutschland; 2018 / 2019; in Prozent

	10 – 49 Beschäftigte	50 – 99 Beschäftigte	100 – 249 Beschäftigte	250 – 499 Beschäftigte	ab 500 Beschäftigte	gesamt
Einhaltung der Richtlinien wird regelmäßig überprüft und Verstöße ggf. geahndet	76,3	78,3	79,5	82,1	80,9	76,7
schriftlich fixierte Richtlinien zur Informations- bzw. IT-Sicherheit	62,6	75,3	84,6	87,5	92,0	66,2
schriftlich fixierte Richtlinien zum Notfallmanagement	50,6	64,6	76,6	78,8	84,4	54,9
Zertifizierung der IT-Sicherheit, z. B. nach ISO 20071 oder BSI Grundschutz	23,2	30,1	30,1	33,2	35,1	24,8

Quelle: Kriminologisches Forschungsinstitut Niedersachsen

Mäßig vorbereitet

Unternehmen mit Analysen, Übungen und Schulungen zur IT-Sicherheit nach Beschäftigtengrößenklassen; Befragung von Entscheidungsträgern in Unternehmen; Deutschland; 2018 / 2019; in Prozent



Quelle: Kriminologisches Forschungsinstitut Niedersachsen

Ähnlich organisiert

Richtlinien & Zertifizierungen nach Beschäftigtengrößenklassen; Befragung von Entscheidungsträgern in Unternehmen; Deutschland; 2018 / 2019; in Prozent

	10 – 49 Beschäftigte	50 – 99 Beschäftigte	100 – 249 Beschäftigte	250 – 499 Beschäftigte	ab 500 Beschäftigte	gesamt
regelmäßige Back-ups	98,6	99,4	99,6	99,3	99,8	98,8
physisch getrennte Aufbewahrung von Back-ups	94,3	96,8	98,0	98,5	97,8	94,9
Mindestanforderungen für Passwörter	85,4	87,0	91,9	91,8	95,4	86,3
individuelle Vergabe von Zugangs- und Nutzerrechten je nach Aufgabe	82,0	94,5	96,2	96,6	96,4	84,7

Quelle: Kriminologisches Forschungsinstitut Niedersachsen

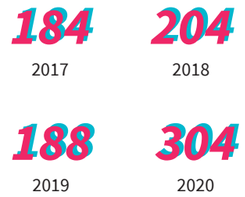
Furchtlos

Zuständigkeiten für IT-Sicherheit im Unternehmen; Befragung von Führungskräften deutscher Unternehmen (n = 453); 2019; in Prozent

Quelle: EY

Grenzenlos

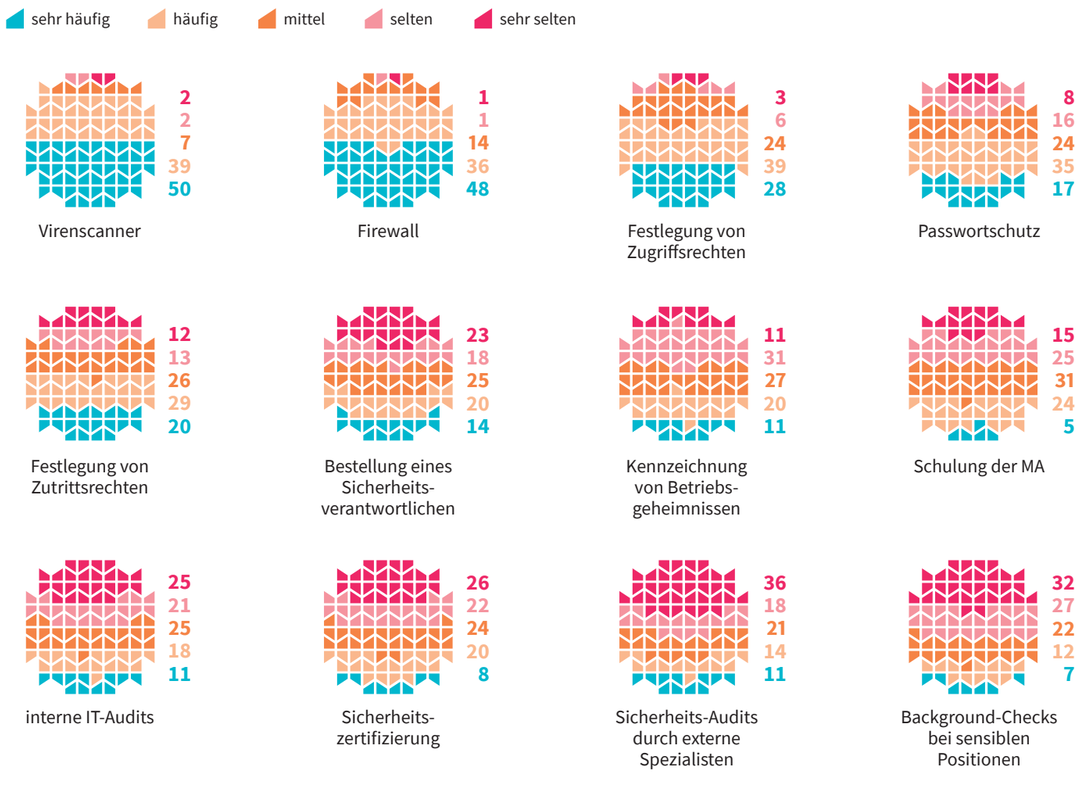
Entwicklung von Ransomware-Attacken; weltweit; Zahl in Millionen



Quellen: Sonic Wall

Anspruchslos

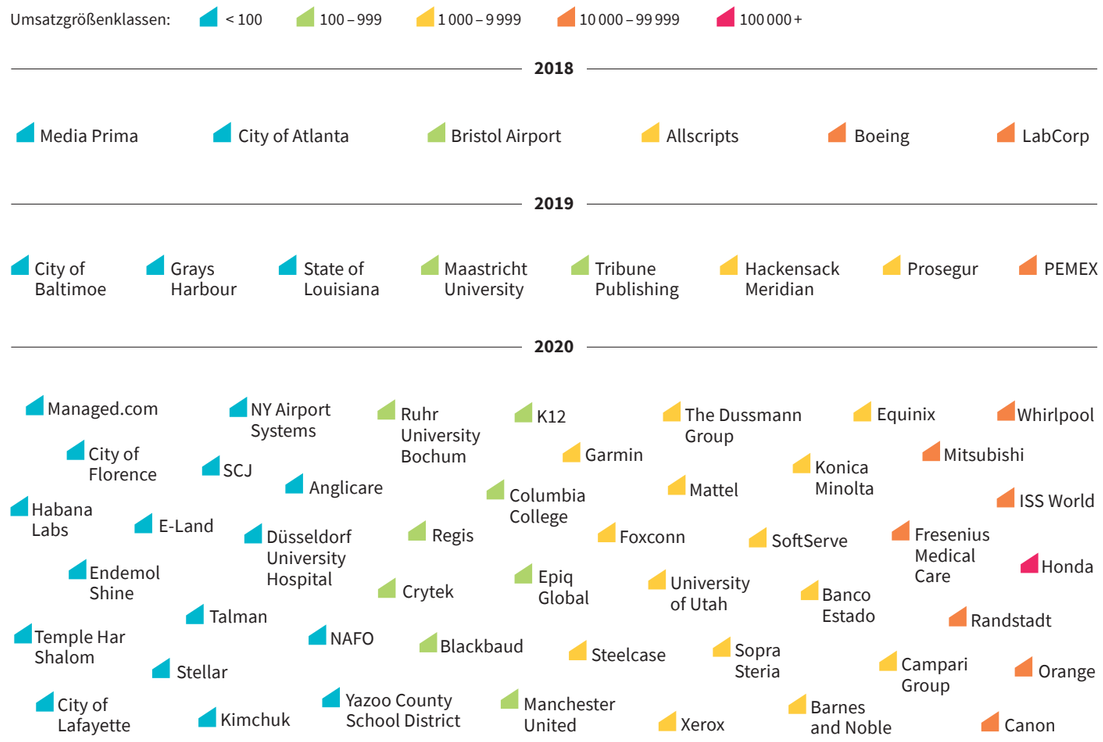
Maßnahmen für Cybersicherheit in Unternehmen; Befragung von Unternehmen aus dem Mittelstand (n = ca. 353); 2019; in Prozent



Quelle: Deloitte

Uferlos

Die Zahl der Ransomware-Angriffe steigt weltweit, Ziel sind Unternehmen jeder Branche und jeder Größe. Hier eine Auswahl von Betroffenen *, sortiert nach Umsatzgrößenklassen; weltweit; in Millionen US-Dollar



* Die Zusammenstellung erhebt keinen Anspruch auf Vollständigkeit. Stand 10. Juli. 2021. Quellen: bleeping computer, zdnet & weitere Presseveröffentlichungen

Schmerzvoll

Schwerwiegendster Cyberangriff nach Angriffsart; Befragung von Entscheidungsträgern in Unternehmen; Deutschland; 2018 / 2019; in Prozent

Phishing	26,0
sonstige Schadsoftware	23,5
Ransomware	22,3
Spyware	8,0
(D)DoS	7,4
CEO-Fraud	7,2
manuelles Hacking	3,5
Defacing	2,7
sonstiger Angriff	0,7

Quelle: Kriminologisches Forschungsinstitut Niedersachsen

Wertvoll

Anteil der Unternehmen mit Kosten infolge des schwerwiegendsten Ransomeware-Angriffs; Befragung von Entscheidungsträgern in Unternehmen; Deutschland; 2018 / 2019; in Prozent *

52,4	45,7	42,0
Wiederherstellung / Wiederbeschaffung	Sofortmaßnahmen zur Abwehr und Aufklärung	Betriebsunterbrechung
37,6	1,5	1,5
externe Beratung	Schadenersatz / Strafen	abgeflossene Gelder

* Mehrfachnennungen möglich.
Quelle: Kriminologisches Forschungsinstitut Niedersachsen

Machtvoll

Zahl der Cyberangriffe in den vergangenen 12 Monaten je 100 Unternehmen nach Angriffsart; Befragung von Entscheidungsträgern in Unternehmen; Deutschland; 2018 / 2019; in Prozent

Phishing	760
sonstige Schadsoftware	352
Spyware	176
Ransomware	49
manuelles Hacking	43
CEO-Fraud	35
(D)DoS	33
Defacing	18

Quelle: Kriminologisches Forschungsinstitut Niedersachsen

Gefahrvoll

Entwicklung des IT-Sicherheitsbudgets während der Corona-Krise *; Befragung von Unternehmen, Organisationen und Verbänden der Wirtschaft aller Branchen mit mindestens 3 Beschäftigten, die Homeoffice angeboten haben (n = 1 000); Deutschland; 2020; in Prozent

Budget-Anteil für Cybersicherheit am IT-Budget

0 Prozent	4
bis zu 10 Prozent	51
11 bis 25 Prozent	24
26 bis 50 Prozent	16
mehr als 50 Prozent	5

Erhöhung des IT-Sicherheitsbudgets während der Corona-Krise

ja, aufgrund der Cybersicherheitslage	11
ja, aber nicht wegen der Cybersicherheitslage	5
nein, Budget blieb unverändert	63
nein, Erhöhung ist erst später geplant	5
nein, Budget musste aufgrund der besonderen Situation verringert werden	4
weiß nicht	11

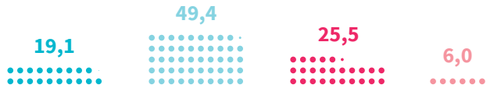
* Gewichtung nach Branchen und Unternehmensgrößen.
Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Hoffnungsvoll

Risikoeinschätzung im Unternehmen in Bezug auf einen Cyberangriff; Befragung von Entscheidungsträgern in Unternehmen; Deutschland; 2018 / 2019; in Prozent

sehr gering · eher gering · eher hoch · sehr hoch

Risiko eines schädigenden ungezielten Angriffs in den nächsten 12 Monaten



Risiko eines schädigenden gezielten Angriffs in den nächsten 12 Monaten

Quelle: Kriminologisches Forschungsinstitut Niedersachsen

Unheilvoll

Infektionswege bei Malware-Angriffen; Befragung von Entscheidungsträgern in Unternehmen; Deutschland; 2018 / 19; in Prozent

ja · vermutlich · nein

Quelle: Kriminologisches Forschungsinstitut Niedersachsen

Leidvoll

Durchschnittliche Ausfallzeit von als wichtig eingestuften IT-Systemen in Unternehmen; Befragung von Entscheidungsträgern in Unternehmen; Deutschland; 2018 / 2019; in Stunden

E-Mail und Kommunikation	64,8
Auftrags- und Kundenverwaltung	76,0
Rechnungswesen und Controlling	73,3
Webauftritt	337,2
weitere Software zur Erbringung von Dienstleistungen	88,7
Banking und Trading	43,9
Lager und Logistik	72,9
Produktionssteuerung	65,3

Quelle: Kriminologisches Forschungsinstitut Niedersachsen

Kummervoll

Anteil der Unternehmen mit Kosten infolge des schwerwiegendsten Cyberangriffs; Befragung von Entscheidungsträgern in Unternehmen; Deutschland; 2018 / 2019; in Prozent

externe Beratung	30,3
Sofortmaßnahmen zur Abwehr und Aufklärung	39,9
Schadenersatz / Strafen	1,4
abgeflossene Gelder	2,2
Betriebsunterbrechung	25,7
Wiederherstellung/Wiederbeschaffung	33,0
Kosten bei mindestens einer Position entstanden	70,0

Quelle: Kriminologisches Forschungsinstitut Niedersachsen

Verhängnisvoll

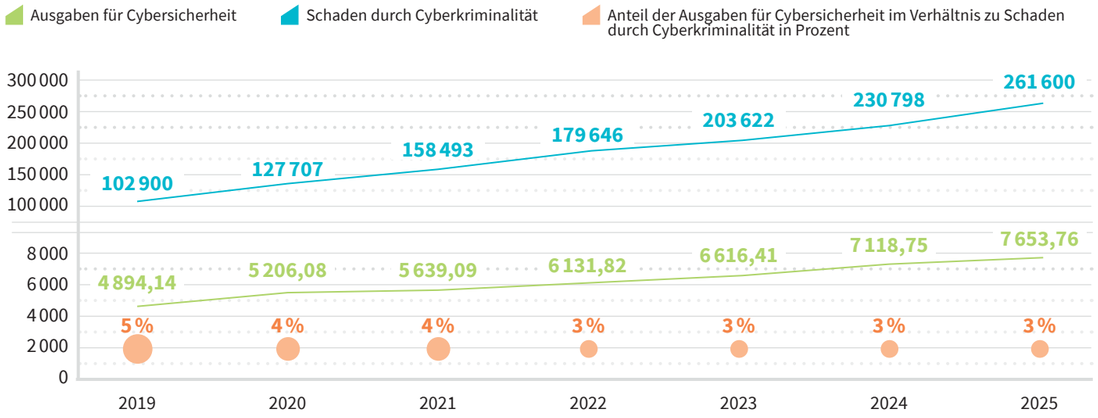
Nichtanzeigegründe einer Cyberattacke nach Position im Unternehmen; Befragung von Entscheidungsträgern in Unternehmen; Deutschland; 2018 / 2019; in Prozent

gesamt · Geschäftsführung · IT · Sonstige

Quelle: Kriminologisches Forschungsinstitut Niedersachsen

Schäden in Millionenhöhe

Verhältnis Investition in Cybersicherheit im Vergleich zu Schaden durch Cyberkriminalität; Deutschland; in Millionen Euro



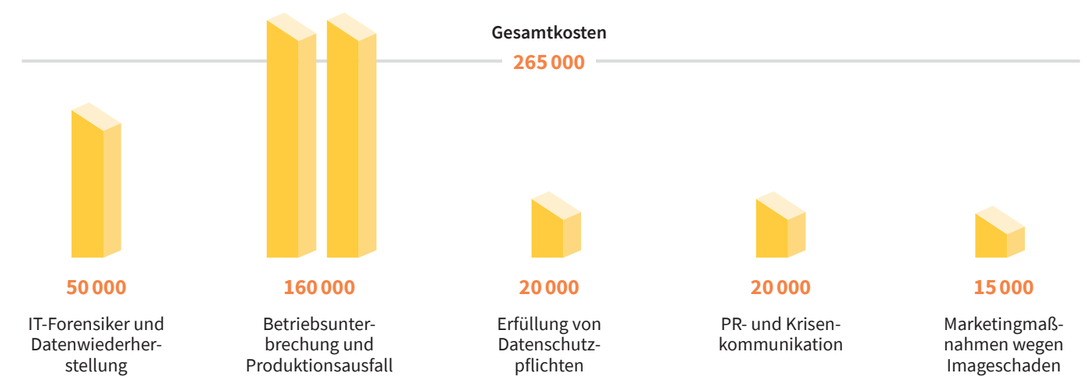
Quellen: Statista, G DATA, Embroker, Bitkom e. V.

Kosten im Einzelfall

Kosten eines Cyberangriffs: Fallbeispiel; Deutschland; 2020; in Euro

Der Fall:
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.

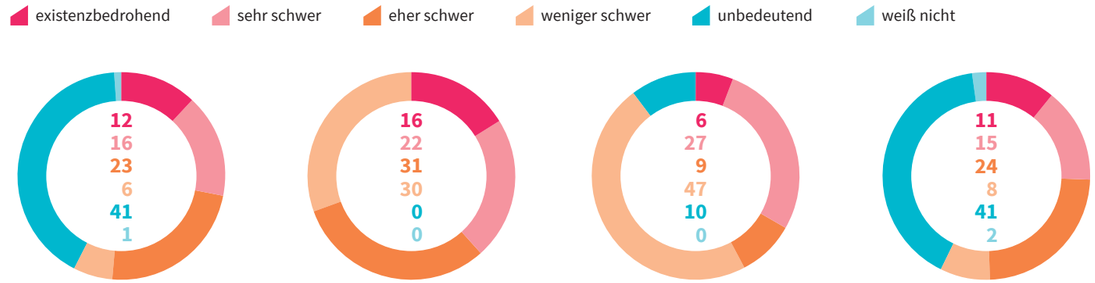
Die Auswirkungen:
Der Trojaner verhindert den Zugang auf alle Rechner, die Produktion steht still, die Sicherheit von Betriebsgeheimnissen, Kunden- und Vertragsdaten ist nicht mehr gewährleistet. Das Unternehmen ist handlungsfähig und informiert zunächst die Polizei über den Angriff. Polizei und Staatsanwaltschaft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



Quelle: Unternehmen Cybersicherheit gemeinsame Initiative von VDMA und VSMA

Im Visier

Bewertung der Schäden durch Cyberangriffe während der Zeit im Homeoffice; Befragung von Unternehmen, Organisationen und Verbänden der Wirtschaft aller Branchen mit mindestens 3 Beschäftigten, die Homeoffice angeboten haben (n = 1 000); Deutschland; 2020; in Prozent



Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Im Wachsen

Betroffenheit von Unternehmen durch Datendiebstahl, Industriespionage oder Sabotage; Befragung von Entscheidern in Deutschland (2019: n = 1 070, 2017: n = 1 069, 2015: n = 1 074); in Prozent

	2015	2017	2019
betroffen	51	53	75
vermutlich betroffen	28	26	13

Quelle: Bitkom e. V.

Im Unklaren

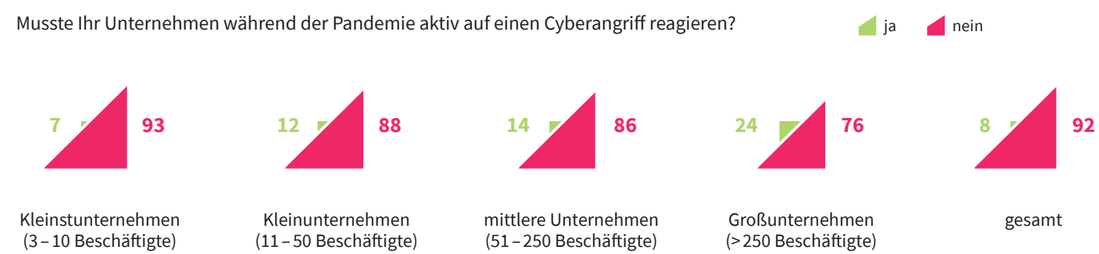
Wahrnehmung eines Risikos durch Cyberkriminalität; Marktforschung unter Entscheidern von KMU in Deutschland (n = 300); 2020; in Prozent

Das Risiko von Cyberkriminalität für mittelständische Unternehmen in Deutschland ist eher bzw. sehr hoch.	69
Das Risiko von Cyberkriminalität für das eigene Unternehmen ist eher bzw. sehr hoch.	28

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

Im Zugzwang

Notwendige Reaktionen auf Cyberangriffe während der Corona-Zeit im Homeoffice; Befragung von Unternehmen, Organisationen und Verbänden der Wirtschaft aller Branchen mit mindestens 3 Beschäftigten, die Homeoffice angeboten haben (n = 1 000); Deutschland; 2020; in Prozent



Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Am liebsten intern

Weiterbildungsmaßnahmen für Mitarbeiter im Unternehmen; Befragung von Unternehmen aus dem Mittelstand (n = ca. 353); 2019; in Prozent

	interne Weiterbildung	externe Weiterbildungsmaßnahmen
Datensicherheit	39	25
Datenschutz	42	29
interne Gefahrensituation	45	13
keine Weiterbildungsmaßnahmen	18	14

Quelle: Deloitte

Vor allem schulen

Umgang und Weiterentwicklung der Mitarbeiter durch Kompetenztrainings; Befragung von Mitarbeitern sowie leitenden Angestellten in kleinen und mittleren Unternehmen (n = 1 038); 2019 / 2020; in Prozent

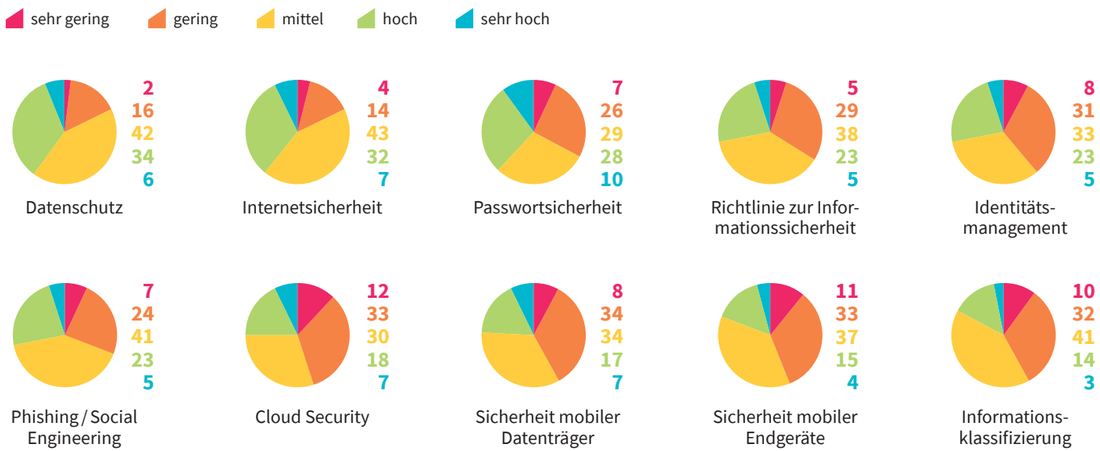
Wie sorgen Unternehmen für angemessene Kompetenztrainings?

Befragte schulen Mitarbeiterinnen und Mitarbeiter regelmäßig und erinnern auch über Schreiben der Geschäftsleitung an die Verantwortung für die Sicherheit im Unternehmen.	47
Befragte ergreifen keine Maßnahmen für mehr Kompetenzen.	24
Befragte haben ihre Sicherheitskultur analysiert und gezielt Kommunikationsmaßnahmen eingeführt, die das Sicherheitsbewusstsein fördern.	16
Befragte führen Awareness-Kampagnen durch und setzen dabei etwa auf Poster, Live-Hacking-Veranstaltungen und Giveaways.	13

Quelle: Deutschland sicher im Netz (DsiN)

Erstaunlich unbedarft

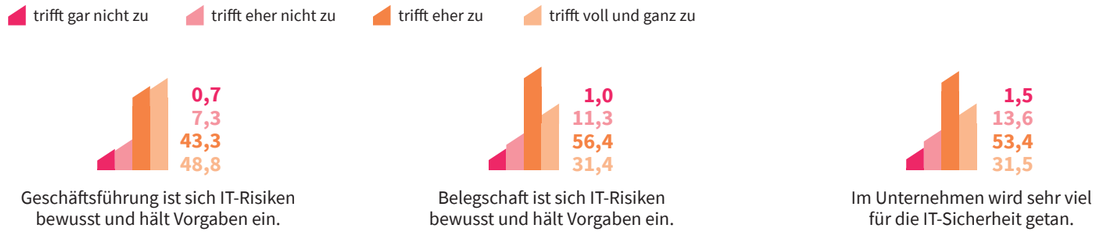
Mitarbeitersensibilisierung im Bereich Cybersicherheit; Befragung von Unternehmen aus dem Mittelstand (n = ca. 353); 2019; in Prozent



Quelle: Deloitte

Bewusst

Einschätzungen zum Risikobewusstsein im Unternehmen; Befragung von Entscheidungsträgern in Unternehmen; Deutschland; 2018 / 2019; in Prozent



Quelle: Kriminologisches Forschungsinstitut Niedersachsen

Nicht ich

Risikoumgang in Unternehmen; Befragung von Mitarbeitern sowie leitenden Angestellten in kleinen und mittleren Unternehmen (n = 1 038); 2019 / 2020; in Prozent

Wer entscheidet im Unternehmen über den konkreten Umgang mit Risiken?

Geschäftsleitung	50
IT-Abteilung oder der IT-Dienstleister	33
Bereichs- / Abteilungsleitende	12
jeweilige Beschäftigte	5

Quelle: Deutschland sicher im Netz (DsiN)

Unbewusst

Wirtschaftliches Wohlergehen durch IT-Sicherheit; Befragung von Mitarbeitern sowie leitenden Angestellten in kleinen und mittleren Unternehmen (n = 1 038); 2019 / 2020; in Prozent

„Sehen Sie einen direkten Zusammenhang zwischen wirtschaftlichem Wohlergehen und IT-Sicherheit?“ Zustimmung bei …

Kleinstunternehmen mit unter 10 Beschäftigten	31
Unternehmen mit 10 bis 50 Unternehmen	26
Unternehmen mit 51 bis 200 Beschäftigten	20
Unternehmen mit 201 bis 500 Beschäftigten	9
Unternehmen mit mehr als 500 Beschäftigten	14

Quelle: Deutschland sicher im Netz (DsiN)

Nicht heute

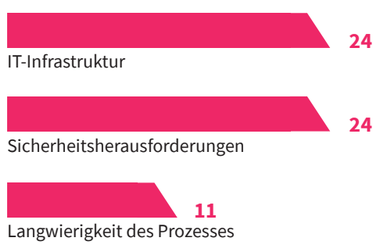
Modernisierung der Legacy-IT; Unternehmen in Deutschland; 2018; in Prozent

Die wichtigsten Modernisierungsprojekte sind …

… abgeschlossen	9,1
… auf einen Zeitraum von 3 Monaten angelegt	8,7
… auf einen Zeitraum von 6 Monaten angelegt	14,2
… auf einen Zeitraum von 12 Monaten angelegt	20,7
… auf einen Zeitraum von 1 bis 2 Jahren angelegt	13,9
… auf einen Zeitraum von 2 bis 3 Jahren angelegt	13,3
… auf einen Zeitraum von 4 bis 5 Jahren angelegt	4,9
… auf einen Zeitraum von 6 bis 7 Jahren angelegt	1,3
… auf einen Zeitraum von 7 bis 10 Jahren angelegt	0,3
Der Zeitraum lässt sich noch nicht abschätzen.	11,0

Quelle: Deloitte

größte Herausforderungen bei der Legacy-Modernisierung:



Motiv: flickr.com/A2K Design

Der ewige Wettlauf

Wir alle kennen Schauergeschichten, in denen Hacker in geheime Systeme eindringen, um Atomwaffen unter ihre Kontrolle zu bringen. Dabei ist die alltägliche Gefahr viel banaler: Mit ständig neuen Tricks greifen professionelle Gangsterbanden nach Geld und Daten naiver Nutzer, während Sicherheitsexperten versuchen, den Ganoven das Geschäft zu vermasseln.
Ein Katz-und-Maus-Spiel mit langer Vorgeschichte.

Text: Ulf J. Froitzheim

Mein erster Rechner

Die Errungenschaften der Informationstechnik sind heute überall. Waren früher PC und Smartphone die Höhepunkte des privaten IT-Komforts, gehören mittlerweile selbst Alltagsgegenstände wie elektrische Zahnbürsten zum Internet der Dinge – und sind damit potenziell anfällig für Manipulationen von außen.

Das beginnt bei harmlosem Schabernack, wenn der Nachbar die Steuerung der LED-Deckenleuchte übernimmt, und reicht bis hin zu echten Gefahren, wenn etwa ungesicherte Haushaltsgeräte von Bot-Netzen gekapert werden. Da ist Schluss mit lustig, denn dann wird die Überwachungskamera vor der Garage zum Tatwerkzeug bei dem Versuch, die Website eines Unternehmens zu torpedieren oder gar sogenannte Kritische Infrastrukturen lahmzulegen.

Fast alles, was fürs öffentliche Leben essenziell ist, hängt irgendwie am Internet: Ölpipelines, Kraftwerke, Verkehrsbetriebe, Banken, Krankenhäuser, Wasserversorgung, Medien. Und alles, was online ist, kann und wird ständig von irgendwem angegriffen – von professionellen Betrügern, Online-Bankräubern oder Erpressern, von wohlwollenden Hacktivisten oder sinistren politischen Intriganten, von der Mafia oder den Geheimdiensten.

Doch die stetige Flut von Angriffen ist alles andere als der digitale Tsunami, als der sie manchmal dargestellt wird. Sie ist weder aus dem Nichts aufgetaucht noch wird sie wieder abebben. Sie hat eine lange Vorgeschichte, die weit in die Zeit zurückreicht, als das Internet noch Zukunftsmusik war. „Es ist ein ewiger Wettlauf“, fasst Horst Görtz, 83, einer der deutschen Pioniere der Cybersecurity, den Kampf um die IT-Sicherheit zusammen.

Für Görtz ertönte der Startschuss zu diesem Rennen Anfang der Achtzigerjahre. „Ich kam auf die Idee, in Sicherheit zu investieren, als ich einen Auftrag verlor,“ erzählt der ehemalige IT-Unternehmer aus dem Taunus. Ein Geschäftskunde hatte eine Anwendungssoftware, die Görtz ihm anbot, nicht haben wollen, weil ihn ein Datenschutzbeauftragter davor warnte. „Er sagte: ‚Mit PCs kann man so was nicht machen, das ist zu unsicher‘“, erinnert sich Görtz. Das war ein sehr weitsichtiges Argument in einer Zeit, in der auf den meisten Schreibtischen noch lärmende Kugelkopf-Schreibmaschinen standen und die Kriminalstatistik mangels Masse keine Computerdelikte auswies.

Die heile Welt ging kaputt, als IBM mit dem 5150 ein revolutionäres Konzept salonfähig machte: den persönlichen Computer für jedermann.

Bevor Görtz mit seinem 1983 gegründeten Softwarehaus Utimaco ins Geschäft mit Sicherheitslösungen für Unternehmenskunden einstieg, hatte er sein Geld mehr als 20 Jahre lang mit Elektronischer Datenverarbeitung (EDV) verdient, erst bei dem französischen Hersteller Bull und dann als Geschäftsführer des Bull-Ablegers Rhein-Main-Rechenzentrum (RM-RZ) in Frankfurt. Es war eine beschauliche Ära, in der sich kaum ein Mittelständler eigene Computer leistete und deshalb fast alle ihre Buchhaltungsdaten elektronisch außer Haus verarbeiten ließen.

Damals bedurfte es dazu voluminöser, stromfressender und vor allem teurer Maschinen, die aus einem Bruchteil der Rechenleistung eines heutigen Smartphones alles herausholten. Die Daten wurden auf Lochstreifen transportiert oder auf Magnetbändern, die an Tonbandspulen erinnerten. Hätte sich jemand dafür interessiert, hätte er den Boten überfallen müssen – aber die Bänder nicht auslesen können.

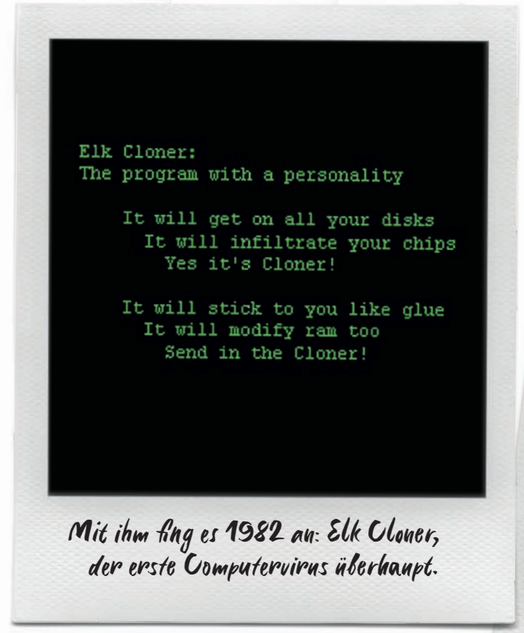
Von der Technik, die sich heutige Hacker zunutze machen, existierte so gut wie nichts. In den Firmen gab es Bildschirm-Terminals für die Datenerfassung, aber die User konnten weder etwas auf Datenträgern abspeichern noch irgendwelche mit Viren infizierten Dateien ins System laden. Es gab nur „dumme“ Terminals: Monitore mit Tastatur – eine hermetische Konstruktion ohne Schnittstelle.

Zwar sammelten Forschungseinrichtungen erste Erfahrungen mit Datenfernübertragungen, doch die Technik war extrem teuer und unterlag zudem dem Monopol der Bundespost. Legale Modems gab es noch nicht zu kaufen – und illegale hätten kein Gegenüber gefunden, mit dem sie sich hätten verbinden können. Um unbefugte Dritte davon abzuhalten, in schutzwürdigen Daten zu schnüffeln, genügte es, vor der Tür des Rechenzentrums einen Pförtner zu postieren, der Betriebsfremden den Zugang verwehrte.

Von allen unterschätzt

Diese simple, heile Welt ging kaputt, als IBM, damals der dominierende Computerhersteller, 1981 mit dem Modell 5150 ein revolutionäres Konzept salonfähig machte: den „persönlichen Computer“ für jedermann, mit „Intelligenz“ in Form eines Prozessorchips – und weit offenen Einfallstoren für Cyberattacken in Gestalt von zwei 5 ¼-Zoll-Floppy-Disk-Laufwerken. Das war die Büchse der digitalen Pandora.

Gestandene EDV-Praktiker unterschätzten zunächst die Tragweite der Innovation. Erstens nahmen sie Startups aus dem Silicon Valley wie Apple, die Ende der Siebziger die ersten derartigen Geräte entwickelt hatten, nicht für voll. Zweitens hatte IBM bei der ersten Version des PC an der Ausstattung gespart. „Die Mikrocomputer wurden anfangs allenfalls als Schreibgeräte verwendet“, erinnert sich Görtz, der später mit einer Stiftung seines Namens zum



Mit ihm fing es 1982 an: Elk Cloner, der erste Computervirus überhaupt.

Der IBM Personal Computer, Modell 5150, war 1981 das Urmodell der heutigen IBM-kompatiblen PCs.

Foto: Wikipedia

wichtigsten Förderer der deutschen IT-Sicherheitsforschung wurde. „Und Behörden oder sicherheitsrelevante Firmen haben in den ersten Jahren gar keine PCs benutzt.“

In vielen Unternehmen wehrten sich zudem die EDV-Leiter gegen Desktop-Computer. Die ITler sahen von den „Fachabteilungen“ – ein Synonym für digitale Analphabeten, die mit kaum umsetzbaren Wünschen Stress machten – ihr Herrschaftswissen und ihre Macht bedroht. Außerdem wollten sie sich nicht die Verantwortung für Technik zuschieben lassen, die sich ihrer Kontrolle entzog. Dabei überwanden die Geräte gerade mit ihrer Offenheit und Zugänglichkeit die in der Bevölkerung weitverbreitete Aversion gegen „Elektronengehirne“, sodass sich mit der Zeit immer mehr Menschen für Informationstechnik begeisterten. Die Markteinführung des PCs war allerdings auch die Geburtsstunde des DAU – des dümmsten anzunehmenden Users.

Manche der nun drohenden Gefahren waren in der Grundlagenliteratur bereits lange zuvor skizziert worden. John von Neumann, der Vater der bis heute üblichen Computerarchitektur, stellte schon in seinem 1949 erschienenen Aufsatz „Theory and Organization of Complicated Automata“ fest, dass sich Programme selbstständig vervielfältigen können – die Basis jedes Virus. Zwei Forscher der Bell Labs machten im folgenden Jahr spielerisch die Probe aufs Exempel, dann geriet das Thema in Vergessenheit.

Erst 1980 wurde es wieder Thema: Ein Diplomand an der Universität Dortmund widmete seine Abschlussarbeit der „Selbstreproduktion bei Programmen“. Bis das Konzept für Malware (also maliziöse, schädliche Software) missbraucht wurde, war es nur eine Frage der Zeit.

In freier Wildbahn tauchte der erste, noch harmlose Virus – bei Computern sind sie maskulin – 1982 auf. Der „Elk Cloner“ infizierte aber nur den Apple II, den in der IBM-Welt niemand ernst nahm, und tat nichts anderes, als in einem Sechszeiler seine Anwesenheit auf der Diskette kundzutun.

Die Metapher vom Computervirus brachte der kalifornische Informatikprofessor Leonard Adleman, bekannt als Co-Autor des RSA-Verschlüsselungsalgorithmus, erst 1983 in Umlauf. Er beschrieb, wie sein Student Fred Cohen seinen Kommilitonen mit falschen Versprechen ein Programm unterjubelte, das ihm erlaubte, deren Accounts zu übernehmen. Cohens von der Fakultätsleitung genehmigtes Experiment lief genauso ab wie heute ein „Hackerangriff“ – nur dass es, wie bei akademischen Studien üblich, in einem nichtöffentlichen Netz stattfand.

Im selben Jahr machte der erste Fall Furore, in dem Computer von außen attackiert wurden. Sechs junge Männer drangen mithilfe von Akustikkopplern in Dutzende von Firmen- und

Damals ganz vorn: Akustikkoppler zur Datenübertragung per Telefon

1969 von IBM vorgestellt, war die Diskette gut 30 Jahre lang das Speichermedium schlechthin.

Behördencomputern ein – ein verblüffender Coup, denn das Jedermann-Internet war noch Zukunftsmusik. Das prominenteste Opfer war das Atomwaffenlabor Los Alamos. Dass die Aktion der Gruppe aus Milwaukee von dem Plot des in dieser Zeit veröffentlichten Films „WarGames“, in dem die Erde am Rand der nuklearen Vernichtung steht, Lichtjahre entfernt war, ging in der weltweiten Aufregung unter. Stattdessen wurde das Wort „Hacker“ zum Synonym für gemeingefährliche Burschen.

Dabei umschrieb der Begriff „Hacking“ ursprünglich etwas völlig anderes: einen harmlosen Studentenulk oder eine unkonventionelle Idee, die schnell zum Ziel führt. Herwart „Wau“ Holland-Moritz, Mitgründer des 1981 in Berlin gestarteten Chaos Computer Clubs (CCC), charakterisierte Hacker einmal als Menschen, die notfalls ihre Kaffeemaschine zum Toaster umbauen. Die Wurzeln dieser Subkultur reichen bis in die späten Fünfzigerjahre zurück, als sich Studenten am Massachusetts Institute of Technology (MIT) Rechenzeit auf sündhaft teuren Großsystemen erschlichen, um damit eine Modelleisenbahn zu steuern. Ihre Vision des freien Zugangs zu Computern für alle fand auch an anderen Elite-Unis Anhänger. Diesem Milieu entstammten viele spätere Vordenker der amerikanischen IT-Szene.

Der Privatheit verpflichtet

Der Amerikaner Steven Levy verdichtete 1984 in seinem Buch „Hackers“ die bis dahin ungeschriebenen Gesetze der Szene zu einer „Hacker-Ethik“, die sich der CCC ebenfalls zu eigen machte, später ergänzt um den Satz: „Öffentliche Daten nützen, private Daten schützen.“ Sollte ein „Chaot“ (oder eine „Haeckse“, wie Hackerinnen sich auch nennen) ein Datenleck entdecken, durch das Informationen über Kunden oder Bürger abgesaugt werden könnten, wird er oder sie dieses Wissen nicht für sich ausbeuten, sondern vor dem Problem warnen. Meistens jedenfalls. Denn es gab auch schwarze Schafe wie Karl Koch, den Gründer des Hannoveraner CCC-Stammtischs, der in der Endphase des Kalten Krieges für das Ostberliner KGB-Büro internationale Rechnernetze hackte und sich die raubkopierte Software gut bezahlen ließ.

Private Computernutzer hatten dagegen in den Achtzigern kaum etwas zu befürchten. Weil kaum jemand ständig online war, verbreitete sich Malware vor allem durch Weitergabe von Datenträgern mit (raub-)kopierten Spielen. Und selten steckte mehr dahinter als der Versuch, Leute zu ärgern oder ihnen

Foto: privat / GettyImages

Der erste Virus auf Diskette war harmlos – und lieferte dennoch den Anlass für die Gründung von G DATA.

einen Schreck einzujagen („Scareware“). Als Andreas Lüning, einer der beiden Gründer von G DATA, 1987 auf einer Diskette einen Virus für den Atari entdeckte, war er von dessen Harmlosigkeit überrascht: „Der hat nichts gemacht, außer sich selbst zu verbreiten“, erzählt er. Dabei überschrieb der Schädling jedoch ein paar Bytes, sodass ein Spiel nicht mehr startete.

Lüning durchsuchte seine Diskettensammlung und fand einen weiteren Virus. Ein Gegenmittel war leicht zu programmieren, und schon im nächsten Jahr verkaufte G DATA auf einer Messe in Düsseldorf mehr als 500 Kopien seiner Antivirus-Software für stolze 99 Mark. Bald gab es eine PC-Version für MS-DOS, und so begann die Spezialisierung der Bochumer auf IT-Sicherheit, eine damals noch kleine Nische der Computerbranche. Nur wenige Jahre später hatten die Anwender schon die Wahl zwischen einer Reihe von Virenscannern deutscher, britischer, amerikanischer, finnischer und japanischer Provenienz.

Das Schneckenrennen zwischen der jungen Branche und den Viren-Urhebern beschleunigte sich nur langsam. Noch in den frühen Neunzigern schickten Kunden infizierte Dateien per Diskette nach Bochum, wo die G DATA-Experten in aller Ruhe Abwehrcodes schrieben. Geschäftskunden bekamen einmal pro Quartal, Privatkunden einmal im Jahr ein Update auf dem Postweg.

Vereinzelt gingen spektakuläre Fälle von Malware durch die Presse: 1987 der Jerusalem-Virus, der bis zum nächsten Freitag, dem 13., untätig schlummerte, um dann alle Programmdateien zu löschen. Oder 1989 das Trojanische Pferd „Aids“, mit dem ein Biologe Geld für den Entschlüsselungscode zu erpressen versuchte – diese erste Ransomware (Erpressersoftware) der Geschichte brachte noch der Postbote ins Haus. Wirklich Tempo kam erst in die Sache, als es mehr Internetzugänge gab. Denn damit fand einerseits neue Malware auch online zu ihren Opfern, während es andererseits zugleich möglich war, Updates der Virenscanner zum Download anzubieten.

Dass Windows 95 ebenso wie der dazugehörige Internet Explorer jede Menge Angriffsfläche bot, heizte das Wettrennen weiter an. Microsoft hatte kein neues Betriebssystem entwickelt, sondern ein abwärtskompatibles: Damit die Kundschaft nicht auf einen Schlag alle Software neu kaufen musste, steckte im neuen Windows noch eine Portion alter Technik.

Der Grund war simpel: Das zuvor von IBM gemeinsam mit Microsoft entwickelte Betriebssystem OS/2, das keine Altlasten mitschleppte, war am Markt gefloppt – unter anderem wegen seiner hohen Anforderungen an die Hardware. Die PC-Hersteller lieferten sich damals einen harten Preiskampf, und die meisten Marketingleute scheuten das Thema Cybersecurity, das wenig Verkaufspotenzial bot – so war der Markt voller Geräte, die kinderleicht angreifbar waren. Zudem unternahmen weder Verbraucherschützer noch Politiker etwas, um die IT-Industrie für die Sicherheit ihrer Produkte in Haftung zu nehmen – schließlich ging es (noch) nicht um Leben und Gesundheit wie etwa bei Autos.

Davon profitierten Spezialisten wie Utimaco, G DATA, H+BEDV Datentechnik und Kryptokom, die früh auf Virenschutz und Verschlüsselung gesetzt hatten. Denn mit der zunehmenden Verbreitung von DSL-Anschlüssen ab der Jahrtausendwende wurde Cybersecurity zu einem Thema, dem sich kaum jemand entziehen konnte: Onlinehandel und Homebanking lockten Betrüger an, Filesharing-Börsen entpuppten sich als veritable Virenschleudern.

Der Wettlauf beschränkte sich nicht mehr darauf, Sicherheitslücken auszunutzen oder wieder zu stopfen und neue Viren zu programmieren oder sie zu erkennen. Die „Cracker“, also die kriminellen Hacker, entwickelten neue Tools und neue, komplexe Strategien – und jeder neue Angriffsvektor erforderte eine angepasste Abwehrmethode. Die Verteidigung wurde zur Sisyphos-Arbeit.

Im Wettlauf um Sicherheit

Mit der Zeit wurde Cybersicherheit zur Gemeinschaftsaufgabe verschiedener Akteure. Mailprovider und Webhoster begannen den Posteingang nach verseuchten Dateianhängen zu scannen, neue Übertragungsprotokolle erschwerten Betrug mittels gefälschter Websites oder das Knacken von Mail-Konten, Firmen errichteten Firewalls gegen Hack-Attacken oder schotteten sich in Virtuellen Privaten Netzen gegenüber dem offenen Internet ab.

Während sich die Sicherheitsbranche stärker ausdifferenzierte, lernten aber auch die Angreifer dazu. Sie missbrauchten beispielsweise das Internet der Dinge für Botnetz-Angriffe, um Websites durch eine Flut von Anfragen unerreichbar zu machen – was Sicherheitsspezialisten konterten, indem sie Websites hinter transparenten Barrieren versteckten.

Mittlerweile wird vieles von politischen Vorgaben bestimmt. So schreibt etwa die europäische Zahlungsdiensterichtlinie PSD2 für digitale Zahlungen eine Zwei-Faktor-Authentifizierung vor. Seit September 2019 genügt es deshalb für das Auslösen einer Online-Zahlung

nicht mehr, etwas zu wissen (PIN oder Passwort). Der Kunde muss auch etwas haben – etwa eine Girocard oder Smartwatch – oder sein, also biometrisch per Fingerabdruck oder Gesichtserkennung beweisen, dass er der Berechtigte ist. Unternehmen, die Teil Kritischer Infrastrukturen sind, unterliegen zudem den strikten Vorschriften des Bundesamtes für Sicherheit in der Informationstechnik – sie zu missachten kann teuer werden.

Doch die Angreifer geben nicht auf. Nach Beobachtung der Spezialisten von G DATA geht die Gefahr für Unternehmen allerdings nicht mehr von Einzeltätern aus, die einen Ransomware-Virus wie Emotet verbreiten, sondern von virtuellen Teams. Wenn es in den Nachrichten heißt, eine Hackergruppe habe eine Benzin-Pipeline lahmgelegt, kann man davon ausgehen, dass es sich um einen professionell eingefädelten Coup handelt, also um Organisierte Kriminalität.

So etwas beginne mit einem automatisierten Scan, erklärt Tim Berghoff, Security Evangelist bei G DATA. Ist eine Hintertür gefunden, wird das Unternehmen vor dem Coup monatelang ausgespäht. „Die Erpresser passen ihre Lösegeldforderungen an die wirtschaftlichen Verhältnisse des Unternehmens an.“ Zum Opfer könnten auch ganz normale Mittelständler werden, bei denen etwa eine wichtige Maschine von einer Software gesteuert wird, die auf einem veralteten Betriebssystem läuft. „Es gibt auch noch politische Hacks“, ergänzt Berghoffs Kollege Matthias Koll, „aber wir haben es mit einer Schattenökonomie zu tun, in der eine Arbeitsteilung herrscht wie in der normalen Wirtschaft. Es geht nur ums Geld.“

So war es auch jüngst im Fall der Colonial Pipeline im Osten der USA. Wie die Ermittlungen des FBI ergaben, war der Leitungsbetreiber, an dem unter anderem Shell beteiligt ist, Opfer von Dark Side geworden, einem Unterwelt-Unternehmen, dessen Sitz in Russland vermutet wird. Es arbeitet als IT-Dienstleister für Kriminelle – eine Art digitaler Erpressungsservice aus der Cloud. Das Geschäftsmodell der Gangster spielt sogar auf die Hackerethik an: Erpresst werden nur Firmen, die sich hohe Lösegelder leisten können – Krankenhäuser oder NGOs bleiben angeblich verschont. Immerhin konnte das FBI rund die Hälfte der erpressten Summe, mehr als zwei Millionen Dollar in Bitcoin, sicherstellen. Auf den Kosten des temporären Betriebsstillstandes bleibt Colonial aber sitzen.

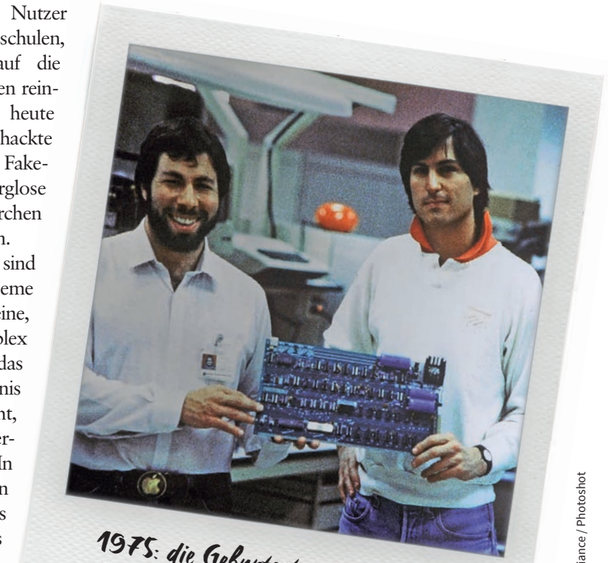
In der Verantwortung des Einzelnen

Der Marathonlauf Gut gegen Böse wird so lange weitergehen, wie es genug Opfer gibt, die nicht alle Risiken kennen und folglich nicht alles in ihrer Macht Stehende tun, um sich davor zu schützen. Schließlich nützt auch die beste Technik nicht viel, warnen Experten unisono, wenn niemand versteht, wie man sie richtig einsetzt. Cybersecurity-Spezialisten wie G DATA entwickeln sich deshalb in jüngster Zeit zu Allroundern, die nicht nur Sicherheitssoftware liefern oder mit Penetrationstests die Abwehrmechanismen ihrer Kunden auf die Probe stellen, sondern auch die Nutzer in den Betrieben schulen, damit sie nicht auf die Tricks der Kriminellen reinfallen – die nutzen heute unter anderem gehackte Informationen für Fake-Telefonanrufe, um arglose Angestellte auszuhorchen oder zu überrumpeln.

Ein Problem sind auch alte IT-Systeme und Security-Bausteine, die derart komplex sind, dass man das technische Verständnis eines Hackers braucht, um sich nicht überfordert zu fühlen. In solchen Systemen kann es durchaus vorkommen, dass selbst diejenigen, die durchaus dazu in der Lage wären, ihre E-Mails nicht verschlüsseln, weil sie davon ausgehen, dass die Empfänger sie nicht öffnen können.

Unlösbar ist diese Herausforderung aber nicht, insbesondere nicht in Bochum, das sich von den Anfängen mit Horst Görtz und G DATA mittlerweile zum weltweit wichtigsten Cluster für IT-Sicherheit entwickelt. An der Zukunft der Sicherheit wird dort auch an renommierten Instituten wie dem Horst-Görtz-Institut für IT-Sicherheit der Ruhr-Universität oder dem Max-Planck-Institut für Sicherheit und Privatsphäre gearbeitet.

Wobei es manchmal gar nicht um welterschütternde Konzepte geht. Professor Christof Paar vom Bochumer Max-Planck-Institut jedenfalls ist zuversichtlich: „Bei uns hat sich die Denke durchgesetzt, dass wir Sicherheitssoftware so schreiben müssen, dass sie von den Menschen akzeptiert wird.“ Die einfachsten Gedanken brauchen eben oft am längsten.



1975: die Geburtsstunde des ersten Apple-Computers

Foto: picture alliance / Photoshot

Foto: privat

Professor Paar, man liest oft, mit Quantencomputern werde man jede Verschlüsselung knacken können. Stimmt das, oder ist das nur Hype?
Christof Paar: Letzteres. Bis wir Quantencomputer bekommen – frühestens in 15 Jahren, nach anderen Schätzungen womöglich auch erst in 50 Jahren –, wird man damit etwa die Hälfte der Kryptoverfahren brechen können, die wir heute nutzen.

Wie das?
Es gibt zwei große Technik-Familien: symmetrische Kryptografie und Public Key. Die bestehenden Verfahren, die mit öffentlichen Schlüsseln arbeiten, kann man brechen. Die wissenschaftliche Community arbeitet jedoch längst an der sogenannten Post-Quanten-Kryptografie, also an Verfahren, die gegen Angriffe per Quantencomputer resistent sind.

Wie weit ist die Entwicklung?
Algorithmen für die neue Public-Key-Generation sind schon fast einsatzbereit. Der weltweite Wettbewerb um die beste Lösung wird derzeit von der amerikanischen Standardisierungsbehörde NIST organisiert. In fünf Jahren dürften wir ein einheitliches Verfahren haben, das man in alle Browser und Smartphones einbauen kann.

So ein Standard ändert nichts daran, dass alle Welt E-Mails unverschlüsselt verschickt. Der deutsche Alleingang mit De-Mail war trotz Edward Snowdens Enthüllungen über die NSA ein Flop. Heute überträgt selbst ein Messenger wie Whatsapp Nachrichten von einem Ende zum anderen verschlüsselt. Wie bringt man die Menschen dazu, ihre Mails zu verschlüsseln oder sich gar das Faxen abzugewöhnen?
Guter Punkt. Das Problem ist die Schnittstelle zwischen Mensch und Technik. Forscher arbeiten seit ein paar Jahren intensiv an „Usable Security“: Sicherheitslösungen müssen gebrauchstauglich werden. Die Usability von PGP (*Pretty Good Privacy, einem kostenlosen Add-on zu gängiger Mailsoftware; Anm. d. Red.*) ist eine Katastrophe.

Allzu lange hieß es, man müsse den User erziehen, aber psychologisch hat das nie funktioniert. Deshalb hat sich die Denke durchgesetzt, dass wir es umgekehrt machen müssen – also Sicherheitssoftware so schreiben, dass sie von den Menschen akzeptiert wird.

„Allzu lange hieß es, man müsse den User erziehen, aber das hat nie funktioniert.“

Ist nicht auch die deutsche Bürokratie ein Teil des Problems?
Der Anspruch, dass alles juristisch wasserfest ist, hat jedenfalls beim deutschen Signaturgesetz zu jahrelangen Diskussionen und zu einem unheimlich komplexen Konstrukt geführt. In den USA gibt es viel unkompliziertere Softwarelösungen für digitale Unterschriften, die von allen Beteiligten akzeptiert werden.

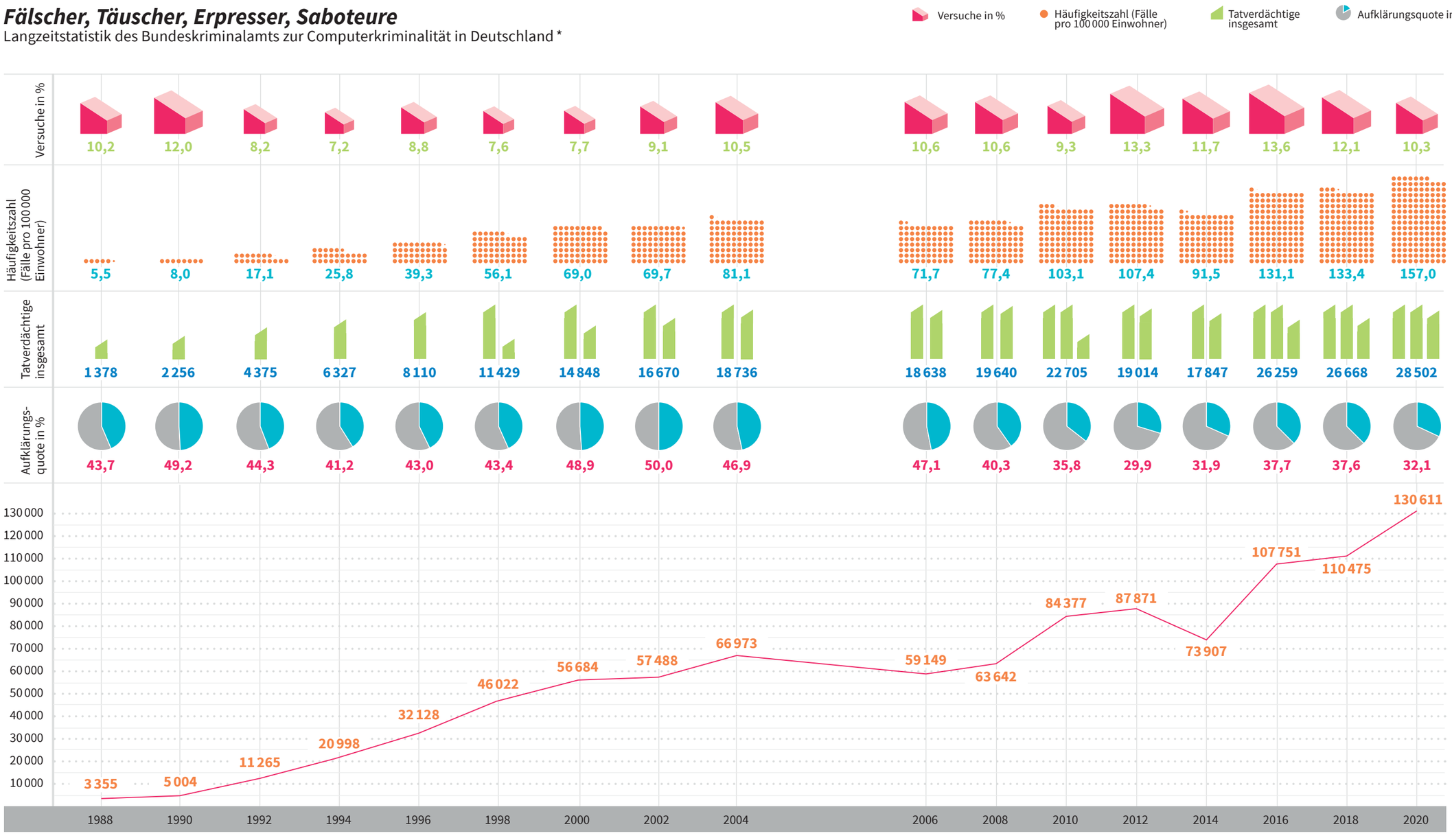
Werden wir in fünf Jahren weiter sein?
Vielleicht. Die Covid-Pandemie hatte eine heilsame Nebenwirkung: Jetzt geht ein starker Digitalisierungs(d)ruck durch die Gesellschaft. Die Absurdität der Faxe und der digitalen Unterschrift, die man anschließend auf Papier nachreichen muss, wird uns langsam bewusst.

WIR

Wie bewegen wir uns im Netz? Welche Angebote nutzen wir beruflich und privat? Welche Altersgruppe ist wie oft und wofür in der digitalen Welt unterwegs – mit welchem Endgerät, in welcher Ausstattung und wie lange pro Tag? Sind wir technisch und persönlich für den Cyberspace gerüstet? Und reichen Wissen und Schutzmaßnahmen aus?

Fälscher, Täuscher, Erpresser, Saboteure

Langzeitstatistik des Bundeskriminalamts zur Computerkriminalität in Deutschland *



Computerkriminalität ist ein sogenannter Summenschlüssel, dem verschiedene Straftaten zugeordnet sind. Er umfasst:

Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung, Datenveränderung, Computersabotage, Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen, Softwarepiraterie (private Anwendung z. B. von Computerspielen), Softwarepiraterie in Form gewerbsmäßigen Handelns, Computerbetrug.

Der Summenschlüssel „Computerkriminalität" weist Überschneidungen mit den Summelschlüsseln „Computerbetrug" und „Cybercrime im engeren Sinne" auf (beide: siehe Seite 66).

Computerbetrug umfasst die Straftaten:

betrügerisches Erlangen von Kfz, weitere Arten des Warenkreditbetrugs, Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN, Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten, Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel, Leistungskreditbetrug, sonstiger Computerbetrug, missbräuchliche Nutzung von Telekommunikationsdiensten, Abrechnungsbetrug im Gesundheitswesen, Überweisungsbetrug.

Cybercime im engeren Sinne umfasst die Straftaten:

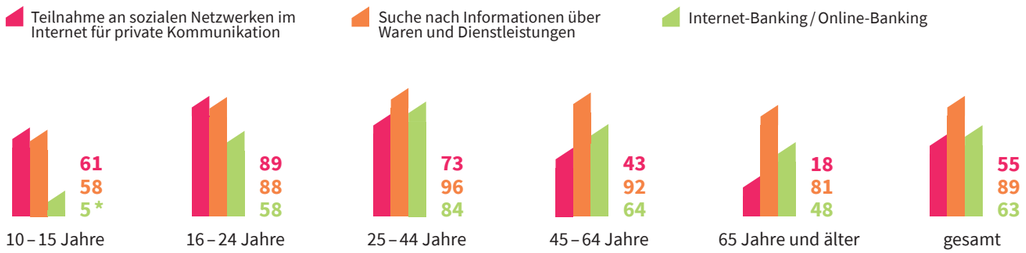
betrügerisches Erlangen von Kfz, weitere Arten des Warenkreditbetruges, Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten, Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel, Leistungskreditbetrug, sonstiger Computerbetrug, missbräuchliche Nutzung von Telekommunikationsdiensten, Abrechnungsbetrug im Gesundheitswesen, Überweisungsbetrug, Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung, Datenveränderung, Computersabotage, Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei.

Unter **„Versuche"** werden alle erfassten Versuche aus den relevanten Straftaten aufgeführt. Bei manchen Straftaten ist laut Strafgesetzbuch (StGB) schon der Versuch einer Straftat strafbar. Das ist zum Beispiel bei „Computerbetrug" der Fall.

*1987 – 1990: alte Bundesländer; 1991 – 1992: alte Bundesländer mit Gesamt-Berlin; ab 1993: Bundesgebiet insgesamt. Quelle: Bundeskriminalamt

Gefragt

Anteil der Personen mit Internet-Aktivitäten zu privaten Zwecken nach Altersgruppen; Personen *, die das Internet im ersten Quartal 2020 genutzt haben; Deutschland; in Prozent



* Aussagewert eingeschränkt, da der Zahlenwert aufgrund der Personenzahlen (50 bis unter 100 Personen) statistisch relativ unsicher ist. Quelle: Destatis

Geschädigt

Art der Straftat bei Opfern von Internetkriminalität; Befragte, die Opfer von Internetkriminalität geworden sind; Deutschland; 2020; in Prozent

	innerhalb der vergangenen 12 Monate	länger zurückliegend
Schadsoftware wie Viren / Trojaner	11	25
Phishing (Ausspionieren vertraulicher Daten)	17	15
Ransomware / Erpressersoftware	6	10
Cybermobbing	10	6
Betrug beim Onlineshopping	44	28
problematische Inhalte	8	6
Fremdzugriff auf einen Online-Account	30	23
Cyberstalking	8	6

Quellen: BSI, ProPK

Geteilt

Online-Einkäufe von Internetnutzern nach Geschlecht; Deutschland; in Prozent

Quelle: Destatis

Januar 2020

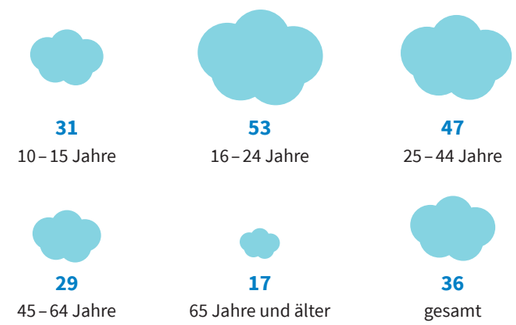
Cybercrime Timeline Deutschland 2020

Am 7.1.20 unterlagen Server eines IT-Finanz-Dienstleisters einem DDoS-Angriff mit der Folge, dass unter anderem die Webseite und die Online-Banking-Möglichkeiten einer bekannten Bank ausfielen. Kunden konnten sich nicht in ihre Konten einloggen, Überweisungen tätigen oder Daueraufträge anlegen.

Quelle: Bundeskriminalamt

Gespeichert

Nutzung von Speicherplatz (Cloud-Computing) im Internet zu privaten Zwecken in den vergangenen drei Monaten nach Altersgruppen; Deutschland; 2020; in Prozent



Quelle: Destatis

Bedroht

Persönliche Erfahrungen mit Cyberkriminalität in den vergangenen 12 Monaten; Internetnutzer ab 16 Jahren (n = 1 004); Deutschland; 2019; in Prozent *

ja	55
davon:	
Computer / Smartphone wurde mit Schadprogrammen infiziert	46
Persönliche Daten wurden ungefragt an Dritte weitergegeben.	26
beim privaten Einkauf oder Verkaufsgeschäften betrogen	19
beim Online-Banking betrogen	12
verbal massiv angegriffen oder schwer beleidigt	9
sexuell belästigt	8
In meinem Namen wurden unerwünschte E-Mails versendet.	5
Eine andere Person hat sich im Internet unter meinem Namen ausgegeben.	5
Computer / Smartphone wurden mit Ransomware infiziert.	2

* Mehrfachnennungen möglich.
Quelle: Bitkom Research

Februar 2020

Cybercrime Timeline Deutschland 2020

Am 15.2.20 wurde ein Automobilzulieferer, der unter anderem Turbolader für Audi, BMW, VW und Ferrari herstellt, Opfer eines Ransomware-Angriffes. Sowohl Standorte in Deutschland als auch im europäischen Ausland waren betroffen. Die Ransomware „Cl0p“ verschlüsselte 130 Server und 600 Clients – und auch die Back-ups.

Quelle: Bundeskriminalamt

Betroffen

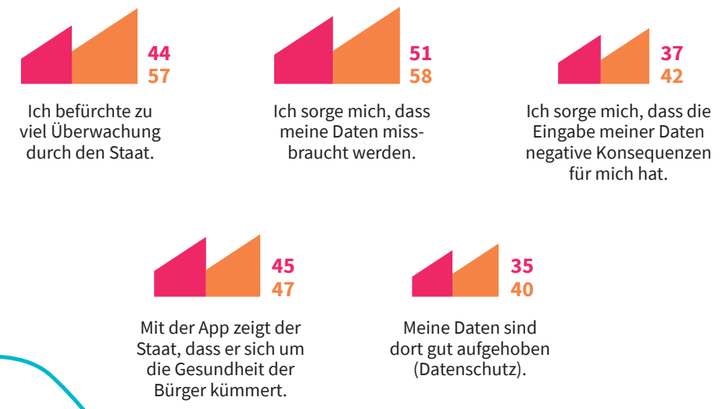
Persönliche Betroffenheit bei Straftaten und Vorkommnissen im Internet; Deutschland; 2018; in Prozent

Quelle: DIVSI

Besorgt

Vertrauen in die Corona-Warn-App; Deutschland; in Prozent

Wie bewerten Sie persönlich die Corona-Warn-App?



Quelle: Initiative D21

Behörden-Angelegenheiten

Kenntnisse und Nutzung von Online-Angeboten der öffentlichen Hand; mehr als 2 000 Verbraucher über 16 Jahre; Deutschland; 2020; in Prozent

	ist bekannt	davon bereits genutzt
elektronische Steuererklärung	68,1	48,9
Arbeitsamt- / Jobcenter-Portal	54,6	42,0
Terminbuchung beim Bürgeramt	51,6	42,2
An- / Abmeldung eines Fahrzeugs	48,6	30,1
An- / Um- / Abmeldung eines Wohnsitzes	40,6	29,6
Beantragung höchstpersönlicher Dokumente	37,5	42,3
Ausbildungsförderung	34,8	21,1
Beantragung von Elterngeld	34,7	20,2
Kita-Finder	29,0	20,6
Gewerbeanmeldungen	27,6	19,9

Quelle: Deutschland sicher im Netz e. V. (DsiN)

März 2020

Cybercrime Timeline Deutschland 2020

Am 29.3.20 stellte ein international tätiger Pharmakonzern einen Angriff mittels einer Ransomware fest. Weite Teile des weltweiten Firmennetzwerks inklusive vieler Server und Backupserver wurden verschlüsselt. Die als Datei aufgefundene Täter-Forderung deutete auf die Ransomware „Prolock“ hin.

Quelle: Bundeskriminalamt

Sicherheitsmaßnahmen

Getroffene Maßnahmen der vergangenen drei Monate, um Zugriff auf persönliche Informationen im Internet zu kontrollieren; Personen ab 10 Jahre; Deutschland; 2020; in Prozent

Deutschland · männlich · weiblich

Prüfung des Sicherheitsstatus der Webseite, auf der persönliche Informationen angegeben werden mussten

Zugang zu persönlichen Informationen beantragt, die Webseiten oder Suchmaschinen über mich gespeichert haben oder verwalten, um sie aktualisieren oder löschen zu lassen

keine der genannten Maßnahmen durchgeführt, um den Zugriff auf persönliche Informationen im Internet zu kontrollieren

Quelle: Destatis

PC-User

Marktanteile der Versionen; Deutschland; 2020; in Prozent

Windows 10	79,78
Windows 7	12,31
Windows 8.1	4,94
Windows 8	1,29
Windows XP	1,16
Windows Vista	0,49
andere	0,04

Windows hat den Support für die Versionen 7, 8, XP und Vista eingestellt. **In 2020 waren also mehr als 15 Prozent aller Windows-PC hierzulande ungeschützt.**

Quelle: Statcounter

Apple-User

Verteilung der verschiedenen iOS-Versionen (Mobile &Tablet); Deutschland; 2021; in Prozent

iOS 14.4	78,4
iOS 12.5	3,8
iOS 14.3	2,4
iOS 14.2	2,3
iOS 14.0	1,0
iOS 9.3	1,5
iOS 10.3	1,2
andere	9,4

Quelle: Statcounter

April 2020

Cybercrime Timeline Deutschland 2020

Die Verantwortlichen eines kommunalen Versorgers in Ludwigshafen stellten am 20.4.20 fest, dass sie Opfer eines Hackerangriffs geworden sind. Die von den Tätern beabsichtigte Verschlüsselung der Systeme mittels der Ransomware „Cl0p“ scheiterte zwar, ein späterer Abfluss von Daten ins Darknet konnte jedoch nicht verhindert werden.

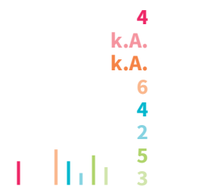
Quelle: Bundeskriminalamt

Nutzerentscheidungen

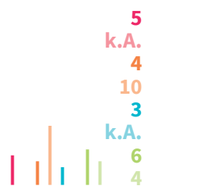
Internet der Dinge: genutzte Geräte / Systeme nach Altersgruppen und Geschlecht; Personen ab 10 Jahre; Deutschland; 2020; in Prozent

Deutschland · 10 – 15 Jahre · 16 – 24 Jahre · 25 – 44 Jahre · 45 – 64 Jahre · 65 Jahre und älter · männlich · weiblich

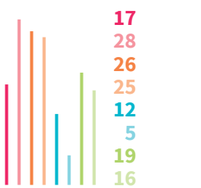
Energiemanagement von Haus / Wohnung (z. B. Thermostat, Stromzähler, Beleuchtung, einschl. Plug-ins / Software-Erweiterungen)



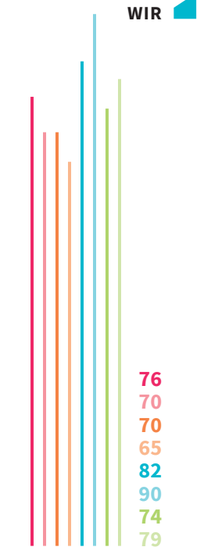
Sicherheitslösungen für Haus / Wohnung (z. B. Hausalarmanlage, Rauchmelder, Überwachungskameras, Türschlösser)



mit dem Internet verbundene Haushaltsgeräte (z. B. Saugroboter, Kühlschränke, Öfen, Kaffeemaschinen)



intelligente Lautsprecher oder Apps (z. B. Google Home, Alexa, Google Assistent, Siri, Cortana, Bixby)



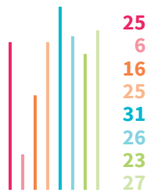
keines der genannten Geräte oder Systeme genutzt

Quelle: Destatis

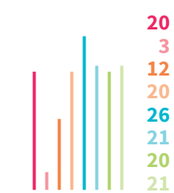
Ablehnungsgründe

Internet der Dinge: Gründe für die Nichtnutzung von Geräten / Systemen nach Altersgruppen und Geschlecht; Personen ab 10 Jahre; Deutschland; 2020; in Prozent

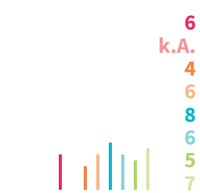
Deutschland · 10 – 15 Jahre · 16 – 24 Jahre · 25 – 44 Jahre · 45 – 64 Jahre · 65 Jahre und älter · männlich · weiblich



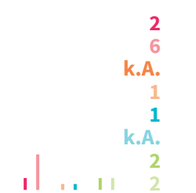
Bedenken hinsichtlich Schutz der Privatsphäre und persönlicher Daten, die über die Geräte / Systeme (u. a. über das Zuhause) generiert werden; Weitergabe personenbezogener Daten



Sicherheitsbedenken in Bezug auf IT-Sicherheit (z. B. Bedenken, dass das Gerät / System gehackt werden könnte)



Sicherheitsbedenken im Bezug auf persönlichen Schutz und gesundheitliche Aspekte (Bedenken, dass die Nutzung des Gerätes / Systems zu Unfällen, Verletzungen oder Gesundheitsproblemen führen könnte)

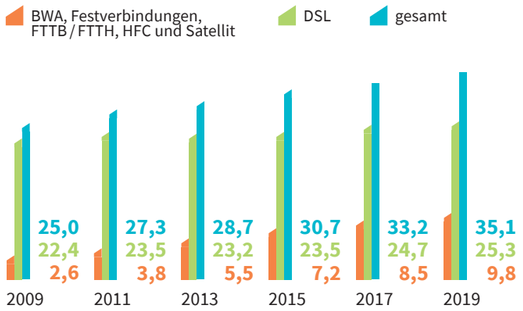


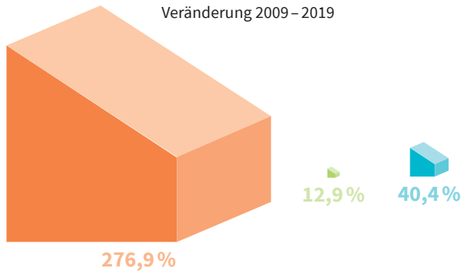
andere Gründe

Quelle: Destatis

Breitbandanschlüsse

Aktive Breitbandanschlüsse in Festnetzen; Deutschland; in Millionen



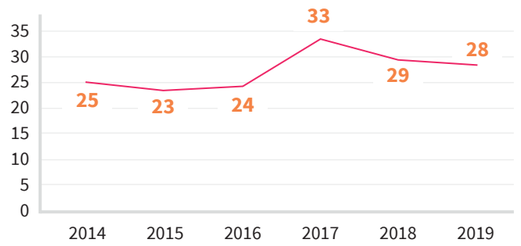


Quelle: Bundesnetzagentur

Misstrauensvotum

Vertrauen in Staat und Behörden beim Umgang mit persönlichen Daten; Anteil der Personen, die die Frage mit „sehr stark“ und „stark“ beantwortet haben; Deutschland; in Prozent

Wie stark vertrauen Sie dem Staat und den Behörden, wenn es um den Umgang mit Ihren persönlichen Daten geht?



Quelle: Bitkom e. V.

Bandbreiten

Verteilung der vermarkteten Bandbreiten bei Festnetz-Breitbandanschlüssen; 2019; in Millionen

unter 10 Mbit/s	2,9
10 bis unter 30 Mbit/s	9,6
30 bis unter 100 Mbit/s	13,4
100 Mbit/s bis unter 1 Gbit/s	9,0
1 Gbit/s und mehr	0,2
gesamt	35,1

Quelle: Bundesnetzagentur

Mai 2020

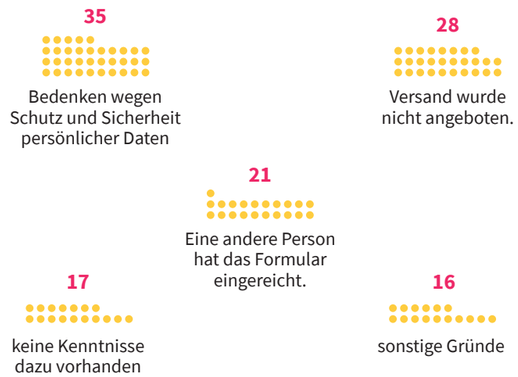
Cybercrime Timeline Deutschland 2020

Im Mai wurde bekannt, dass mehrere Forschungszentren in Europa angegriffen wurden, wodurch einige sogenannte Supercomputer in Deutschland kompromittiert wurden. Eintrittsvektor waren zuvor ausgelesene Nutzerdaten, worüber eine Backdoor installiert werden konnte. Es bestanden Verdachtsmomente, dass weitere Daten abgeflossen sind und die Rechner für das Kryptomining genutzt wurden.

Quelle: Bundeskriminalamt

Unsicherheitsgefühl

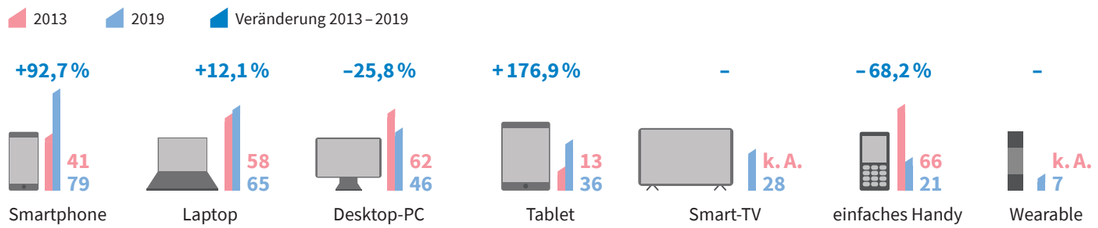
Gründe, warum ausgefüllte Formulare an eine Behörde / öffentliche Einrichtung nicht über das Internet zurückgesendet wurden; Deutschland; 2018 / 2019; in Prozent



Quelle: Destatis

Haben

Nutzung von digitalen Geräten; Personen ab 14 Jahren; Deutschland; in Prozent



Quelle: Initiative D21 e. V.

Wissen

Bekanntheitsgrad von Sicherheitsmaßnahmen; mehr als 2 000 Personen über 16 Jahre; Deutschland; 2020; in Prozent

Die bekanntesten Sicherheitsmaßnahmen:

unterschiedliche Passwörter für untersch. Zwecke	98,5
Änderung von Passwörtern	98,3
starke Passwörter	98,3
Antiviren-Programm	98,0
Update des Betriebssystems des Computers	98,0

Die unbekanntesten Sicherheitsmaßnahmen:

Inkognito-Funktion	82,7
Plug-ins zur Erhöhung der Datensicherheit (z. B. Skript-Blocker etc.)	82,1
Auslesen der E-Mail-Header	81,7

Quelle: Deutschland sicher im Netz e. V. (DsiN)

Machen

Nutzung von Sicherheitsmaßnahmen; mehr als 2 000 Personen über 16 Jahre; Deutschland; 2020; in Prozent

Die meistgenutzten Sicherheitsmaßnahmen:

Schutz des Handys mit z. B. PIN	76,1
regelmäßiges Update des Betriebssystems	75,5
Nutzung sicherer Zahlungssysteme	75,2
ständige Aktivierung eines Antiviren-Programms	72,7
Verwendung unterschiedlicher Passwörter für unterschiedliche Zwecke	72,6

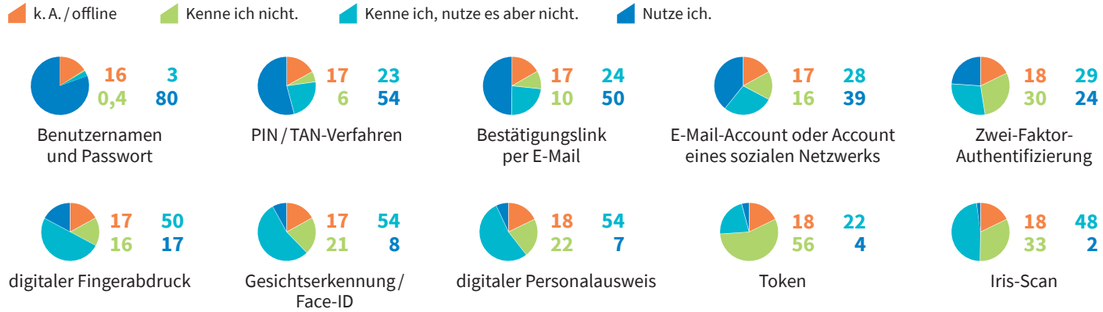
Die am wenigsten genutzten Sicherheitsmaßnahmen:

Nutzung eines Passwortmanagers	30,1
Verschlüsselung der Festplatte	29,4
Einsatz elektronischer Signaturen (z. B. durch den neuen Personalausweis)	21,9

Quelle: Deutschland sicher im Netz e. V. (DsiN)

Nutzen

Nutzung von Identifikationsverfahren im Internet; Personen ab 14 Jahren; Deutschland; 2019; in Prozent



Quelle: Initiative D21 e. V.

Juni 2020
Cybercrime Timeline Deutschland 2020

Über einen bösartigen E-Mail-Anhang wurden am 11.6.20 weite Teile der IT einer mittelständischen Unternehmensgruppe mit Sitz in Süddeutschland, die unter anderem im Handel mit Baumaschinen tätig ist und allein in Deutschland über 38 Niederlassungen verfügt, verschlüsselt. Für die Entschlüsselung forderten die Täter ein Lösegeld im siebenstelligen Eurobereich – zahlbar in Bitcoin.

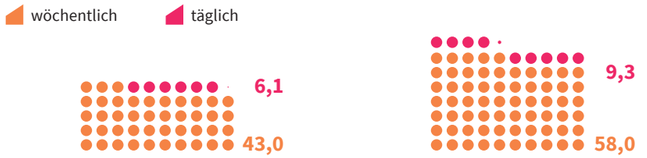
Quelle: Bundeskriminalamt

Heimlich
Befall durch Schadsoftware bei Smartphones; Internetnutzer ab 10 Jahren; Deutschland; 2020; in Prozent

haben das Smartphone genutzt, um für private Zwecke ins Internet zu gelangen	91
darunter: Verlust von Informationen, Dokumenten, Bildern oder anderen Daten auf dem Smartphone durch Schadsoftware:	
nein	81
ja	3
weiß nicht	5

Quelle: Destatis

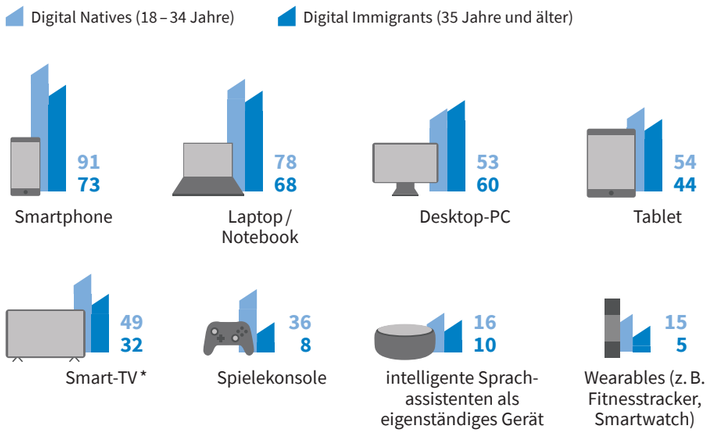
Erheblich
Wöchentliche und tägliche Internetnutzung nach Altersgruppen; Deutschland; 2019; in Stunden



Digital Immigrants (35 Jahre und älter) | Digital Natives (18 – 34 Jahre)

Quelle: Postbank

Förmlich
Digitale Nutzung von Endgeräten nach Altersgruppen; Deutschland; 2020; in Prozent



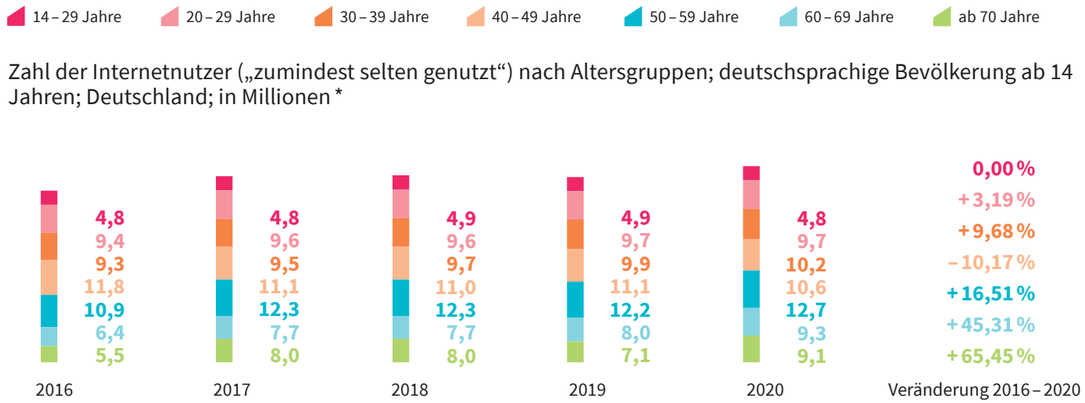
* internet- und netzfähige Fernsehgeräte. Quelle: Postbank

Juli 2020
Cybercrime Timeline Deutschland 2020

Ein börsennotiertes Unternehmen, das u. a. im Bereich der Halbleiterherstellung tätig ist, wurde Anfang Juli Opfer der Ransomware „MAZE“. Folge: Die IT-Infrastruktur des Unternehmens wurde verschlüsselt, die Täter drohten bei Nichtzahlung der geforderten Summe mit der Veröffentlichung von Kundendaten. Allein am Standort in Deutschland waren 750 Mitarbeitende durch den Angriff nicht mehr arbeitsfähig.

Quelle: Bundeskriminalamt

Alljährlich, täglich, minütlich
Internetnutzung



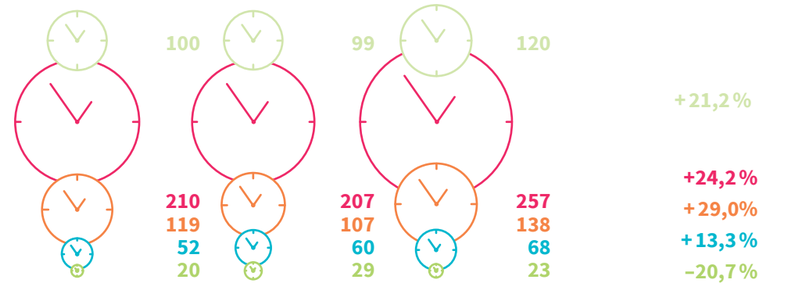
Zahl der Internetnutzer („zumindest selten genutzt“) nach Altersgruppen; deutschsprachige Bevölkerung ab 14 Jahren; Deutschland; in Millionen *

	2016	2017	2018	2019	2020	Veränderung 2016 – 2020
14 – 29 Jahre	4,8	4,8	4,9	4,9	4,8	0,00 %
20 – 29 Jahre	9,4	9,6	9,6	9,7	9,7	+ 3,19 %
30 – 39 Jahre	9,3	9,5	9,7	9,9	10,2	+ 9,68 %
40 – 49 Jahre	11,8	11,1	11,0	11,1	10,6	– 10,17 %
50 – 59 Jahre	10,9	12,3	12,3	12,2	12,7	+ 16,51 %
60 – 69 Jahre	6,4	7,7	7,7	8,0	9,3	+ 45,31 %
ab 70 Jahre	5,5	8,0	8,0	7,1	9,1	+ 65,45 %

Tägliche Internetnutzung (Tagesreichweite *) nach Altersgruppen; deutschsprachige Bevölkerung ab 14 Jahren; Deutschland; in Millionen **

	2018	2019	2020	Veränderung 2018 – 2020
14 – 29 Jahre	4,7	4,9	4,7	0,00 %
20 – 29 Jahre	9,1	9,4	9,4	+ 3,30 %
30 – 39 Jahre	8,7	8,7	9,1	+ 4,60 %
40 – 49 Jahre	8,4	9,1	8,8	+ 4,76 %
50 – 59 Jahre	8,8	9,0	8,8	0,00 %
60 – 69 Jahre	4,7	5,3	5,7	+ 21,28 %
ab 70 Jahre	3,6	4,3	4,2	+ 16,67 %

Mediales Internet: tägliche Nutzungsdauer nach Altersgruppen; deutschsprachige Bevölkerung ab 14 Jahren; Deutschland; in Minuten



2018 | 2019 | 2020 | Veränderung 2019 – 2020

* Die Tagesreichweite umfasst alle Personen, die zumindest für ein Viertelstunden-Intervall eine Tätigkeit ausüben. ** Daten wurden auf die Gesamtbevölkerung hochgerechnet. Quelle: ARD / ZDF

August 2020
Cybercrime Timeline Deutschland 2020

Die Gruppierung „Fancy Bear“ * machte mit einem DDoS-Angriff bei einem deutschen Finanzinstitut auf sich aufmerksam und flankierte die Drohung weiterer Angriffe mit einer Erpressungsmail. Bereits in den Jahren 2017 und 2019 konnten gleich gelagerte Fälle mutmaßlich dieser Gruppierung in Deutschland festgestellt werden.

* Wird nach Einschätzung von Geheimdiensten vom russischen Militärgeheimdienst gesteuert. Quelle: Bundeskriminalamt

Mehr Fälle, weniger Aufklärung I
Statistik zum Computerbetrug * in Deutschland

	Zahl erfasster Fälle	Häufigkeitszahl (Fälle pro 100 000 Einwohner)	Versuche Zahl	Versuche in %	Aufklärungsquote in %
2016	84 060	102,3	13 851	16,5	38,8
2017	86 372	104,7	13 415	15,5	40,5
2018	89 901	108,6	12 919	14,4	38,0
2019	100 814	121,4	13 741	13,6	31,9
2020	105 049	126,3	12 933	12,3	32,8

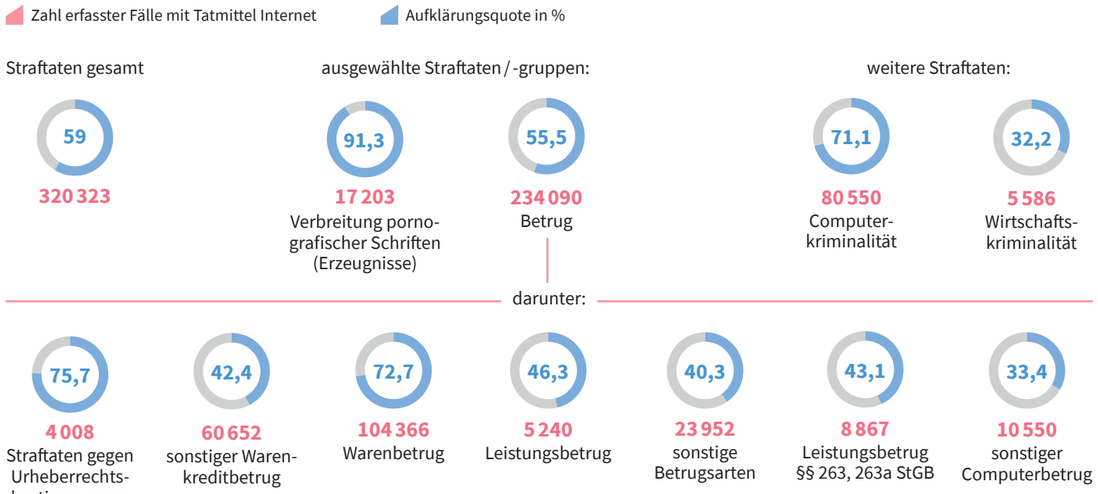
* Informationen zur Abgrenzung zwischen „Computerkriminalität“, „Computerbetrug“ und „Cybercrime“ im engeren Sinne“ siehe Randspalte auf Seit 57. Quelle: Bundeskriminalamt

Mehr Fälle, weniger Aufklärung II
Zeitliche Entwicklung und Aufklärung von Cybercrime im engeren Sinne * in Deutschland

	Zahl erfasster Fälle	Zahl aufgeklärter Fälle	Aufklärungsquote in %
2016	82 649	31 962	38,7
2018	87 106	33 862	38,9
2019	100 514	32 489	32,3
2020	108 474	35 390	32,6

* Informationen zur Abgrenzung zwischen „Computerkriminalität“, „Computerbetrug“ und „Cybercrime“ im engeren Sinne“ siehe Randspalte auf Seit 57. Quelle: Bundeskriminalamt

Pornografie, Betrug und Computerkriminalität
Ausgewählte Straftaten / -gruppen mit Tatmittel Internet * in Deutschland; 2020



* Die Zusammenstellung ausgewählter Straftaten hat keinen Anspruch auf Vollständigkeit, deckt aber die größten Bereiche der Polizeilichen Kriminalstatistik ab.
Quelle: Bundeskriminalamt

Verunsichert bei E-Mails und vertraulichen Daten
Unsicherheitsgefühl im Internet; mehr als 2 000 Befragte über 16 Jahre; Deutschland; in Prozent

Dabei fühlen sich die Befragten am unsichersten:	2019	2020	Veränderung 2019 – 2020
Öffnen von Anhängen in E-Mails	57,8	56,7	– 1,9 %
Austausch vertraulicher Inhalte	38,6	40,7	5,4 %
in sozialen Netzwerken	38,3	39,5	3,1 %
Herunterladen von Software (keine Updates)	38,8	36,4	– 6,2 %
Dating-Anwendungen	34,6	36,2	4,6 %

Dabei fühlen sich die Befragten am wenigsten unsicher:	2019	2020	Veränderung 2019 – 2020
Recherchieren in Suchmaschinen und Nachschlagewerken	14,2	16,5	16,2 %
Nutzung von (Weiter-) Bildungsangeboten (z. B. Webinare etc.)	12,2	16,3	33,6 %
Lesen von Nachrichtenseiten	9,0	12,4	37,8 %

Quelle: Deutschland sicher im Netz e. V. (DsiN)

Durch Fälschungen hereingelegt
IT-Sicherheitsvorfälle; mehr als 2 000 Befragte über 16 Jahre; Deutschland; in Prozent

Die häufigsten IT-Sicherheitsvorfälle:	2019	2020	Veränderung 2019 – 2020
Phishing-Versuch	30,7	28,8	– 6,2 %
Erhalt infizierter E-Mails / Anhänge / Weblinks	26,3	23,2	– 11,8 %
Betrug beim Online-Einkauf / bei Online-Buchungen	8,3	10,7	28,9 %
Betrug beim Bezahlen im Internet (Zahlungsvorgang)	5,0	9,7	94,0 %
Ausspähen von Zugangsdaten zu Online-Plattformen	8,6	9,6	11,6 %

Die seltensten IT-Sicherheitsvorfälle:	2019	2020	Veränderung 2019 – 2020
Betrug mit virtuellen Währungen (z. B. Bitcoins)	4,2	7,4	76,2 %
unbefugter Zugriff auf verlorenes oder gestohlenes Gerät	3,9	6,7	71,8 %
Vorfälle bei der Nutzung von Online-Angeboten der öffentlichen Hand	k. A.	6,5	k. A.
Manipulation von Hausvernetzung (Smart Home, z. B. Smart-TV)	3,3	6,1	84,8 %

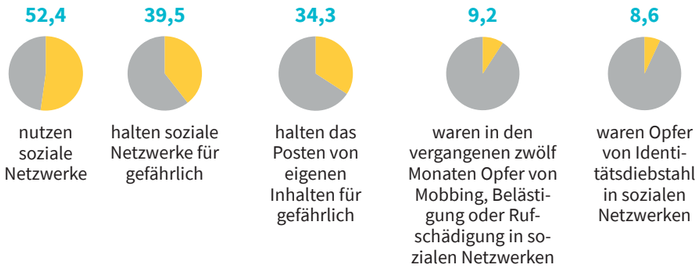
Quelle: Deutschland sicher im Netz e. V. (DsiN)

September 2020
Cybercrime Timeline Deutschland 2020

Ein Universitätsklinikum in NRW wurde Mitte September Opfer eines Ransomware-Angriffs. Durch den Angriff wurden 30 Server verschlüsselt und die Klinik-IT lahmgelegt. Akute Fälle konnten nicht aufgenommen und mussten auf umliegende Krankenhäuser verteilt werden.

Quelle: Bundeskriminalamt

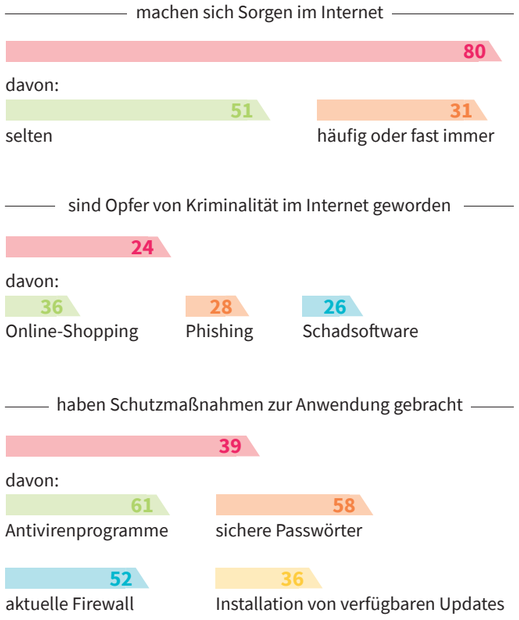
In sozialen Netzen gemobbt und belästigt
Gefahren und Vorkommnisse bei der Nutzung sozialer Medien; mehr als 2 000 Befragte über 16 Jahre; Deutschland; 2020; in Prozent



Quelle: Deutschland sicher im Netz e. V. (DsiN)

Wenig Schutz

Umfrage zur Sicherheit im Internet; Deutschland; 2020; in Prozent



Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Viele Attacken

Entwicklung der Bedrohung durch Cyberattacken; Deutschland, Österreich, Schweiz; 2020

Zahl der von G DATA entdeckten Cyberattacken	
2019	4,9 Mio.
2020	16,1 Mio.
Veränderung in %	228,6

Zahl der uniquen Samples von Emotet, der gefährlichsten Malware 2020 *	
2019	70 883
2020	888 793
Veränderung in %	1 154,8

*Am 27. Januar 2021 gab das BKA bekannt, die Emotet-Schadsoftware zerschlagen zu haben. Quellen: G DATA, Bundeskriminalamt

Top-Angriffe

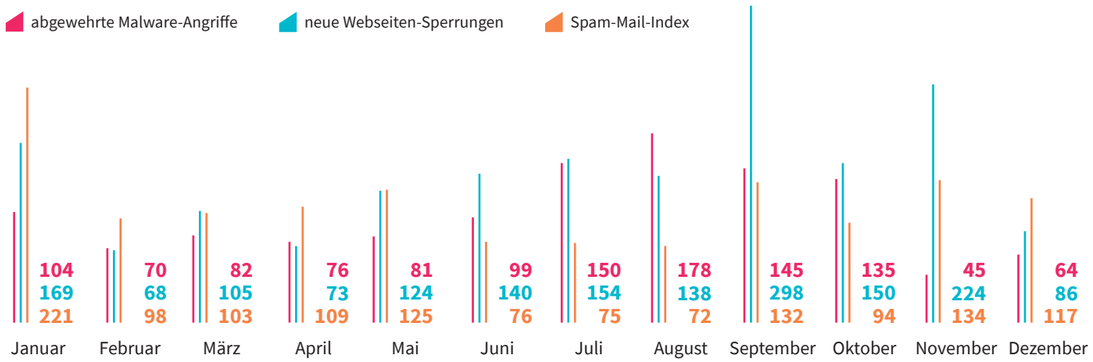
Zahl der häufigsten Malware-Samples *; Deutschland, Österreich, Schweiz; 2020

Emotet (Malware-Distributor)	888 793
Qbot (Remote-Access-Trojaner)	98 800
Urelas (Downloader)	64 136

* Am 27. Januar 2021 gab das BKA bekannt, die Emotet-Schadsoftware zerschlagen zu haben. **Remote-Access-Trojaner** sind Programme, die eine verdeckte Überwachung oder den unberechtigten Zugriff auf einen Opfer-PC ermöglichen. Primäre Funktionalität von einem **Downloader** ist das Herunterladen von Inhalten wie Konfigurations- oder Befehlsinformationen, verschiedenen Dateien, anderer Malware, irreführenden Apps, sekundären Komponenten des bestehenden Angriffs oder Upgrades für diesen. Quellen: G DATA, Bundeskriminalamt

Top-Abwehr

Abwehr-Indizes *; Deutschland; 2020; Indexpunkte (Basisjahr: 2018 = 100)



* Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) erhebt fortlaufend die sogenannten Abwehr-Indizes, die das Aufkommen und die Entwicklung von Malware-Angriffen per E-Mail auf die Netze des Bundes sowie die Menge präventiver Sperrungen von maliziösen Webseiten messen. Auch die in den Netzen des Bundes festgestellte Zahl der Spam-Mails ist Gegenstand regelmäßiger Auswertungen des BSI. Quelle: Bundeskriminalamt

Im Angebot: Tools für Kriminelle

Cybercrime as a Service: Angebote im Darknet; Deutschland; 2020; in US-Dollar

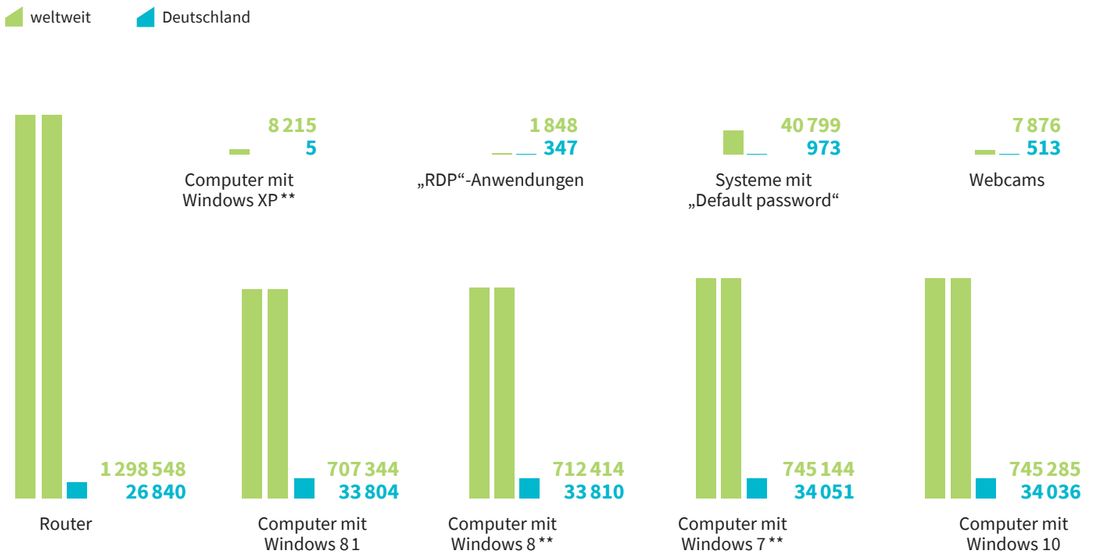
Angebot:	Nutzungsbedingungen:	Preis in US-Dollar:
BankingTrojaner	Kauf: Desktop-Version	1 000 – 10 000
	Kauf: mobile Version	1 000 – 10 000
RAT * (Remote-Administration-Tool)	Kauf	89 – 530
	Miete pro Monat	ca. 3 000
Mining Bots *	Miete pro Monat	50 – 150
Crypting	Kauf	20 – 100
	Wochen-Abo mit 50 Crypts pro Tag	360 – 500
Spam	pro Spam	10 ct – 4
DDoS as a Service	pro Monat bei Miete	80 – 1 500
Bulletproof-Hosting *	Miete pro Monat: Shared	5 – 50
	Miete pro Monat: Dedicated	50 – 700

* **Mining Bots** (Botnets) sind automatisierte Programme, die von ihren Schöpfern in Form von Codezeilen entwickelt wurden und sich in das Computergerät eines Benutzers einschleichen sollen. Botnets nutzen die Rechenleistung des Geräts, den Strom und die Internetbandbreite, um eine bestimmte Kryptowährung zu schürfen. **Bulletproof-Hosting** ist ein Service, der von einigen Hosting-Firmen (z. B. Cloud-, Dedicated-, Domain- oder Web-Hosting) angeboten wird, die ihren Kunden beträchtliche Nachsicht gewähren – etwa bei der Art des Materials, das sie hochladen und verbreiten dürfen, oder bei den Aktivitäten, die sie mit ihrem gekauften Host durchführen können, ohne aufgrund von Beschwerden und (formalen) Missbrauchsberichten vom Netz genommen zu werden. Spammer, Cyberkriminelle, Blackhat-Hacker und Anbieter von Online-Glücksspielen oder illegaler Pornografie gehören zu den Nutzern solcher Hosting-Firmen, da sie wissen, dass sie für das Fortbestehen ihrer Aktivitäten besser geeignet sind als normales Hosting. Als **Crypting** wird die Verschlüsselung / Verfremdung des Schadcodes bezeichnet. Ziel ist es, den Code ständig weiterzuentwickeln und die Komplexität zu steigern, um dadurch möglichst lange von Sicherheitssystemen unentdeckt zu bleiben. Ein **RAT** oder Remote-Administration-Tool ist eine Software, die einer Person die volle Kontrolle über ein technisches Gerät gibt, und zwar aus der Ferne. Das RAT gibt dem Benutzer Zugriff auf Ihr System, so, als ob er physischen Zugriff auf Ihr Gerät hätte. Mit diesem Zugriff kann die Person auf Ihre Dateien zugreifen, Ihre Kamera verwenden und sogar Ihr Gerät ein- und ausschalten.

Quelle: Bundeskriminalamt

Unsicher

Zahl der via Shodan über das Internet auffindbaren Internet-connected devices *; 2021



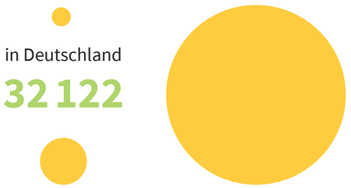
* Shodan ist eine Suchmaschine, die ungeschützte Anwendungen oder Systeme („Internet-connected devices") mit nur geringen Sicherheitsvorkehrungen im Internet findet. Geräte / Anwendungen / Systeme, die über shodan.io gefunden werden, bieten leichte Ziele für missbräuchliche Angriffe aus dem Bereich Cybercrime. ** Versionen, die nicht mehr supported werden. Quelle: Shodan.io

Unerkannt
Identifizierung einer Microsoft-Exchange-Sicherheitslücke durch Shodan *; weltweit; 2021

Datum, an dem das Bundesamt für Sicherheit und Informationstechnik (BSI) in Deutschland eine Warnung über Systemfehler bei Microsoft-Exchange-Servern veröffentlichte („Sofortiges Handeln notwendig“):
5.3.21

Datum, an dem Shodan.io eine entsprechende Suchanfrage durchführte
13.4.21

Zahl der betroffenen Systeme, die bei dieser Suchanfrage identifiziert wurden:



* Die Zahlen zeigen durch Shodan.io identifizierte, also online auffindbare Systeme mit öffentlich adressierbaren Microsoft-Exchange-Servern. Quellen: Shodan.io, BSI

Unabsehbar
Android-Schadsoftware; Österreich, Deutschland, Schweiz; 2019

Gesamtanzahl Android-Schadsoftware	18 792 234
neue Android-Malware (2019)	4 180 000
neue schädliche Apps pro Tag	10 000

= eine infizierte Android-App alle 7,5 Sekunden

Quellen: G DATA, Bundeskriminalamt

November 2020
Cybercrime Timeline Deutschland 2020

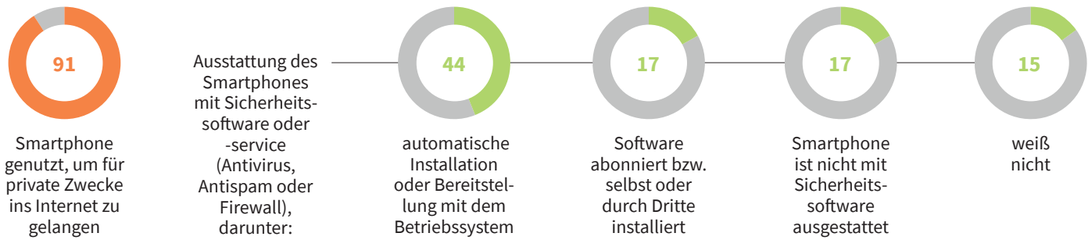
Eine Landesrundfunkanstalt wurde am 7.11.20 Opfer einer DDoS-Attacke. Der Angriff führte zum zeitweisen Ausfall der Webseite, sodass keine neuen redaktionellen Beiträge veröffentlicht und keine digitalen Angebote aktualisiert werden konnten.

Quelle: Bundeskriminalamt

Unerfreulich
Neue Android-Schadsoftware im Zeitverlauf; Deutschland, Österreich, Schweiz; in Millionen

Quelle: G DATA

Unbedarft
Smartphone: Umfrage zu Schutzmaßnahmen; Internetnutzer ab 10 Jahre, die das Internet in den vergangenen drei Monaten nutzten; Deutschland; 2020; in Prozent



Quelle: Destatis

Oktober 2020
Cybercrime Timeline Deutschland 2020

Am 9.10.20 stellte eines der größten Unternehmen der Computerspielbranche mit Hauptsitz in Frankfurt/M. fest, dass seine gesamte interne Windows-Infrastruktur verschlüsselt wurde. Lösegeldforderungen fanden sich als Datei auf Servern und Arbeitsplatzrechnern und als Ausdruck in jedem Drucker. Es konnte auf die Ransomware „Egregor“ geschlossen werden. Die Erpresser gaben an, Daten nicht nur verschlüsselt, sondern auch kopiert zu haben. Mit einer schrittweisen Veröffentlichung von internen Daten wurde gedroht, was im weiteren Verlauf auch erfolgte.

Quelle: Bundeskriminalamt

Ungenügend
Verwendete Schutzmaßnahmen im Internet; deutschsprachige Bevölkerung im Alter von 14 bis 69 Jahren; Deutschland; 2020; in Prozent *

aktuelles Virenschutzprogramm	57
sichere Passwörter	48
aktuelle Firewall	47
Zwei-Faktor-Authentisierung	33
sichere https-Verbindung bei der Übertragung persönlicher Daten	31
regelmäßiges Ändern von Passwörtern	28
Einstellung der automatischen Installation von Updates	25
regelmäßiges Anlegen von Sicherheitskopien	20
verschlüsselte E-Mail-Kommunikation	18
Verzicht auf Online-Banking	10
Verzicht auf soziale Medien	10

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

Unbelehrbar
Sicherheitsmaßnahmen im Internet; deutschsprachige Wohnbevölkerung zwischen 14 und 24 Jahren; Deutschland; in Prozent

	2014	2018	Veränderung 2014 – 2018
Ich habe einen Virenscanner installiert.	86	75	– 12,8 %
Ich sichere alle meine Geräte mit einem persönlichen Passwort.	75	74	– 1,3 %
Ich habe meine Firewall aktiviert.	80	62	– 22,5 %
Ich benutze Pop-up oder Adblocker .	53	58	9,4 %
Ich benutze immer verschiedene Passwörter .	49	57	16,3 %
Ich aktualisiere meine persönlichen Sicherheitseinstellungen bei Social-Media-Angeboten.	69	48	– 30,4 %
Ich nutze nur Seiten, bei denen ich weiß, dass sie sicher sind.	67	46	– 31,3 %
Ich gebe keine persönlichen Daten preis.	56	41	– 26,8 %
Ich achte darauf, keine Dateien hochzuladen.	67	33	– 50,7 %
Ich achte darauf, keine Dateien herunterzuladen.	45	29	– 35,6 %
Ich mache falsche bzw. irreführende persönliche Angaben.	18	25	38,9 %

Quelle: DIVSI

Ungeschützt
Verwendete elektronische Identifikationsverfahren bei Online-Diensten; Internetnutzer ab 10 Jahre, die das Internet in den vergangenen drei Monaten nutzten; Deutschland; 2020; in Prozent

Quelle: Destatis

Eher inkonsequent

Kenntnis und Umsetzung von Sicherheitsempfehlungen zum Schutz vor Kriminalität im Internet; Deutschland; 2020; in Prozent *

kein Opfer von Cyberkriminalität · einmaliges Opfer von Cyberkriminalität · mehrfaches Opfer von Cyberkriminalität

Kennen Sie die aktuellen Sicherheitsempfehlungen zum Schutz vor Kriminalität im Internet?

- 32 / 23 / 23 — Nein, sind mir noch nie begegnet.
- 42 / 57 / 57 — jJa, habe ich schon mal gesehen.
- 11 / 12 / 12 — Ja, ich achte genau darauf.
- 15 / 9 / 9 — weiß nicht / keine Angabe

Inwiefern halten Sie sich an diese Sicherheitsempfehlungen?

- 40 / 42 / 33 — direkte Umsetzung der Sicherheits-empfehlungen
- 16 / 15 / 31 — Umsetzung nur im Problemfall
- 41 / 42 / 32 — Umsetzung, wenn es gerade passt
- 1 / 1 / 4 — keine Umsetzung
- 2 / k. A. / 2 — weiß nicht / keine Angabe

Quellen: Bundesamt für Sicherheit in der Informationstechnik (BSI), Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK)

Eher einig

Bedingungen für die Nutzung eines Angebots im Internet; Deutschland; 2020; Basis n = 2 995; in Prozent

Damit ich ein digitales Angebot regelmäßig nutze, muss es …

- **96** … vertrauenswürdig sein
- **96** … glaubwürdig sein
- **96** … seriös sein
- **96** … meine Daten schützen
- **93** … einen Nutzen haben
- **91** … aktuell sein
- **91** … transparent sein
- **80** … mich gut unterhalten
- **79** … mir optisch gut gefallen
- **77** … mich inspirieren
- **41** … von vielen Personen genutzt werden

Quelle: Bundesverband Digitale Wirtschaft e. V. (BVDW)

Eher vorsichtig

Vertrauen und Vorsicht im Internet; Deutschland; 2020; Top-2-Angaben auf einer Skala von (1) trifft voll und ganz zu bis (4) trifft überhaupt nicht zu; in Prozent

Generell vertraue ich dem Internet – da kann nicht viel schiefgehen.	30
Ich bin im Netz sehr vorsichtig, weil man nie weiß, wen man wirklich vor sich hat.	89

Quelle: Bundesverband Digitale Wirtschaft e. V. (BVDW)

Dezember 2020

Cybercrime Timeline Deutschland 2020

Am 12.12.20 wurde bei einem börsennotierten Unternehmen der Lebensmittel- und Kosmetikbranche ein Angriff auf die weltweite IT-Infrastruktur festgestellt. Große Teile der Systeme wurden verschlüsselt, sodass ein Produktions- und Kommunikationsausfall nicht verhindert werden konnte. Der entstandene wirtschaftliche Schaden wurde auf mehrere Millionen Euro pro Ausfalltag geschätzt. Über ein schadhaftes Excel-Dokument wurde weitere Schadsoftware wie ein Remote-Access-Trojaner (RAT) und die „Cl0p"-Ransomware nachgeladen und ausgeführt. Quelle: Bundeskriminalamt

Eher uneinheitlich

Kenntnisse, Verhalten und Einstellungen in Bezug auf Internetsicherheit; Deutschland; 2019 / 2020; in Prozent

37 — Anteil der 14- bis 29-Jährigen, bei denen der Schutz ihrer Daten z. B. mit sicheren oder unterschiedlichen Passwörtern oder aktueller Anti-Virensoftware im Alltag meistens untergeht

22 — Anteil der 50+-Jährigen, bei denen der Schutz ihrer Daten z. B. mit sicheren oder unterschiedlichen Passwörtern oder aktueller Anti-Virensoftware im Alltag meistens untergeht

38,9 — Anteil der 10- bis 15-Jährigen, die keine Bedenken haben, dass Online-Aktivitäten aufgezeichnet werden, um maßgeschneiderte Werbung anzubieten

4,8 — Anteil der 65+-Jährigen, die keine Bedenken haben, dass Online-Aktivitäten aufgezeichnet werden, um maßgeschneiderte Werbung anzubieten

Anteil der Deutschen, die der Meinung sind, für einen verantwortungsvollen Umgang mit persönlichen Daten seien hauptsächlich verantwortlich …

… die Nutzer eines Dienstes	… die Anbieter eines Dienstes	… die Politik, durch entsprechende Gesetze
43	34	19

Anteil der Deutschen, …

- **9,4** … die beim Ausspähen von Zugangsdaten zum Online-Banking betroffen waren
- **35,4** … die Online-Banking für gefährlich halten
- **63,0** … die auf verschlüsselte Datenverbindung beim Online-Banking achten

Anteil der Deutschen, …

- **42,7** … die in puncto Sicherheit skeptisch sind und deshalb bewusst auf einige Angebote verzichten
- **34,8** … die sich mit Sicherheitsfragen befassen, bevor sie sich für ein neues digitales Angebot entscheiden

Anteil der Deutschen, …

- **41** … die sich Sorgen machen, dass ihre Daten im Internet missbraucht werden könnten
- **40** … die sich gut vor Viren und Datenmissbrauch geschützt fühlen

- **91,8** — Anteil der 16- bis 24-Jährigen, denen der Zweck und Einsatz von Cookies bekannt ist
- **53,1** — Anteil der 65+-Jährigen, denen der Zweck und Einsatz von Cookies bekannt ist

Anteil der Deutschen, …

- **7,0** … die vernetzte Haustechnik (Licht, Heizung usw.) nutzen
- **32,4** … die vernetzte Haustechnik für gefährlich halten
- **6,1** … die in diesem Jahr einen Cyberangriff erlebt haben
- **12,7** … die vernetzte Unterhaltungselektronik (Smart TVs, Sprach-Assistenten usw.) nutzen
- **36,0** … die vernetzte Unterhaltungselektronik für gefährlich halten

Quelle: Deutschland sicher im Netz e. V. (DsiN) · Quelle: Destatis · Quelle: Initiative D21 e. V. · Quelle: Statista Global Consumer Survey

„Ideale Regeln kann es nicht geben.“

Der Bundesdatenschutzbeauftragte Ulrich Kelber über Vertrauen in Technologie, Kontrollillusionen und darüber, wie man mit Whatsapp ganz schnell kriminell werden kann.

Text: Peter Lau

„Ich brauche für die Digitalisierung ein gewisses Vertrauen – ohne geht es nicht.“

Foto: Bundesregierung/Kugler

Ulrich Kelber ist in vielerlei Hinsicht eine Ausnahme, aber eines sticht besonders hervor: Im Gegensatz zu seinen Kollegen in den Bundesländern, die überwiegend eine juristische Ausbildung haben, ist der oberste deutsche Datenschützer tatsächlich vom Fach – er ist Diplom-Informatiker. Zudem hat der 1968 in Bamberg geborene Politiker vor seiner Zeit im Bundestag, in dem er von September 2000 bis Januar 2019 saß, in der Branche gearbeitet. Er kennt den Bereich also sogar aus der Praxis.

Kelber wuchs in Bonn auf, wo er immer noch lebt, hat fünf Kinder und steht seit dem 7. Januar 2019 als Bundesbeauftragter für den Datenschutz und die Informationsfreiheit an der Spitze der Behörde. Bereits 2000 griff er die Initiative des früheren Bundestagsabgeordneten Norbert Gansel zum Gläsernen Bundestagsabgeordneten auf. Er veröffentlichte als erster Bundestagsabgeordneter seine Steuerbescheide, berichtete über alle Dienstreisen und sein Abstimmungsverhalten zu allen Themen und listet seit 2009 auch sämtliche Gespräche mit Lobbyisten auf.

Die Videokonferenz mit Ulrich Kelber, der im Homeoffice war, fand über die Plattform der BDBOS (Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben) statt. Sie war also sicher, datengeschützt – und es gab nicht ein einziges technisches Problem.

Herr Kelber, als Datenschutzbeauftragter sind Sie quasi verpflichtet, misstrauisch zu sein. Mussten Sie das erst lernen, oder liegt Ihnen das im Blut?
Nein, gar nicht. Ich lebe eigentlich nach dem Prinzip: Vertraue bis zum Beweis des Gegenteils. Aber das gilt für Menschen, nicht für Organisationen oder Software.

Würden Sie sagen, dass das Internet und die IT-Welt grundsätzlich weniger vertrauenswürdig sind als unsere alltägliche Welt?
Sie sind anonymer, undurchschaubarer und komplexer. Wenn ich zum Beispiel einer Einzelperson im Alltag eine Information gebe, kann ich in der Regel überblicken, welche Auswirkungen das haben wird. Bei einem Algorithmus dagegen weiß ich nicht, welche Informationen er über mich schon aus anderen Quellen hat und wie er in der Kombination neue Erkenntnisse über mich gewinnt. Es überfordert Menschen, das im Alltag alles zu überblicken.

Aber lässt sich dieses Problem über Regeln und Gesetze lösen? Anders gesagt: Wäre eine Situation vorstellbar, in der ich als IT-Nutzer machen kann, was immer ich will, ohne weiter darüber nachdenken zu müssen?
Nein, das glaube ich nicht. Die Menschen müssen sich zumindest darauf verlassen können, dass es Regeln gibt, die sie grundsätzlich schützen.

Wie sähen für Sie solche Regeln im Idealfall aus?
Ideale Regeln kann es nicht geben. Einfach schon deshalb, weil es immer ein Gleichgewicht zwischen verschiedenen Zielen und Interessen geben muss. Ich kann natürlich bestimmte Szenarien mit einzelnen Gesetzen regeln, aber dann gelten sie eben nur für diesen einen Fall – und wenn der sich ändert, bräuchte ich schon wieder ein neues Gesetz.

Deshalb müssen gute Gesetze flexibel sein, sodass sie auch auf zukünftige Technologien anwendbar sind. Außerdem sollen sie den Behörden und Gerichten ermöglichen, selber die Details zu regeln.

Gibt es so etwas bereits?
Ich halte die Europäische Datenschutz-Grundverordnung (DSGVO) zurzeit für den Goldstandard. Einige Länder, die sich ebenfalls daran orientieren, haben allerdings einzelne Felder schon weiterentwickelt. In Kalifornien etwa hat man sich auch um das Thema Profiling gekümmert, was bei uns noch fehlt.

Die DSGVO ist grundsätzlich eine gute Sache, aber insbesondere für kleinere Unternehmen bedeutet sie einen enormen Aufwand, für die viele weder die Ressourcen noch das Wissen haben. Und das in der KMU-Hochburg Deutschland! Was würden Sie einem Unternehmer mit begrenzten Möglichkeiten raten, um seine Situation zu verbessern?
Unternehmer sollten sich anschauen, wo überhaupt die Verarbeitung personenbezogener Daten notwendig ist. Manchmal fällt erst dann auf, dass viele Daten gar nicht für einen konkreten Zweck erhoben werden.

Die Daten, die erhoben werden, sollten natürlich technisch gegen den Zugriff von Unbefugten gesichert sein. Meine Kolleginnen und Kollegen von den Landesdatenschutzbehörden haben dazu viele Hinweise auf ihren Internetseiten und beraten bei Fragen.

Die Gesetzeslage in Europa ist zwar tatsächlich vergleichsweise gut, aber es zeigt sich auch, dass die schönsten Gesetze nichts bringen, wenn sie nicht umgesetzt werden. Irland zum Beispiel verschleppt immer wieder Klagen, weil es die Konzerne nicht verärgern möchte. (1)
Ja, das stimmt. Das hat viele Gründe: Es liegt an der Unterbesetzung der zuständigen Behörde, am irischen Verfahrensrecht und wohl auch an der Rechtsauffassung meiner irischen Kollegin. Und das führt in der Tat Teile der Datenschutz-Grundverordnung ad absurdum.

Da müssen wir stärker Druck auf das Land ausüben, was wir zurzeit auch tun: Wir haben zum Beispiel neue Verfahrensregeln entwickelt, sodass in Zukunft bei Urteilen in einzelnen Ländern auch die Datenschutzbeauftragten anderer Länder Einfluss nehmen können. Natürlich muss in Irland selbst ebenfalls etwas passieren, aber da bin ich ganz zuversichtlich: Nach einer Anhörung im irischen Parlament waren sich die beiden Regierungsfraktionen einig, dass sich etwas ändern muss.

Manchmal wirkt es, als wäre gerade in der Verwaltung das Misstrauen gegenüber dem Datenschutz besonders hoch. Im vergangenen August drängte sich dieser Eindruck förmlich auf, als Ihre Behörde vom Innenministerium verklagt wurde (2). Ganz zu schweigen davon, dass die Beamten damals unmissverständlich klarmachten, dass sie auch den Bürgern grundsätzlich misstrauen.
Das mag von außen so wirken, aber auch hier gilt es, Interessen auszugleichen. Einerseits müssen die Auskunftsrechte der Bürgerinnen und Bürger erfüllt werden. Andererseits muss aber auch dafür gesorgt werden, dass eine Behörde nicht durch Missbrauch lahmgelegt wird.

Ein ähnlicher Fall sind die Überwachungsgesetze: Der Staat muss selbstverständlich in der Lage sein zu handeln, darf seine Bürgerinnen und Bürger aber nicht unter Generalverdacht stellen und von allen Daten sammeln.

Die Idee scheint zu sein: Die Technik gibt mir die Möglichkeit, etwas zu kontrollieren – also kontrolliere ich es.
Ja, aber dieser Gedanke ist falsch: Schwächen Sie die Verschlüsselung gängiger Tools, erwischen Sie vielleicht einige unbeholfene Kriminelle und daneben, aufgrund von Fehlern, etliche unbescholtene Menschen – aber nicht die Profis. Denn die bauen sich dann eigene Verschlüsselungen. Das ist schließlich keine Hexerei.

Kurz gesagt: Auf die Technik allein kann man sich nicht verlassen?
Ja, einerseits. Andererseits ist ein gewisses Vertrauen in die Technik heute trotzdem unbedingt nötig. Schließlich haben wir nicht mehr wie früher nur einen PC – wir sind von Geräten umgeben. Und ich werde nicht jedes dieser Geräte jederzeit evaluieren können, weder selber noch über Dritte. Also muss ich denen vertrauen können, die sie in den Verkehr bringen. Sonst kann ich keine Videokamera an meinen Eingang stellen, keinen intelligenten Thermostat installieren und so weiter. Ich brauche für die Digitalisierung ein gewisses Vertrauen – ohne geht es nicht.

Wir sind von Geräten umgeben. Und ich werde nicht jedes dieser Geräte jederzeit evaluieren können, weder selbst noch über Dritte. Also muss ich denen vertrauen können, die sie in den Verkehr bringen.

(1): Damit europaweit agierende Konzerne nicht mit den Datenschützern aller 27 Länder verhandeln müssen, wurde in der Europäischen Datenschutz-Grundverordnung festgelegt, dass das Land, in dem die europäische Firmenzentrale liegt, für sämtliche Datenschutzverfahren zuständig ist. Bei Facebook, Google und Twitter ist das Irland.

(2): Die Plattform FragDenStaat unterstützt basierend auf dem Informationsfreiheitsgesetz (IFG) Personen dabei, ihnen rechtlich zustehende Anträge auf Zugang zu amtlichen Informationen zu stellen. Das Innenministerium hat dafür lange die Angabe einer Postadresse vorausgesetzt, bis der Datenschutzbeauftragte 2020 die Behörden anwies, darauf zu verzichten, um nicht mehr Daten als nötig einzufordern. Das Ministerium hat dagegen geklagt, weil es fürchtet, von anonymen Anfragen überflutet zu werden.

Das ist viel verlangt, denn einerseits hören wir ständig von Cyberkriminalität, die zu einem immer größeren Problem wird – kidnappen die demnächst meinen Kühlschrank? Und auf der anderen Seite, noch viel schlimmer: Einige Firmen sammeln ganz legal Unmengen von Daten über uns, die letztlich nur dazu dienen, uns zu manipulieren. Bis dann die Frage im Raum steht: Entscheidet Facebook die nächste Bundestagswahl?
Das ist tatsächlich ein Problem, aber es muss in vielen Fällen keines sein. Wenn ich Dienstleister habe und Services nutze, denen ich vertrauen kann, und ein Mobilgerät, von dem ich weiß, dass es mich fragt, bevor es meine Daten an Dritte weitergibt, kann ich schon sehr viel machen.

Das kann sein, aber woher soll ich denn wissen, wem ich vertrauen kann? Da bräuchte ich eigentlich ein Gütesiegel.
Da haben Sie recht, vertrauenswürdige Zertifikate werden in Zukunft tatsächlich ganz wichtig sein. Deshalb hoffe ich auch, dass noch in diesem Jahr die Deutsche Akkreditierungsstelle zusammen mit den Datenschutzaufsichtsbehörden erste Zertifizierungen für einzelne, datenschutzkonforme Dienste ausstellen kann.

Das wird ein Stempel sein, der für die gesamte europäische Union gilt und zwei Vorteile hat: Zum einen hilft er natürlich den Endverbrauchern, sich bei ihren Entscheidungen zu orientieren. Daneben können aber auch alle, die eigene Services und Dienstleistungen entwickeln, sofort sehen, welche Bausteine sie selbst für datenschutzkonforme und sichere Angebote nutzen können.

Für welche Anbieter ist so etwas interessant? Sicherlich nicht für all jene, die von dem Verkauf der Metadaten ihrer Nutzer leben.
Nach Schrems 2 (3) wären zum Beispiel bestimmte Cloud-Services, die ihr Geld mit ihrer eigentlichen Dienstleistung verdienen, sehr froh, wenn sie sich zertifizieren könnten. Denn dann wäre klar, dass sie datenschutzkonform sind und es keine Probleme mit internationalen Transfers gibt.

Gut, das wird zumindest in der Wirtschaft und Verwaltung für mehr Klarheit sorgen. Aber was mache ich als Einzelperson, die keine IT-Abteilung hat, die sich um so was kümmert, und außerdem weder Lust noch Zeit hat, sich mit Datenschutz und IT-Sicherheit zu beschäftigen? Wie komme ich als Einzelperson sicher, ungetrackt und einfach durch die IT-Welt?
Zuerst einmal kommen Sie als Einzelperson zumindest mit der Datenschutz-Grundverordnung in der Regel nicht in Konflikt, denn da gibt es die Haushaltsausnahme für rein private Zwecke.

Aber auch da gibt es natürlich Ausnahmen, wenn Sie zum Beispiel auf Whatsapp den Zugriff auf das ganze Adressbuch erlauben – wenn da 1000 Adressen drin sind, überschreitet das die private Nutzung. Das ist, als würden Sie auf der Straße Fotokopien Ihres persönlichen Telefonbuchs an wildfremde Leute verteilen – das geht auch nicht.

Das wird man bei Facebook nicht gern hören.
Ansonsten reicht oft gesunder Menschenverstand: Würde ich bestimmte Daten Menschen anvertrauen, die ich zufällig getroffen habe und die ich nicht kenne? Manchmal kann man mit wenig Recherche herausfinden, ob es Alternativen gibt. Und wenn es die gibt – nicht davor drücken! Nach dem Motto: Ich habe zwar 20 Koch-Apps auf meinem Smartphone, aber ein zweiter Messenger ist mir zu viel.

Auch hilfreich: ein Passwort-Manager. Einmal anschaffen, sich dafür ein Passwort überlegen – und der Rest geht automatisch. Und schließlich: Wenn es eine Zwei-Faktor-Authentifizierungsoption gibt – einfach machen!

Also letztlich die Trägheit überwinden?
Ganz sicher. Ich würde mir aber auch wünschen, dass Sicherheit und Datenschutz noch stärker zum gängigen Service-Angebot gehören. Also dass zum Beispiel Anbieter von Betriebssystemen oder Dienstleistungen die Nutzer gleich zu Anfang durch die Konfiguration einer vorinstallierten Sicherheitsebene führen. Das hilft!

Denken Sie an die Router: Vor 15 Jahren wurden die offen ausgeliefert – ich musste ein Spezialist sein, um sie zu schließen. Als dann Haftungsprobleme auftraten, wurden sie geschlossen ausgeliefert, und nun müssen sie aktiv Ports öffnen, SSIDs sichtbar machen, Passwortverschlüsselung ausschalten und so weiter.

Und was ist das Ergebnis? Vor 15 Jahren gab es um mich herum ganz viele offene Router – ich habe meinem Nachbarn eine Nachricht auf seinen Desktop gelegt: „Hallo, ich bin es, Ulrich von nebenan. Das ist gefährlich, was du da machst, ruf mich mal an.“ Heute geht das nicht mehr, denn nahezu jedes WLAN ist gesichert.

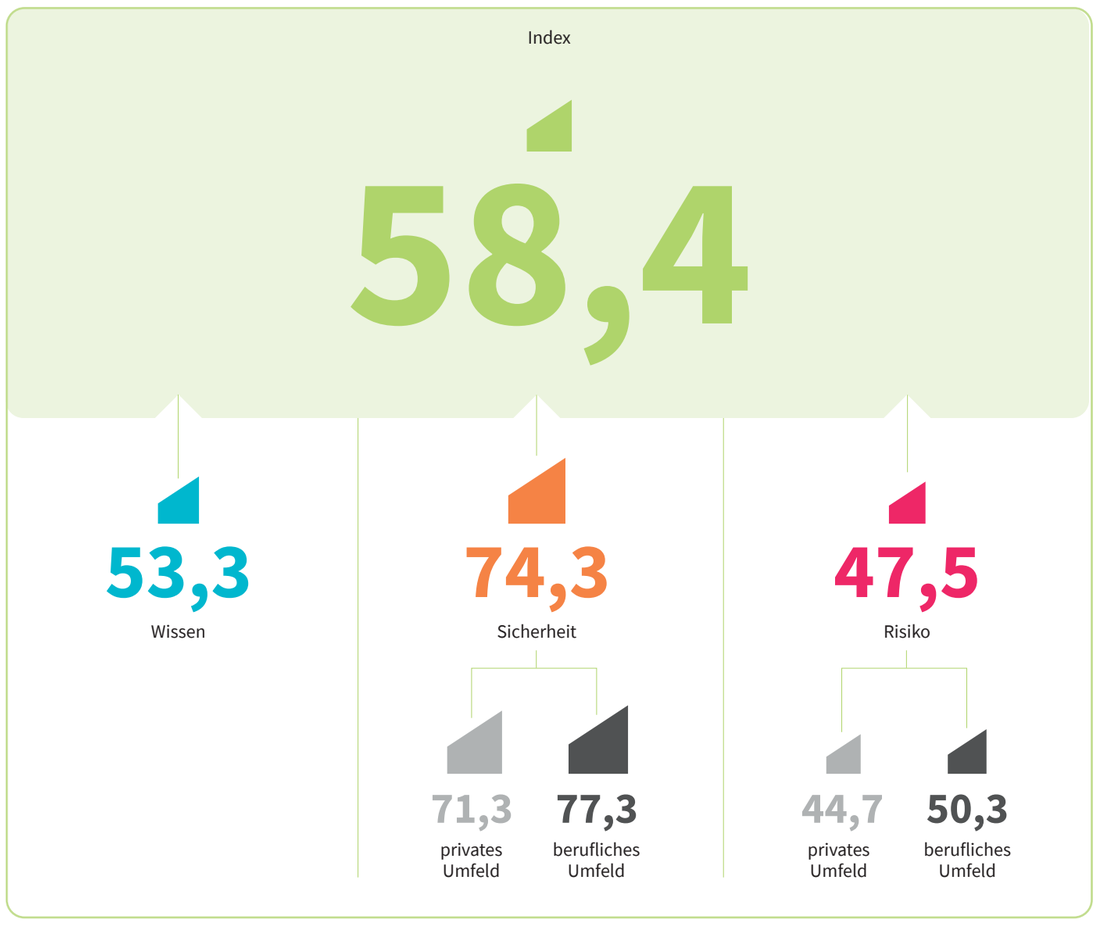
(3): Urteil des Europäischen Gerichtshofs im Juli 2020, das das bisherige Vorgehen bei internationalen Datentransfers für ungültig erklärt hat.

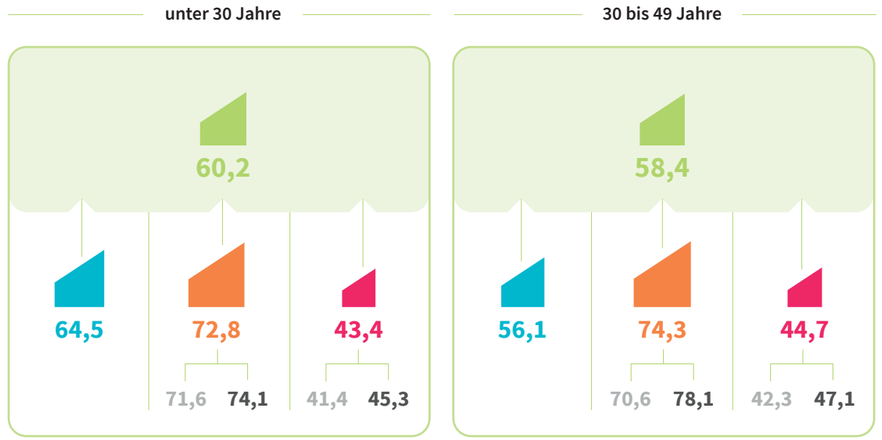
G DATA INDEX – CYBERSICHERHEIT

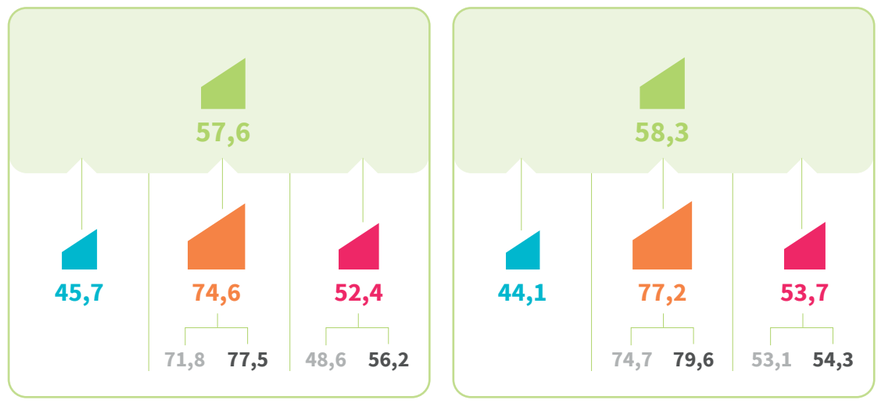
Wie steht es um die IT-Sicherheit in Deutschland – beruflich und privat? Fühlen wir uns im Umgang mit Daten kompetent und informiert und sowohl im Homeoffice als auch am Arbeitsplatz ausreichend geschützt? Wie unterscheidet sich unsere Wahrnehmung – je nach Alter und Geschlecht? Der G DATA Index gibt Auskunft.

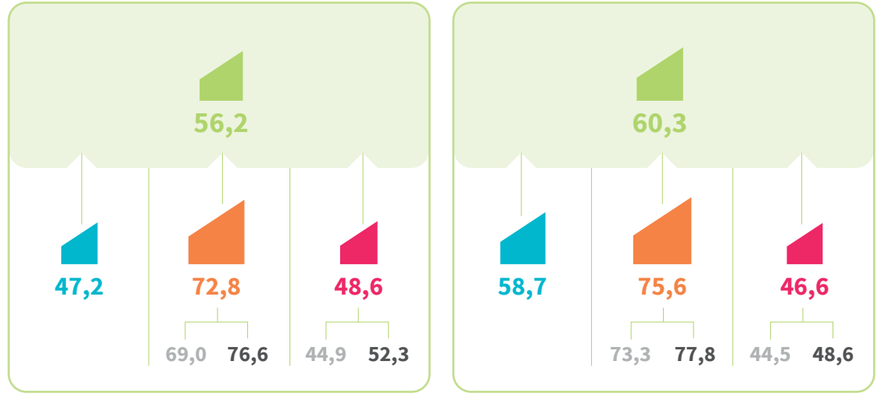
Luft nach oben

G DATA Index – Cybersicherheit; Arbeitnehmer in Deutschland; 2021; Indexpunkte: 0 = geringe gefühlte Sicherheit; 100 = sehr hohe gefühlte Sicherheit









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).

Quelle: Statista im Auftrag von G DATA

Fühlen Sie sich sicher im Netz?

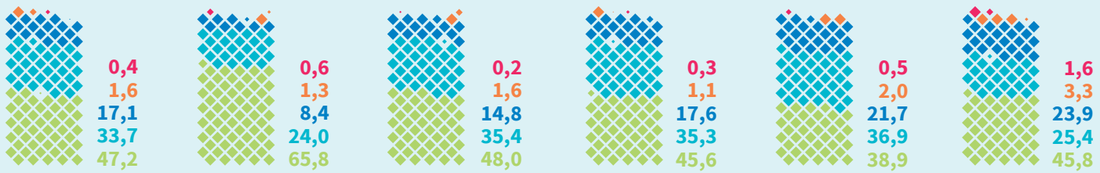
In einer repräsentativen Umfrage im März / April 2021 gaben mehr als 5000 Menschen zwischen 18 und 75 Jahren in Deutschland Auskunft über ihr Wissen, ihre Einschätzungen und ihre Erfahrungen im Umgang mit IT. Fühlen sie sich sicher? Wie verhalten sie sich in kritischen Situationen? Vertrauen sie Behörden, Arbeitgebern, sich selbst?

Von souverän bis sorglos

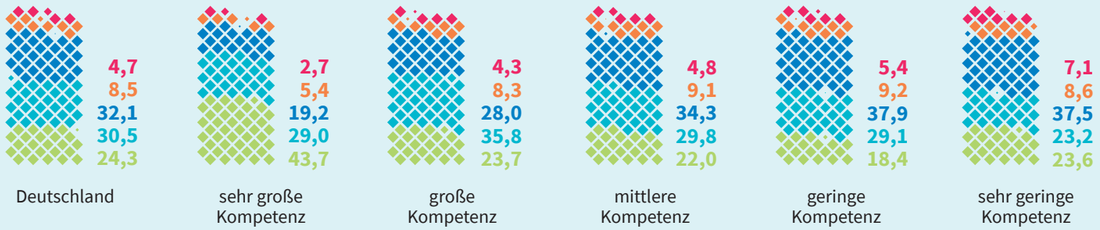
Einschätzung von Aussagen rund um IT-Sicherheit nach persönlicher Kompetenz; Arbeitnehmer in Deutschland; 2021; in Prozent

„Inwieweit treffen die folgenden Aussagen auf Sie zu?“

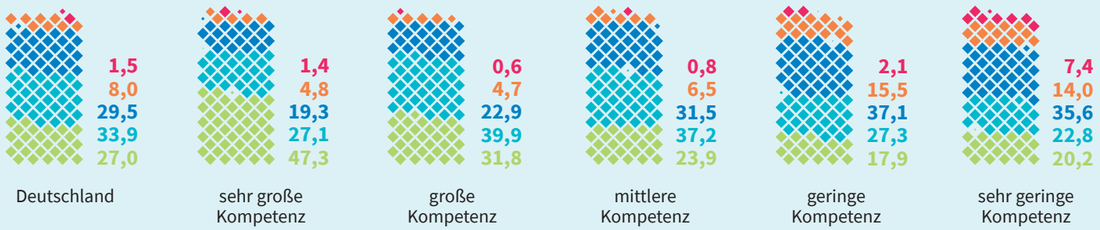
Sicherheit im Internet ist mir im Allgemeinen sehr wichtig.



IT-Sicherheit sollte in meinem Unternehmen einen höheren Stellenwert einnehmen als bisher.



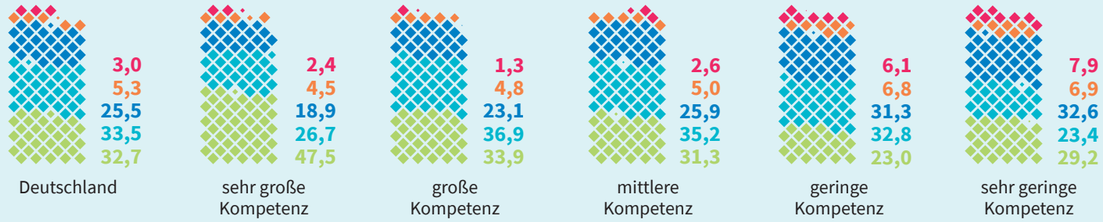
Ich überprüfe regelmäßig die Sicherheits- und Schutzmaßnahmen auf meinen privat verwendeten Geräten (z. B. Mobiltelefon, Tablet, Laptop, PC).



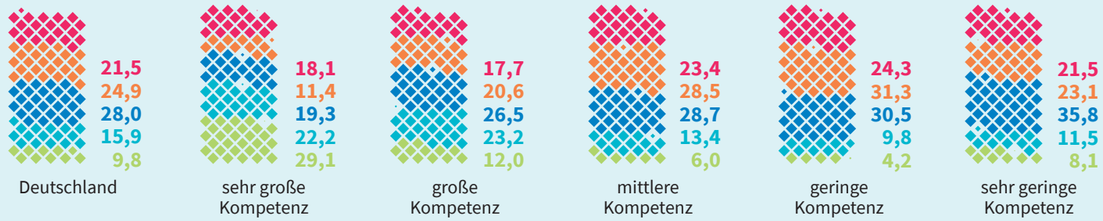
Befragte … in Deutschland mit (nach eigener Einschätzung) sehr großer … bis sehr geringer IT-Kompetenz

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

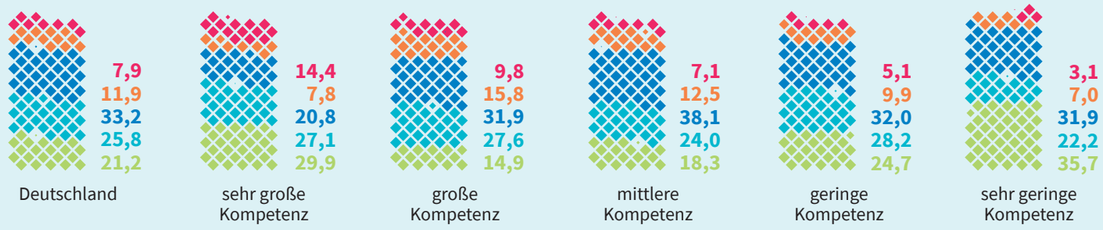
Wenn ich meine privaten Geräte für die Arbeit nutze, befolge ich die Sicherheitsmaßnahmen und Verhaltensweisen dafür sehr genau. (nur Befragte, die ihre privaten Geräte auch für die Arbeit nutzen dürfen)



Die häufigen Warnungen vor Cyberkriminalität oder Hacker-Angriffen halte ich für unnötige Panikmache.



IT-Sicherheit ist für mich als Mitarbeiter kein Thema, dafür sind Experten zuständig.



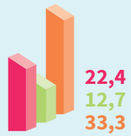
Quelle: Statista im Auftrag von G DATA

Wer hilft bei einem Verdachtsfall im Privaten oder Büro?

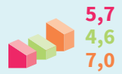
Ansprechpartner bei verdächtiger Situation im Internet im privaten Umfeld und im Büro nach Geschlecht und Altersgruppen; Arbeitnehmer in Deutschland; 2021; in Prozent

Deutschland · männlich · weiblich

im privaten Umfeld

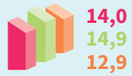


22,4 · 12,7 · 33,3 — Ich wende mich an meine/n Partner/in.

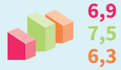


5,7 · 4,6 · 7,0 — Ich wende mich an mein/e Kind/er (nur Befragte, die Kinder haben).

3,3 · 3,4 · 3,2 — Ich wende mich an meine Eltern.

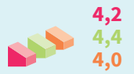


14,0 · 14,9 · 12,9 — Ich wende mich an Bekannte/Freunde (ausgenommen Arbeitskollegen).

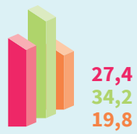


6,9 · 7,5 · 6,3 — Ich wende mich an Arbeitskollegen oder meinen Chef.

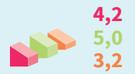
11,9 · 13,4 · 10,2 — Ich wende mich an einen externen IT-Dienstleister.



4,2 · 4,4 · 4,0 — Ich wende mich an jemand anderen.

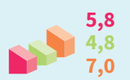


27,4 · 34,2 · 19,8 — Ich probiere trotz Unsicherheiten, das Problem selbst zu lösen.



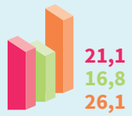
4,2 · 5,0 · 3,2 — Ich ignoriere das Problem, da ich meinen Sicherheitsprogrammen vertraue.

im beruflichen Umfeld

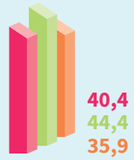


5,8 · 4,8 · 7,0 — Ich wende mich an meine/n Partner/in.

12,8 · 10,7 · 15,2 — Ich wende mich an Arbeitskollegen (ausgenommen Chef).



21,1 · 16,8 · 26,1 — Ich wende mich an meinen Chef.

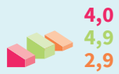


40,4 · 44,4 · 35,9 — Ich wende mich an meine IT-Abteilung.

7,4 · 8,2 · 6,5 — Ich wende mich an einen externen IT-Dienstleister.

2,8 · 3,1 · 2,5 — Ich wende mich an jemand anderen.

5,7 · 7,2 · 4,0 — Ich probiere trotz Unsicherheit, das Problem zu lösen.



4,0 · 4,9 · 2,9 — Ich ignoriere das Problem, da ich meinen Sicherheitsprogrammen vertraue.

20,0 Anteil der Befragten unter 30 Jahren, die sich an Arbeitskollegen wenden

9,5 Anteil der Befragten von 50 bis 64 Jahren, die sich an Arbeitskollegen wenden

27,1 Anteil der Befragten unter 30 Jahren, die sich an die IT-Abteilung wenden

45,8 Anteil der Befragten von 50 bis 64 Jahren, die sich an die IT-Abteilung wenden

3,8 Anteil der Befragten unter 30 Jahren, die trotz Unsicherheiten probieren, das Problem selbst zu lösen

6,2 Anteil der Befragten von 50 bis 64 Jahren, die trotz Unsicherheiten probieren, das Problem selbst zu lösen

Quelle: Statista im Auftrag von G DATA

Wer hilft bei einem Verdachtsfall im Homeoffice?

Ansprechpartner bei verdächtiger Situation im Internet im Homeoffice nach Unternehmensgröße, Homeoffice-Möglichkeit und nach persönlicher Kompetenz; Arbeitnehmer in Deutschland, die im Homeoffice arbeiten; 2021; in Prozent

Deutschland · unter 50 Mitarbeiter · 50 bis 999 Mitarbeiter · 1 000 und mehr Mitarbeiter · teilweise im Homeoffice · komplett im Homeoffice

9,8 · 13,0 · 10,5 · 4,9 · 11,4 · 7,1 — Ich wende mich an meine/n Partner/in.

3,0 · 3,0 · 3,5 · 2,0 · 3,5 · 2,1 — Ich wende mich an mein/e Kind/er (nur Befragte, die Kinder haben).

3,1 · 3,6 · 3,7 · 1,5 · 3,7 · 2,1 — Ich wende mich an meine Eltern.

7,2 · 5,7 · 9,5 · 4,8 · 8,1 · 5,6 — Ich wende mich an Bekannte/Freunde (ausgenommen Arbeitskollegen).

9,9 · 9,3 · 11,5 · 8,0 · 10,4 · 9,2 — Ich wende mich an Arbeitskollegen (ausgenommen Chef).

10,0 · 14,3 · 8,6 · 7,6 · 10,2 · 9,6 — Ich wende mich an meinen Chef.

38,0 · 22,0 · 36,6 · 58,9 · 35,6 · 42,0 — Ich wende mich an meine IT-Abteilung.

6,3 · 10,1 · 5,7 · 3,0 · 6,8 · 5,4 — Ich wende mich an einen externen IT-Dienstleister.

2,1 · 3,7 · 1,5 · 1,2 · 1,7 · 2,7 — Ich wende mich an jemand anderen.

8,6 · 13,2 · 7,1 · 6,1 · 7,1 · 11,2 — Ich probiere trotz Unsicherheiten, das Problem selbst zu lösen.

2,0 · 2,3 · 1,7 · 2,1 · 1,5 · 2,9 — Ich ignoriere das Problem, da ich meinen Sicherheitsprogrammen vertraue.

Anteil der Befragten mit sehr großer Kompetenz, die sich an ihre IT-Abteilung wenden ***22,2***

Anteil der Befragten mit großer Kompetenz, die sich an ihre IT-Abteilung wenden ***34,6***

Anteil der Befragten mit mittlerer Kompetenz, die sich an ihre IT-Abteilung wenden ***45,2***

Anteil der Befragten mit geringer Kompetenz, die sich an ihre IT-Abteilung wenden ***47,5***

Anteil der Befragten mit sehr geringer Kompetenz, die sich an ihre IT-Abteilung wenden ***30,6***

Anteil der Befragten unter 30 Jahren, die sich an ihre IT-Abteilung wenden ***20,2***

Anteil der Befragten von 50 bis 64 Jahren, die sich an ihre IT-Abteilung wenden ***47,3***

Anteil der Befragten von 30 bis 49 Jahren, die sich an ihre IT-Abteilung wenden ***38,6***

Anteil der Befragten von 30 bis 49 Jahren, die sich an Arbeitskollegen wenden ***9,5***

Anteil der Befragten unter 30 Jahren, die sich an Arbeitskollegen wenden ***16,0***

Anteil der Befragten von 50 bis 64 Jahren, die sich an Arbeitskollegen wenden ***7,1***

Quelle: Statista im Auftrag von G DATA

Was machen Sie im Netz?

Aktivitäten, für die das Internet genutzt wird, nach Alter; Arbeitnehmer in Deutschland; 2021; in Prozent *

	Deutschland	unter 30 Jahre	30 bis 49 Jahre	50 bis 64 Jahre	65 Jahre und älter
E-Mails	89,0	73,5	89,0	94,8	97,2
Online-Shopping	85,9	75,5	87,2	88,4	87,1
Online-Banking	78,6	63,5	81,7	80,8	78,3
Nutzung einer Suchmaschine	77,5	58,0	76,7	85,7	92,2
Informieren (Newsletter, Nachrichten, Wetter etc.)	72,7	54,3	72,6	79,8	83,7
Musik hören und Videos schauen	66,3	69,9	73,2	57,5	43,2
Social Media	66,2	72,7	72,0	57,4	47,2
Filme und Serien schauen	57,4	67,7	66,7	43,1	32,7
zum Arbeiten	54,2	48,1	57,3	52,6	59,5
zum Spielen	51,9	57,1	59,6	41,5	26,2
zum Teilen von Inhalten mit anderen	43,0	39,8	47,2	39,3	36,8
für keine dieser Aktivitäten	0,5	0,6	0,5	0,6	0,0

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

Wie fit sind Sie beim Thema IT-Sicherheit – ganz persönlich?

Einschätzung der persönlichen Kompetenz zum Thema IT-Sicherheit nach Alter, Geschlecht und Homeoffice-Möglichkeit; Arbeitnehmer in Deutschland; 2021; in Prozent

	unter 30 Jahre	30 bis 49 Jahre	50 bis 64 Jahre	65 Jahre und älter
5 = sehr große Kompetenz	21,7	12,5	5,4	5,2
4 = große Kompetenz	30,0	27,5	15,1	13,2
3 = mittlere Kompetenz	35,2	38,5	46,1	44,4
2 = geringe Kometenz	10,6	14,8	23,6	27,2
1 = sehr geringe Kompetenz	2,4	6,6	9,7	10,1
Mittelwert	**3,6**	**3,3**	**2,8**	**2,8**

Anteil der …

… weiblichen Befragten, die ihre Kompetenz als sehr groß oder groß einschätzen
24,7

… männlichen Befragten, die ihre Kompetenz als sehr groß oder groß einschätzen
42,5

… Befragten, die teilweise im Homeoffice arbeiten und ihre Kompetenz als sehr groß oder groß einschätzen
51,1

… Befragten, die nicht im Homeoffice arbeiten und ihre Kompetenz als sehr groß oder groß einschätzen
19,2

… Befragten, die komplett im Homeoffice arbeiten und ihre Kompetenz als gering oder sehr gering einschätzen
16,6

… weiblichen Befragten, die ihre Kompetenz als gering oder sehr gering einschätzen
33,4

… männlichen Befragten, die ihre Kompetenz als gering oder sehr gering einschätzen
17,3

… Befragten, die komplett im Homeoffice arbeiten und ihre Kompetenz als sehr groß oder groß einschätzen
41,1

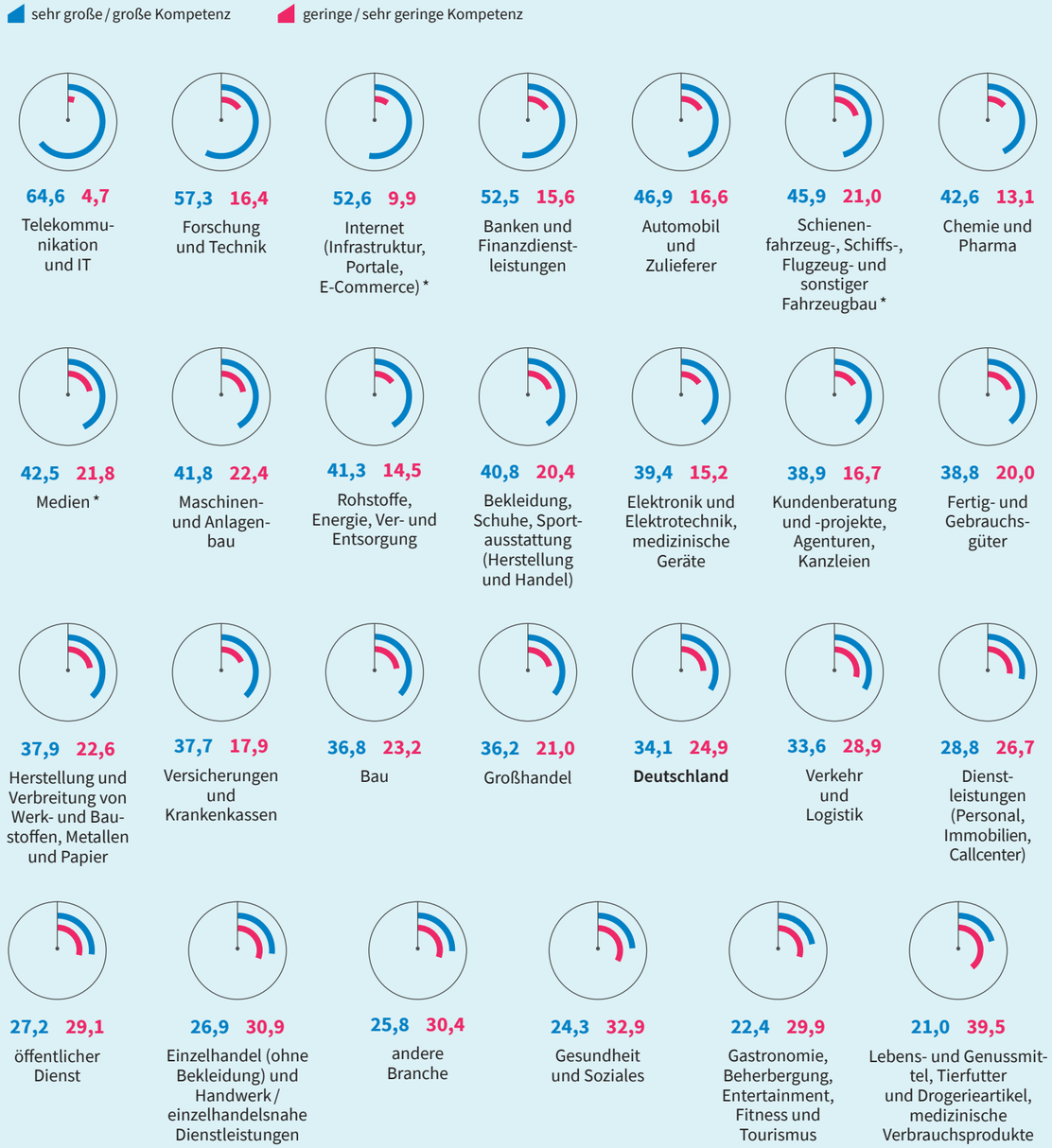
… Befragten, die teilweise im Homeoffice arbeiten und ihre Kompetenz als gering oder sehr gering einschätzen
11,8

… Befragten, die nicht im Homeoffice arbeiten und ihre Kompetenz als gering oder sehr gering einschätzen
37,5

Quelle: Statista im Auftrag von G DATA

Wie fit sind Sie beim Thema IT-Sicherheit – nach Branchen?

Einschätzung der persönlichen Kompetenz zum Thema IT-Sicherheit nach Branchen; Arbeitnehmer in Deutschland; 2021; in Prozent



* Branchen mit weniger als 50 Befragten; die Daten sollten daher mit Vorsicht interpretiert werden. Quelle: Statista im Auftrag von G DATA

Wir kennen uns aus

Einschätzung von Aussagen über Wissen und Relevanz zum Thema IT-Sicherheit nach Geschlecht und persönlicher Kompetenz; Arbeitnehmer in Deutschland; 2021; in Prozent *

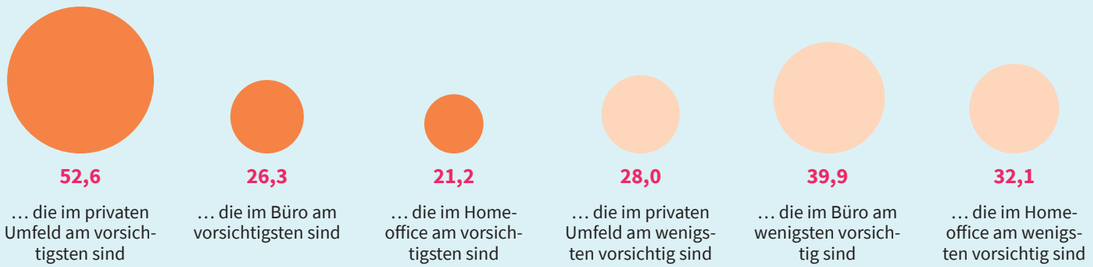
	Deutschland	männlich	weiblich
Ich informiere mich regelmäßig über aktuelle Themen und Trends im Bereich IT-Sicherheit.	24,4	30,9	17,0
Ich weiß, was die Berechtigungen bedeuten, die die Apps auf meinem Smartphone anfordern.	44,5	48,0	40,6
Ich weiß, was die Funktion einer Firewall ist.	55,6	60,7	49,8
Ich kenne die wichtigsten Schutzprogramme auf meinem Dienstrechner.	42,2	49,2	34,3
Ich sichere meine internetfähigen Geräte durch entsprechende Tools und Programme ab.	46,3	52,3	39,5
Ich bin häufig Ansprechpartner, wenn jemand in meinem privaten Umfeld etwas zum Thema IT-Sicherheit wissen möchte.	18,2	25,3	10,3
Keine dieser Aussagen trifft auf mich zu.	9,7	6,1	13,7
Anteil der Befragten, die wissen, was die Berechtigungen bedeuten, die die Apps auf ihrem Smartphone anfordern:			
… mit sehr großer Kompetenz	48,2		
… mit großer Komeptenz	55,9		
… mit mittlerer Kompetenz	47,7		
Anteil der Befragten, die wissen, was die Funktion einer Firewall ist:			
… mit sehr großer Kompetenz	48,3		
… mit großer Komeptenz	58,2		
… mit mittlerer Kompetenz	61,4		
Anteil der Befragten, die ihre internetfähigen Geräte durch entsprechende Tools und Programme absichern:			
… mit sehr großer Kompetenz	47,8		
… mit großer Komeptenz	55,1		
… mit mittlerer Kompetenz	51,0		
Anteil der Befragten, die häufig Ansprechpartner sind, wenn jemand in ihrem privaten Umfeld etwas zum Thema IT-Sicherheit wissen möchte:			
… mit sehr großer Kompetenz	43,9		
… mit großer Komeptenz	38,7		
… mit mittlerer Kompetenz	10,1		

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

Wir sind vorsichtig

Lebensbereiche nach ausgeübter Vorsicht im Bereich IT-Sicherheit; Arbeitnehmer in Deutschland; 2021; in Prozent

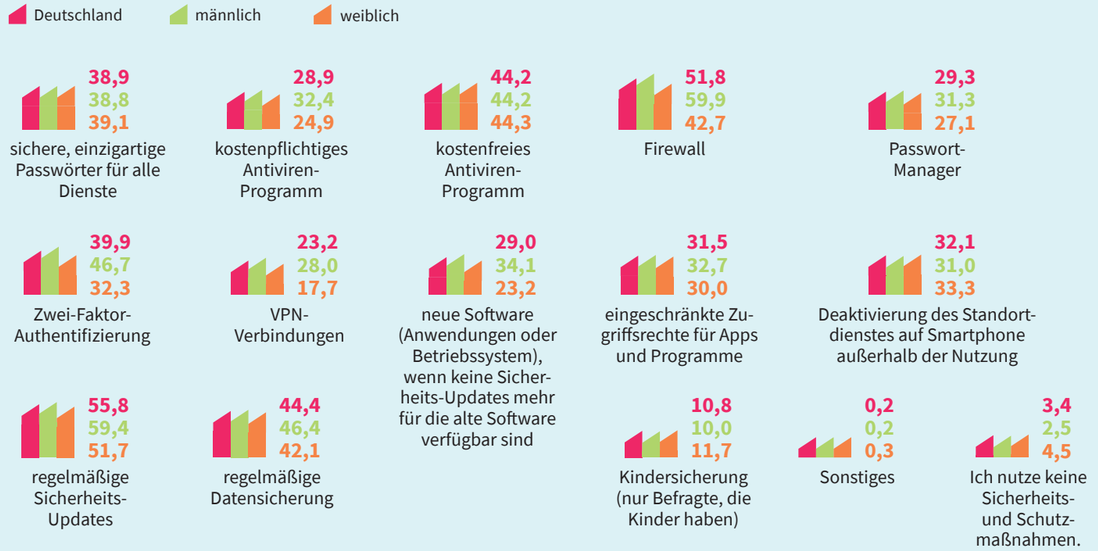
Anteil der Befragten, …



Quelle: Statista im Auftrag von G DATA

Wir sorgen vor – privat

IT-Sicherheits- und Schutzmaßnahmen im privaten Umfeld nach Geschlecht; Arbeitnehmer in Deutschland; 2021; in Prozent *



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

Wir sorgen vor – beruflich

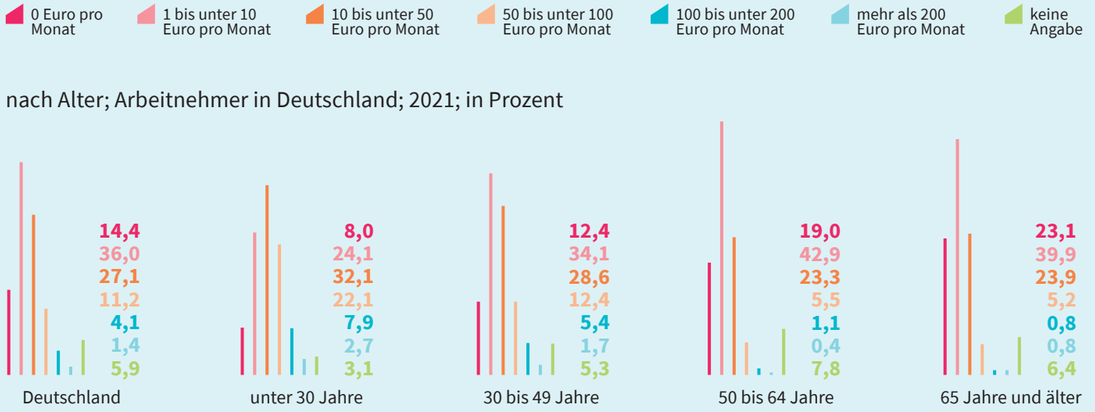
IT-Sicherheits- und Schutzmaßnahmen im beruflichen Umfeld nach Homeoffice-Möglichkeit; Arbeitnehmer in Deutschland; 2021; in Prozent *

	Deutschland	teilweise im Homeoffice	komplett im Homeoffice	kein Homeoffice
Firewall	45,8	52,1	58,8	36,1
regelmäßige Sicherheits-Updates	45,7	52,3	59,3	35,4
regelmäßige Datensicherung	42,9	48,9	55,4	33,6
kostenpflichtiges Antiviren-Programm	38,5	44,8	47,8	30,2
sichere, einzigartige Passwörter für alle Dienste	32,6	38,9	42,3	24,1
neue Software (Anwendungen oder Betriebssystem), wenn keine Sicherheits-Updates mehr für die alte Software verfügbar sind	29,5	37,3	40,2	19,6
eingeschränkte Zugriffsrechte für Apps und Programme	28,7	35,5	39,3	19,5
VPN-Verbindungen	27,8	36,7	45,2	14,3
Zwei-Faktor-Authentifizierung	27,7	35,8	41,5	16,3
Passwort-Manager	24,4	29,7	31,8	17,7
Deaktivierung des Standortdienstes auf Smartphone außerhalb der Nutzung	17,7	23,2	24,3	11,2
kostenfreies Antiviren-Programm	16,0	17,0	17,9	14,5
Ich nutze keine Sicherheits- und Schutzmaßnahmen.	14,6	3,4	3,8	26,8
Sonstiges	2,3	0,9	1,6	3,5

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

Wir sind bereit, in IT-Sicherheit zu investieren

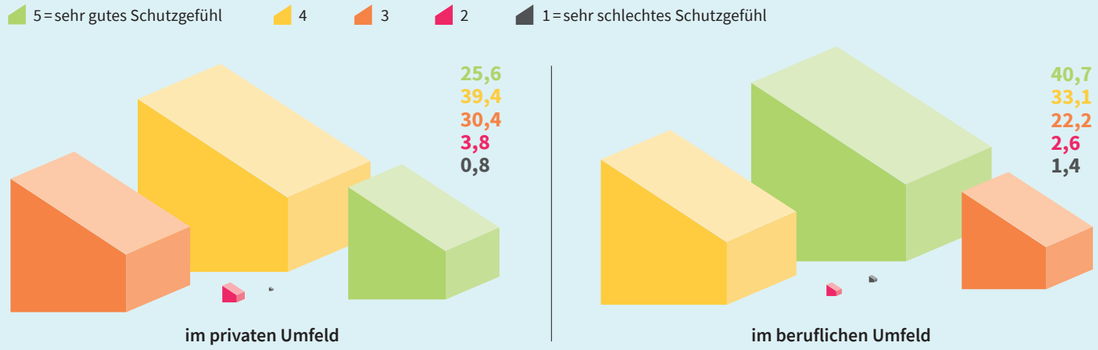
Investitionsbereitschaft in ein IT-Sicherheits- und Schutzpaket im privaten Umfeld



Quelle: Statista im Auftrag von G DATA

Wir fühlen uns gut geschützt – grundsätzlich

Schutzgefühl durch IT-Sicherheitsmaßnahmen im privaten und beruflichen Umfeld; Arbeitnehmer in Deutschland; 2021; in Prozent



Quelle: Statista im Auftrag von G DATA

Wir fühlen uns gut geschützt – privat und beruflich

Schutzgefühl durch IT-Sicherheitsmaßnahmen im privaten und beruflichen Umfeld nach persönlicher Kompetenz; Arbeitnehmer in Deutschland; 2021; in Prozent

	sehr große Kompetenz	große Kompetenz	mittlere Kompetenz	geringe Kompetenz	sehr geringe Kompetenz
im privaten Umfeld					
5 = sehr gutes Schutzgefühl	64,7	30,5	17,9	12,9	23,9
4	24,4	49,0	42,3	34,5	27,2
3	8,8	18,9	36,3	42,4	37,9
2	1,9	1,1	3,3	8,8	5,8
1 = sehr schlechtes Schutzgefühl	0,3	0,5	0,2	1,4	5,2
Top-2 (5 + 4)	89,1	79,5	60,3	47,4	51,1
Bottom-2 (2 +1)	2,1	1,6	3,5	10,2	11,0
Mittelwert	4,5	4,1	3,7	3,5	3,6
im beruflichen Umfeld					
5 = sehr gutes Schutzgefühl	57,9	44,9	38,1	32,7	35,5
4	26,9	37,5	35,2	31,2	21,9
3	12,7	16,1	23,5	29,1	32,0
2	1,9	1,2	2,1	4,6	5,4
1 = sehr schlechtes Schutzgefühl	0,7	0,4	1,1	2,4	5,2
Top-2 (5 + 4)	84,8	82,3	73,3	63,9	57,4
Bottom-2 (2 +1	2,5	1,6	3,2	7,1	10,6
Mittelwert	4,4	4,3	4,1	3,9	3,8

Quelle: Statista im Auftrag von G DATA

Wegen der Kinder

IT-Sicherheitsmaßnahmen wegen Kindern nach persönlicher Kompetenz; Arbeitnehmer in Deutschland, bei denen Kinder im Haushalt leben; 2021; in Prozent

ja nein

„Haben Sie zu Hause wegen Ihrer Kinder zusätzliche IT-Sicherheits- oder Schutzmaßnahmen eingeführt (oder werden dies zukünftig tun), die Sie ohne Ihren Nachwuchs nicht nutzen würden?“

Anteil der Arbeitnehmer, …
… die teilweise im Homeoffice arbeiten und IT-Sicherheitsmaßnahmen wegen Kindern eingeführt haben 61,3
… die komplett im Homeoffice arbeiten und IT-Sicherheitsmaßnahmen wegen Kindern eingeführt haben 49,9
… die nicht im Homeoffice arbeiten und IT-Sicherheitsmaßnahmen wegen Kindern eingeführt haben 32,7

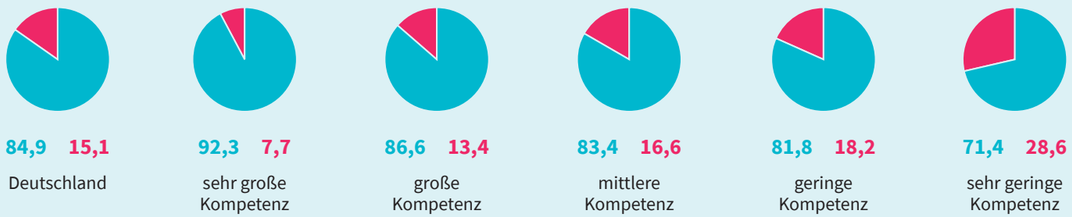
Quelle: Statista im Auftrag von G DATA

Für die Kinder

Aufklärung der Kinder über Internetnutzung nach persönlicher Kompetenz; Arbeitnehmer in Deutschland, bei denen Kinder im Haushalt leben; 2021; in Prozent

ja nein

„Haben Sie Ihre Kinder über mögliche Risiken der Internetnutzung aufgeklärt oder haben vor, das zu tun, wenn Ihre Kinder das Internet nutzen?“



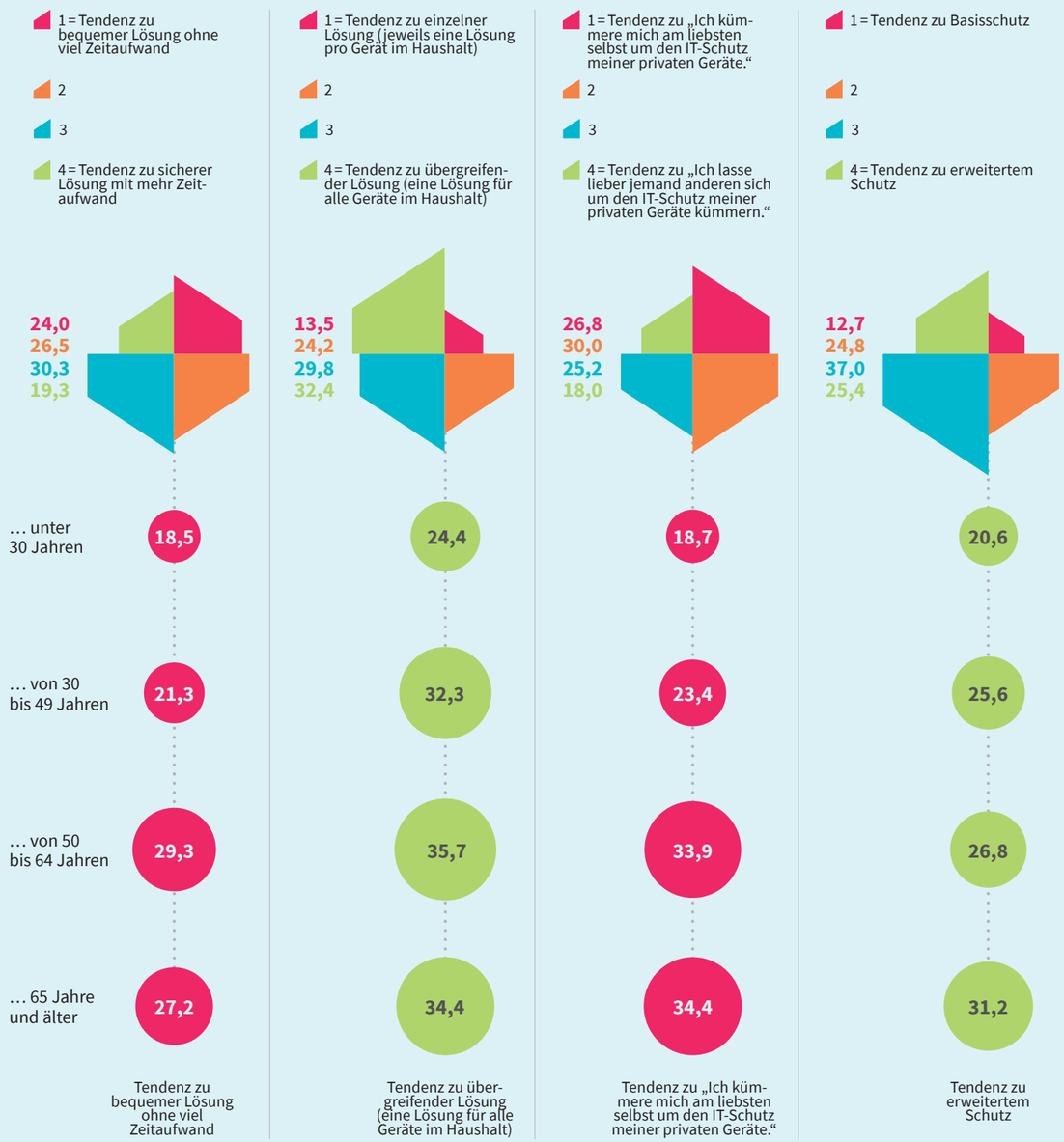
Anteil der Arbeitnehmer, …
… die teilweise im Homeoffice arbeiten und ihre Kinder über mögliche Risiken der Internetnutzung aufgeklärt haben 86,1
… die komplett im Homeoffice arbeiten und ihre Kinder über mögliche Risiken der Internetnutzung aufgeklärt haben 86,1
… die nicht im Homeoffice arbeiten und ihre Kinder über mögliche Risiken der Internetnutzung aufgeklärt haben 83,0

Quelle: Statista im Auftrag von G DATA

Für mehr Schutz und Sicherheit

Relevanz von IT-Sicherheits- und Schutzmaßnahmen; Arbeitnehmer in Deutschland; 2021; in Prozent

„Wozu tendieren Sie, wenn Sie an das Thema Sicherheitsmaßnahmen rund um IT denken?“



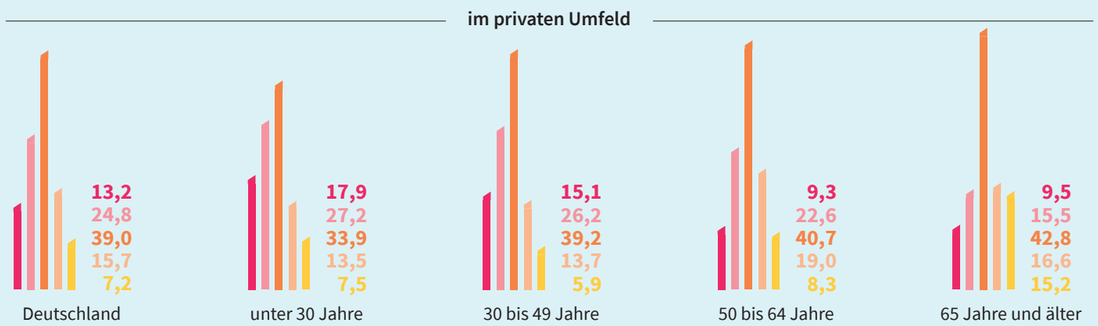
Quelle: Statista im Auftrag von G DATA

Das gefühlte Risiko – ist eine Frage des Alters

Risikoeinschätzung zum Thema Cyberkriminalität im privaten und beruflichen Umfeld nach Alter; Arbeitnehmer in Deutschland; 2021; in Prozent

5 = sehr hoch · 4 · 3 · 2 · 1 = sehr gering

„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)?“



Quelle: Statista im Auftrag von G DATA

Das tatsächliche Risiko – steigt mit Kindern im Haushalt

Empfänger einer Phishing-Mail nach Kindern im Haushalt; Arbeitnehmer in Deutschland; 2021; in Prozent *

„Waren Sie schon einmal Opfer einer Phishing-Mail (gefälschte E-Mail, mit der z. B. versucht wird, an sensible Daten wie Bankdaten, Unternehmensdaten etc. zu gelangen)?“

	Deutschland	Kinder im Haushalt	keine Kinder im Haushalt
ja, im privaten Umfeld	31,0	35,5	28,0
ja, im Büro	16,7	21,6	13,5
ja, im Homeoffice (nur Befragte, die im Homeoffice arbeiten)	7,5	11,1	5,0
nein, in keinem der genannten Lebensbereiche	48,8	41,9	53,4
Das weiß ich nicht. / Das kann ich nicht beurteilen.	8,4	7,1	9,2

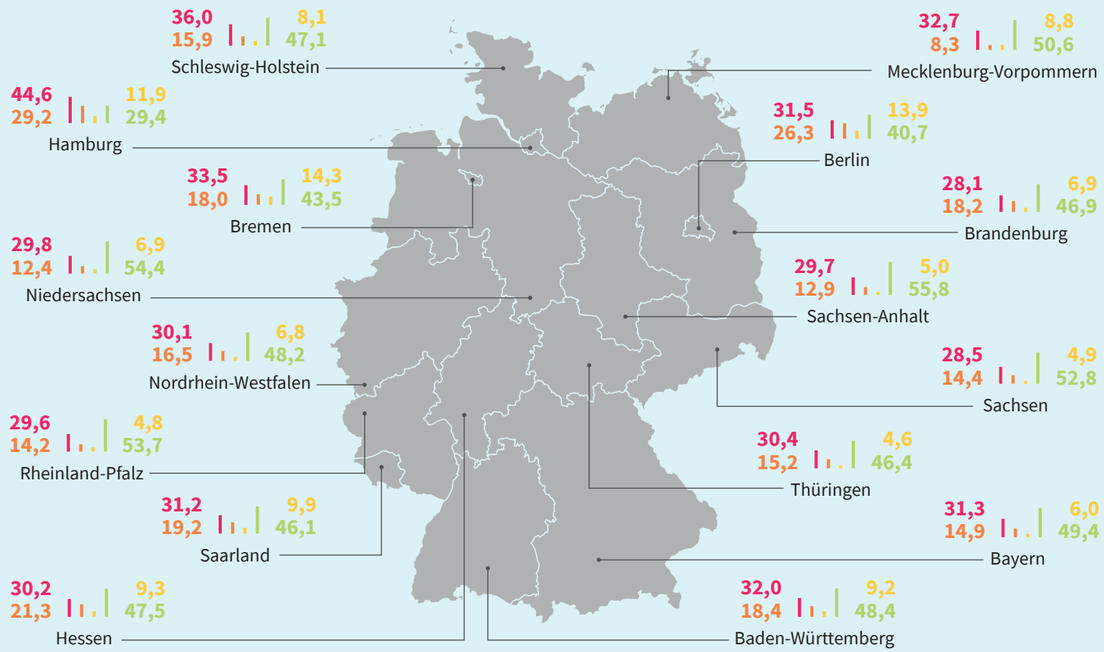
*Mehrfachauswahl möglich. Quelle: Statista im Auftrag von G DATA

Das tatsächliche Risiko – ist regional verschieden

Empfänger einer Phishing-Mail nach Bundesländern; Arbeitnehmer in Deutschland; 2021; in Prozent *

„Waren Sie schon einmal Opfer einer Phishing-Mail (gefälschte E-Mail, mit der z. B. versucht wird, an sensible Daten wie Bankdaten, Unternehmensdaten etc. zu gelangen)?“

ja, im privaten Umfeld · ja, im Büro · ja, im Homeoffice ** · nein, in keinem der genannten Lebensbereiche



* Mehrfachauswahl möglich. ** Nur Befragte, die im Homeoffice arbeiten. Quelle: Statista im Auftrag von G DATA

Das tatsächliche Risiko – ist im Homeoffice am größten

Durch Phishing-Mails entstandener Schaden; Arbeitnehmer in Deutschland, die im privaten Umfeld / im Büro / im Homeoffice schon einmal Empfänger einer Phishing-Mail waren; 2021; in Prozent *

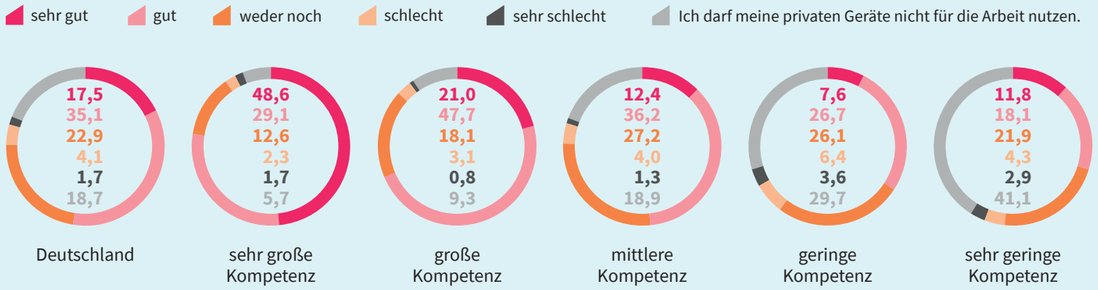
	im privaten Umfeld	im Büro	im Homeoffice
finanzieller Schaden	11,1	14,6	18,0
Verlust von Daten (z. B. persönliche Daten)	12,1	18,2	18,1
Diebstahl von Daten (z. B. Zugangsdaten, persönliche Daten)	14,0	14,5	20,1
Identitätsdiebstahl	12,1	12,5	19,6
Installation von Malware	13,1	15,5	17,8
Ich konnte meinen Rechner mehrere Stunden nicht nutzen.	12,2	17,2	18,4
sonstiger Schaden	0,6	0,3	0,5
Es ist kein Schaden entstanden.	49,4	35,5	31,1
Das weiß ich nicht. / Das kann ich nicht beurteilen.	5,8	7,6	5,6

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

Mehr Kompetenz, besseres Gefühl

Aufklärung zur Nutzung privater Geräte für die Arbeit nach persönlicher Kompetenz; Arbeitnehmer in Deutschland; 2021; in Prozent

„Wie gut fühlen Sie sich durch Ihren Arbeitgeber über die ordnungsgemäße Nutzung von privaten Geräten und mögliche Gefahren informiert?“



Quelle: Statista im Auftrag von G DATA

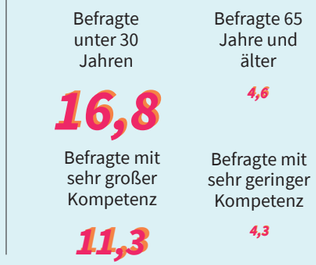
Mehr Kompetenz, weniger Scheu

Einschätzung von Aussagen über Risiken und Vertrauen im privaten Umfeld; Arbeitnehmer in Deutschland; 2021; in Prozent *

Ich vertraue darauf, dass die installierten bzw. angewendeten IT-Sicherheitsmaßnahmen ordnungsgemäß funktionieren und mich gut schützen.	41,5
Ich habe keine Angst davor, einen Fehler im Bereich IT-Sicherheit zuzugeben.	34,8
Im Fall einer sicherheitsrelevanten Situation weiß ich genau, was zu tun ist, um bestmögliche Schadensbegrenzung zu ermöglichen.	28,2
Ich vertraue lieber anderen als mir selbst, wenn es um das Thema IT-Sicherheit geht.	22,0
Ich habe schon mal einen Sicherheitshinweis ignoriert.	11,6
Ich müsste meinen Rechner besser schützen, tue es aber nicht, weil ich glaube, dass mein Rechner sowieso nicht relevant für andere ist.	8,3
Mir fehlt die Lust bzw. Zeit, sicherere Passwörter für meinen Rechner bzw. Programme zu wählen.	5,6
Ich würde eine Komponente der IT-Sicherheitsmaßnahmen ausschalten, wenn ich dadurch weniger Aufwand habe (z. B. durch weniger Sicherheitsabfragen).	2,2
keine dieser Aussagen	8,4

„Ich habe keine Angst davor, einen Fehler im Bereich IT-Sicherheit zuzugeben.“

„Ich habe schon mal einen Sicherheitshinweis ignoriert.“



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

Großes Vertrauen

Vertrauen in Arbeitgeber; Arbeitnehmer in Deutschland; 2021; in Prozent
Skala von 5 = sehr großes Vertrauen bis 1 = sehr geringes Vertrauen; Top-2 (= 5 + 4;) Bottom-2 (= 2 + 1)

Wie sehr vertrauen Sie Ihrem Arbeitgeber, …

… dass er auf den bestmöglichen IT-Schutz im Büro achtet?	
großes Vertrauen	73,0
geringes Vertrauen	5,1
… dass er auf den bestmöglichen IT-Schutz im Homeoffice achtet?	
großes Vertrauen	62,9
geringes Vertrauen	9,0
… dass er mit Ihren persönlichen Daten ordnungsgemäß umgeht?	
großes Vertrauen	68,9
geringes Vertrauen	6,2
… dass er immer gemäß der DSGVO handelt?	
großes Vertrauen	67,9
geringes Vertrauen	6,8
… dass er Sie darüber informiert, wenn Ihre persönlichen Daten an einen unbefugten Dritten gelangen würden?	
großes Vertrauen	66,8
geringes Vertrauen	8,3
… dass er sich Ihnen gegenüber korrekt verhält, wenn Sie einen IT-Sicherheitsschaden verursacht haben?	
großes Vertrauen	66,4
geringes Vertrauen	6,6
… dass er IT-Sicherheitsvorfälle umgehend behebt?	
großes Vertrauen	69,8
geringes Vertrauen	6,3
… dass er große IT-Sicherheitsvorfälle an alle Mitarbeiter kommuniziert?	
großes Vertrauen	67,0
geringes Vertrauen	6,8
… dass er mit entsprechenden Vorkehrungen und Programmen gut vor einem Cyberangriff geschützt ist?	
großes Vertrauen	70,2
geringes Vertrauen	5,3

Quelle: Statista im Auftrag von G DATA

Große Unterschiede

Vertrauen in Arbeitgeber nach Alter; Arbeitnehmer in Deutschland; 2021; in Prozent
Skala von 5 = sehr großes Vertrauen bis 1 = sehr geringes Vertrauen; Top-2 (= 5 + 4)

Befragte, die darauf vertrauen,

… dass Ihr Arbeitgeber auf den bestmöglichen IT-Schutz im Büro achtet	
unter 30 Jahre	66,1
50 bis 64 Jahre	76,2
… dass er auf den bestmöglichen IT-Schutz im Homeoffice achtet	
unter 30 Jahre	57,6
50 bis 64 Jahre	65,6
… dass er mit Ihren persönlichen Daten ordnungsgemäß umgeht	
unter 30 Jahre	60,0
50 bis 64 Jahre	73,8
… dass er immer gemäß der DSGVO handelt	
unter 30 Jahre	56,5
50 bis 64 Jahre	73,3
… dass er Sie darüber informiert, wenn Ihre persönlichen Daten an einen unbefugten Dritten gelangen würden	
unter 30 Jahre	58,9
50 bis 64 Jahre	71,4
… dass er sich Ihnen gegenüber korrekt verhält, wenn Sie einen IT-Sicherheitsschaden verursacht haben?	
unter 30 Jahre	56,7
50 bis 64 Jahre	71,2
… dass er IT-Sicherheitsvorfälle umgehend behebt?	
unter 30 Jahre	58,7
50 bis 64 Jahre	76,3
… dass er große IT-Sicherheitsvorfälle an alle Mitarbeiter kommuniziert?	
unter 30 Jahre	55,7
50 bis 64 Jahre	72,9
… dass er mit entsprechenden Vorkehrungen und Programmen gut vor einem Cyberangriff geschützt ist?	
unter 30 Jahre	59,2
50 bis 64 Jahre	76,3

Quelle: Statista im Auftrag von G DATA

Je größer das Unternehmen, desto größer das vermutete Risiko

Arbeitgeber als Ziel von Cyberattacken nach Geschlecht, persönlicher Kompetenz, Unternehmensgröße und Homeoffice-Möglichkeit; Arbeitnehmer in Deutschland; 2021; in Prozent

sehr hoch | hoch | weder noch | gering | sehr gering | Das kann ich nicht beurteilen.

„Wie hoch schätzen Sie das Risiko ein, dass Ihr Arbeitgeber das Ziel von Cyberattacken wird?“

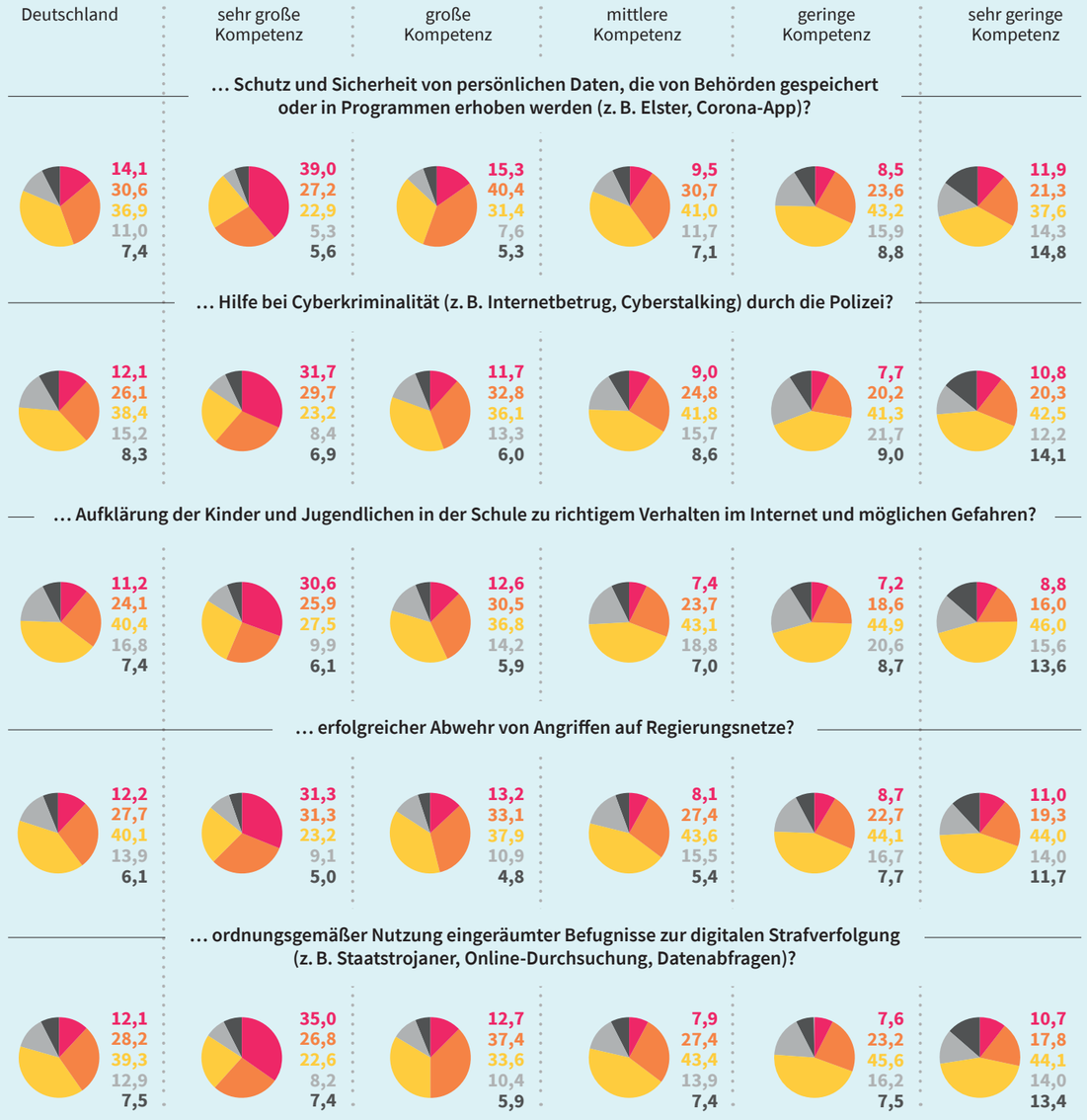
Quelle: Statista im Auftrag von G DATA

Je größer die Kompetenz, desto größer das Vertrauen

Vertrauen in deutsche Behörden und Institutionen nach persönlicher Kompetenz; Arbeitnehmer in Deutschland; 2021; in Prozent

5 = sehr großes Vertrauen | 4 | 3 | 2 | 1 = sehr geringes Vertrauen

„Wie sehr vertrauen Sie deutschen Behörden und Institutionen bezüglich …“



Quelle: Statista im Auftrag von G DATA

Welche Branchen und Industrien sind besonders gefährdet?

Besonders gefährdete Branchen und Industrien nach Alter und Unternehmensgröße; Arbeitnehmer in Deutschland; 2021; in Prozent *

„Welche der folgenden Branchen bzw. Industrien sind Ihrer Ansicht nach besonders gefährdet, wenn es um IT-Sicherheit geht?“

	Deutschland	unter 30 Jahre	30 bis 49 Jahre	50 bis 64 Jahre	65 Jahre und älter
Banken und Finanzdienstleistungen	48,1	35,7	47,3	53,7	54,9
Telekommunikation und IT	20,6	21,2	22,6	17,9	19,9
Forschung und Technik	28,8	19,6	25,8	35,5	41,9
Regierung	38,0	26,1	35,2	45,8	46,3
Wirtschaft und Handel (Herstellung, Verkauf und Handel)	25,4	16,6	26,0	27,9	35,2
Medien	10,1	20,3	10,5	5,7	5,4
Handwerk	3,6	6,4	4,0	2,0	2,4
Gesundheit und Soziales	11,2	14,5	11,8	9,0	13,4
Chemie und Pharma	15,3	11,8	16,0	16,1	10,3
Energie und Rohstoffe	11,0	8,7	10,7	12,0	12,8
Bildung	4,2	8,1	5,1	1,7	0,8
Internet (Infrastruktur, Portale, E-Commerce)	22,4	21,4	22,1	23,2	23,4
Verkehr und Logistik	7,1	10,5	6,5	6,8	2,1
Automobil und Zulieferer	6,8	8,8	7,2	5,8	4,0
sonstige Branche / Industrie	0,6	0,4	0,5	0,7	1,3
keine der genannten	4,8	4,7	4,4	5,5	2,5

	unter 50 Mitarbeiter	50 bis 999 Mitarbeiter	1 000 und mehr Mitarbeiter
Banken und Finanzdienstleistungen	48,5	44,9	52,9
Telekommunikation und IT	18,9	20,5	23,4
Forschung und Technik	28,0	27,6	31,8
Regierung	38,4	34,5	43,2
Wirtschaft und Handel (Herstellung, Verkauf und Handel)	24,2	25,3	27,4
Medien	9,7	11,6	8,2
Handwerk	4,2	4,4	1,4
Gesundheit und Soziales	12,0	11,8	9,1
Chemie und Pharma	16,3	14,2	15,5
Energie und Rohstoffe	10,3	11,2	11,5
Bildung	4,0	5,5	2,5
Internet (Infrastruktur, Portale, E-Commerce)	21,8	22,7	22,9
Verkehr und Logistik	6,6	7,2	7,6
Automobil und Zulieferer	5,4	7,8	7,3
sonstige Branche / Industrie	0,8	0,3	0,6
keine der genannten	5,4	4,4	4,6

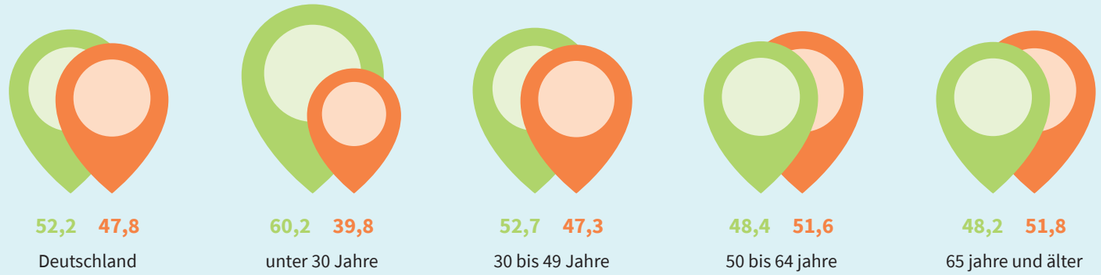
* Mehrfachauswahl möglich (max. 3 Nennungen). Quelle: Statista im Auftrag von G DATA

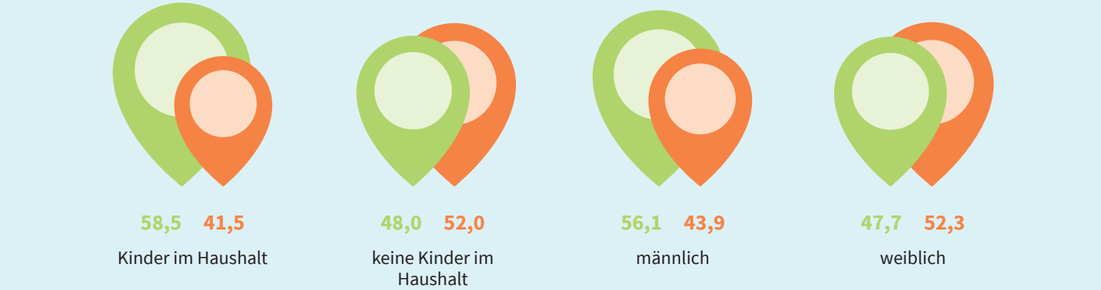
Spielt der Standort eines Anbieters für die Sicherheit eine Rolle?

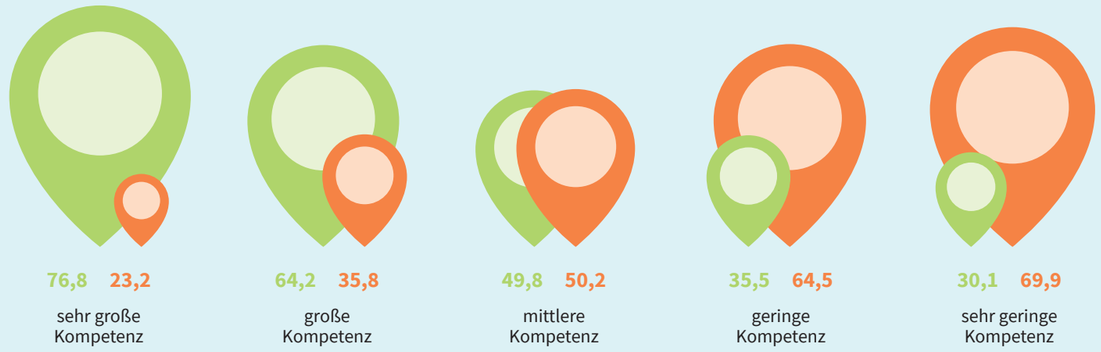
Relevanz des Standortes eines IT-Sicherheitsanbieters nach Alter, Geschlecht, Kindern im Haushalt und persönlicher Kompetenz; Arbeitnehmer in Deutschland; 2021; in Prozent

ja nein

„Ist es Ihnen wichtig, wo ein Anbieter von IT-Sicherheitslösungen seinen Standort hat?“







Quelle: Statista im Auftrag von G DATA

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.

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.

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.

Cyberraum: Der Cyberraum ist der virtuelle Raum aller weltweit auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme. Dem Cyberraum liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, das durch beliebige andere Datennetze erweitert werden kann.

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).
Für den Begriff Datenschutz existieren zwei englische Übersetzungen: „Data Protection“ meint den Datenschutz als Rechtsbegriff. „Privacy“ zielt dagegen auf die gesellschaftliche Lebensweise ab (Schutz der Privatsphäre) und wird überwiegend im amerikanischen Sprachumfeld und mittlerweile auch im EU-Raum vermehrt genutzt.

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.

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.

E-Mail Spoofing: vom Englischen „spoof“, hereinlegen, verulken: das illegale Verwenden von fremden Domain-Namen in Mail-Adressen.

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.

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

Hacker: 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.

Hoax: Der Begriff Hoax bezeichnet eine Falschmeldung (Gerücht oder Scherz), die über E-Mail, Messenger-Programme, SMS oder MMS verbreitet wird.

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 Informationssicherheitsbeauftragter (ISB) verwendet.

IT-System: IT-Systeme sind technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden. Typische IT-Systeme sind Server, Clients, Einzelplatz-Computer, Mobiltelefone, Router, Switches und Sicherheits-Gateways.

Junk-Mail: Als Junk-Mails (junk = Müll) oder Spam-Mails bezeichnet man Massen-Mails, die einem Empfänger ungewollt zugestellt werden und meist Werbeangebote enthalten.

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.

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.

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.

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.

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

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

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.

Spear-Phishing: Spear-Phishing ist eine Spezialform eines Phishing-Angriffs, bei dem nicht breitflächig, sondern nur ein kleiner Empfängerkreis (Führungskräfte oder Wissensträger auf Leitungsebene) attackiert wird. Voraussetzung für einen erfolgreichen Angriff ist eine gute Vorbereitung und die Einbettung des Angriffs in einen für das Opfer glaubwürdigen Kontext. Spear-Phishing richtet sich zumeist nicht gegen allgemein nutzbare Dienste wie Online-Banking, sondern gegen Dienste, die für Angreifer einen besonderen Wert haben.

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.

Standardsoftware: Software (Programme, Programm-Module, Tools etc.), die für die Bedürfnisse einer Mehrzahl von Kunden am Markt und nicht speziell vom Auftragnehmer für den Auftraggeber entwickelt wurde, einschließlich der zugehörigen Dokumentation. Sie zeichnet sich außerdem dadurch aus, dass sie vom Anwender selbst installiert werden soll und dass nur geringer Aufwand für die anwenderspezifische Anpassung notwendig ist.

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.

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

Accenture
ARD
Bertelsmann Stiftung
Bitkom e. V.
bleeping computer
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Bundeskriminalamt
Bundesnetzagentur
Bundesverband Digitale Wirtschaft e. V. (BVDW)
Capgemini
Center for International Governance Innovation (CIGI)
Chainalysis.com
CVE
DataReportal
Deloitte
Destatis
Deutscher Gewerkschaftsbund
Deutschland sicher im Netz (DsiN)
DSGVO-Portal
Embroker
Europäische Kommission
Eurostat
EY
FBI
Gartner
G DATA
Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GdV)
Global Web Index
Hasso-Plattner-Institut für Digital Engineering gGmbH (HPI)
Hiscox
Hootsuite
IBM Security
IDG Research Services
ifo institut
Initiative D21 e. V.
International Telecommuniction Union
Internet Crime Complaint Center
Ipsos
Kantar
Kriminologisches Forschungsinstitut Niedersachsen
Marsh
Microsoft
Mimecast
Munich Re
nCipher Security
Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK)
Ponemon Institute
Postbank
Ranstadt
Shodan.io
Sonic Wall
Spiceworks
Statcounter
Statista
Statistisches Bundesamt
Thales Group
UNCTAD
UpGuard
Unternehmen Cybersicherheit – gemeinsame Initiative von VDMA und VSMA
US Departmen of Justice
Varonis
Verizon
We Are Social
Wifor Institute
ZDF
zdnet

IMPRESSUM

Herausgeber: G DATA CyberDefense AG • G DATA Campus • Königsallee 178, 44799 Bochum, vertreten durch die Vorstände Kai Figge, Frank Heisler, Andreas Lüning
Projektleitung G DATA: Hauke Gierow
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 Froitzheim, Sarah Sommer
Marktforschung, Recherche, Daten und Quellen:
Christian Cramer, Cindy Karwowski, Ana-Cristina Martus, Robin Rehfeldt, Nina Reuschling, Tobias Steddin