G DATA CyberDefense

Warum sind Cyberangriffe auf Unternehmen oft erfolgreich?

Zahlen & Fakten aus Umfragen

Whitepaper

Warum sind Cyberangriffe auf Unternehmen oft erfolgreich?

Zahlen & Fakten aus Umfragen in Unternehmen

Whitepaper

Inhalt

Liebe Leserinnen und Leser,

Cyberangriffe nehmen nicht nur in ihrer Häufigkeit zu, sondern werden auch immer komplexer und zielgerichteter – auch durch den Einsatz von Künstlicher Intelligenz. Unternehmen jeder Branche und jeder Größenordnung stehen vor der Herausforderung, sich gegen diese Bedrohungen effektiv zu schützen – eine Aufgabe, die nicht nur technologisches Know-how, sondern auch ein tiefes Verständnis für die Risiken und Konsequenzen erfordert.

Im vorliegenden Whitepaper beleuchten wir den aktuellen Status Quo der IT-Sicherheit in Unternehmen. Die Ergebnisse zeigen eindrucksvoll, wie wichtig es ist, sich mit Cybersicherheit ganzheitlich auseinanderzusetzen – von der technischen Ausstattung über die Sensibilisierung der Mitarbeitenden bis hin zu einer umfassenden strategischen Planung. Besonders alarmierend ist die Diskrepanz zwischen der tatsächlichen Bedrohungslage und der Wahrnehmung vieler Mitarbeiterinnen und Mitarbeiter, die ihre Unternehmen häufig nicht als Angriffsziel sehen.

Als Gründer und Vorstand der G DATA CyberDefense AG liegt mir das Thema IT-Sicherheit seit Jahrzehnten am Herzen. Wir verstehen uns nicht nur als Lösungsanbieter, sondern auch als Partner, der Unternehmen dabei unterstützt, ihre IT-Sicherheitsarchitektur zukunftssicher aufzustellen. Unser Ziel ist es, nicht nur akute Bedrohungen abzuwehren, sondern Organisationen nachhaltig resilient gegen Cyberangriffe zu machen. Generell stellt sich mir die Frage: Können die Unternehmen das Thema IT-Sicherheit allein bewältigen? Können sie einen laufenden Angriff identifizieren und diesen durch die richtige Reaktion stoppen, um weitere Schäden zu verhindern? Ich glaube, dass viele Firmen sich dabei schwertun und Hilfe brauchen. Wir bei G DATA sind davon überzeugt, dass Managed Extended Detection and Response die richtige Lösung für Unternehmen ist.

Ich lade Sie ein, die Erkenntnisse dieses Whitepapers zu nutzen, um die IT-Sicherheitsstrategie in Ihrem Unternehmen zu überprüfen und weiterzuentwickeln. Denn eines ist sicher: Cybersicherheit ist nicht nur eine technische, sondern vor allem auch eine strategische Herausforderung.

Herzliche Grüße,

Andreas Lüning

Vorstand und Mitgründer | G DATA CyberDefense AG

Status Quo der IT-Sicherheit in Unternehmen

Alle Unternehmen sind generell ein interessantes Angriffsziel für Cyberkriminelle. In allen Firmen lassen sich Daten, zum Beispiel Kundeninformationen, ausspähen, die nicht in die Hände Dritter gehören. Zusätzlich erfolgt oft die Verschlüsselung der IT-Systeme mit Ransomware und die Angreifer verlangen Lösegeld.

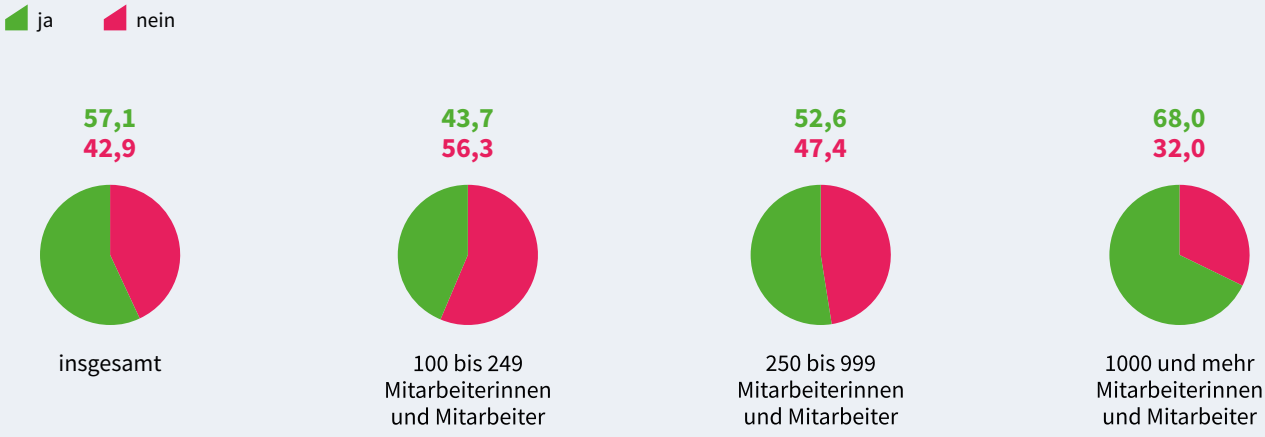
Unsere Umfrage, die wir in Zusammenarbeit mit Statista und brand eins durchgeführt haben, zeigt, dass viele Arbeitnehmer ihr Unternehmen nicht als interessantes Angriffsziel sehen – obwohl die Gefahr durch Cyberkriminalität sehr hoch ist. Nur 57 Prozent der Angestellten gehen davon aus, dass ihre Firma angegriffen werden könnte. Bei Unternehmen mit einer Belegschaftsgröße von 100 bis 249 Mitarbeitenden liegt der Wert sogar bei annähernd 44 Prozent.

Auffällig ist: Je weniger Angestellte die Firma beschäftigt, desto weniger interessant für Cyberkriminelle erscheint sie den Befragten.

Zu unbekümmert

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

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



Quelle: Statista im Auftrag von G DATA

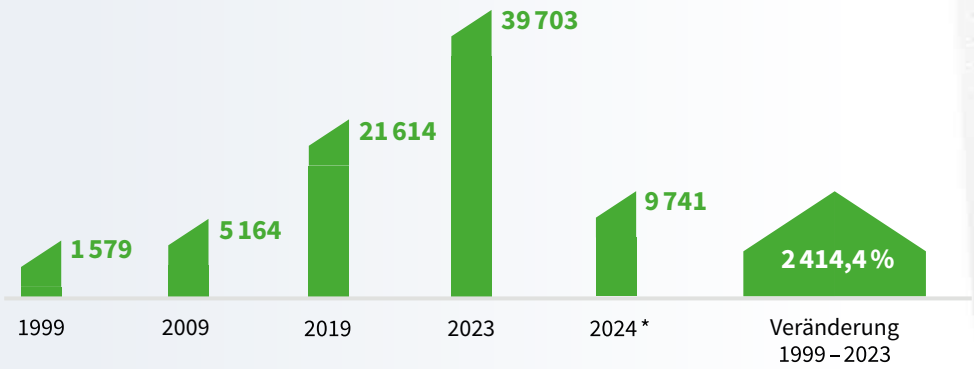
Ein Blick auf die Anzahl der vom CVE-Programm (CVE = Common Vulnerabilities and Exposures) dokumentierten weltweiten Schwachstellen verdeutlicht die Gefahr, in der Unternehmen schweben.

In Firmen kommt eine Vielzahl von Betriebssystemen und Programmen zum Einsatz und diese müssen immer auf dem neuesten Stand sein, indem die aktuell verfügbaren Updates eingespielt sind. Sicherheitslücken in Anwendungen sind ein oft genutzter Angriffsvektor für Cyberkriminelle, um in ein Netzwerk einzudringen.

Im Jahr 2023 wurden fast 40.000 Schwachstellen gezählt. Innerhalb von 24 Jahren (1999 bis 2023) stieg die Zahl der dokumentierten Lücken um mehr als 2.400 Prozent an.

Geteilt

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



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

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

Ein großes Problem für Unternehmen ist Ransomware. Sind die IT-Systeme erst einmal verschlüsselt, bleibt vielen IT-Verantwortlichen im schlimmsten Fall nur die Möglichkeit, das geforderte Lösegeld zu bezahlen, um die Daten beziehungsweise das Netzwerk wieder freizukaufen – insbesondere dann, wenn kein funktionstüchtiges Backup zur Verfügung steht. Im zweiten Quartal 2023 lag die durchschnittliche Höhe der Lösegeld-Zahlungen bei mehr als 684.000 Euro. IT-Verantwortliche haben bei der Bewältigung der Attacke allerdings mit höheren Kosten zu kämpfen, da die Systeme wieder bereinigt werden müssen und eventuell weitere Investitionen in die IT-Systeme nötig sind, um zukünftig für mehr Schutz zu sorgen.

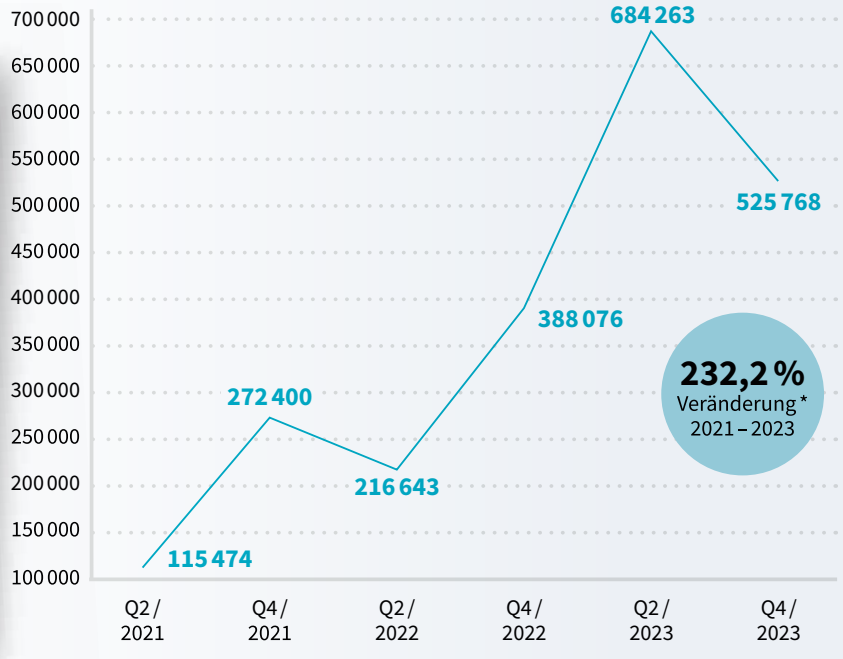
Zudem ist es auch möglich, dass nur ein Teil der verschlüsselten Komponenten und Daten freigegeben wird und eine weitere Lösegeldzahlung von der Angreifergruppe verlangt wird. Daher ist es ratsam, die IT-Sicherheit so aufzustellen, dass es nach Möglichkeit erst gar nicht zu einer erfolgreichen Attacke kommt oder diese direkt in den Anfängen beendet werden kann.

Abkassiert

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

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

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



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

Oft stellen die Mitarbeitenden die Security-Architektur ihres Unternehmens auf die Probe. Sie gehen aus Neugier Risiken ein:

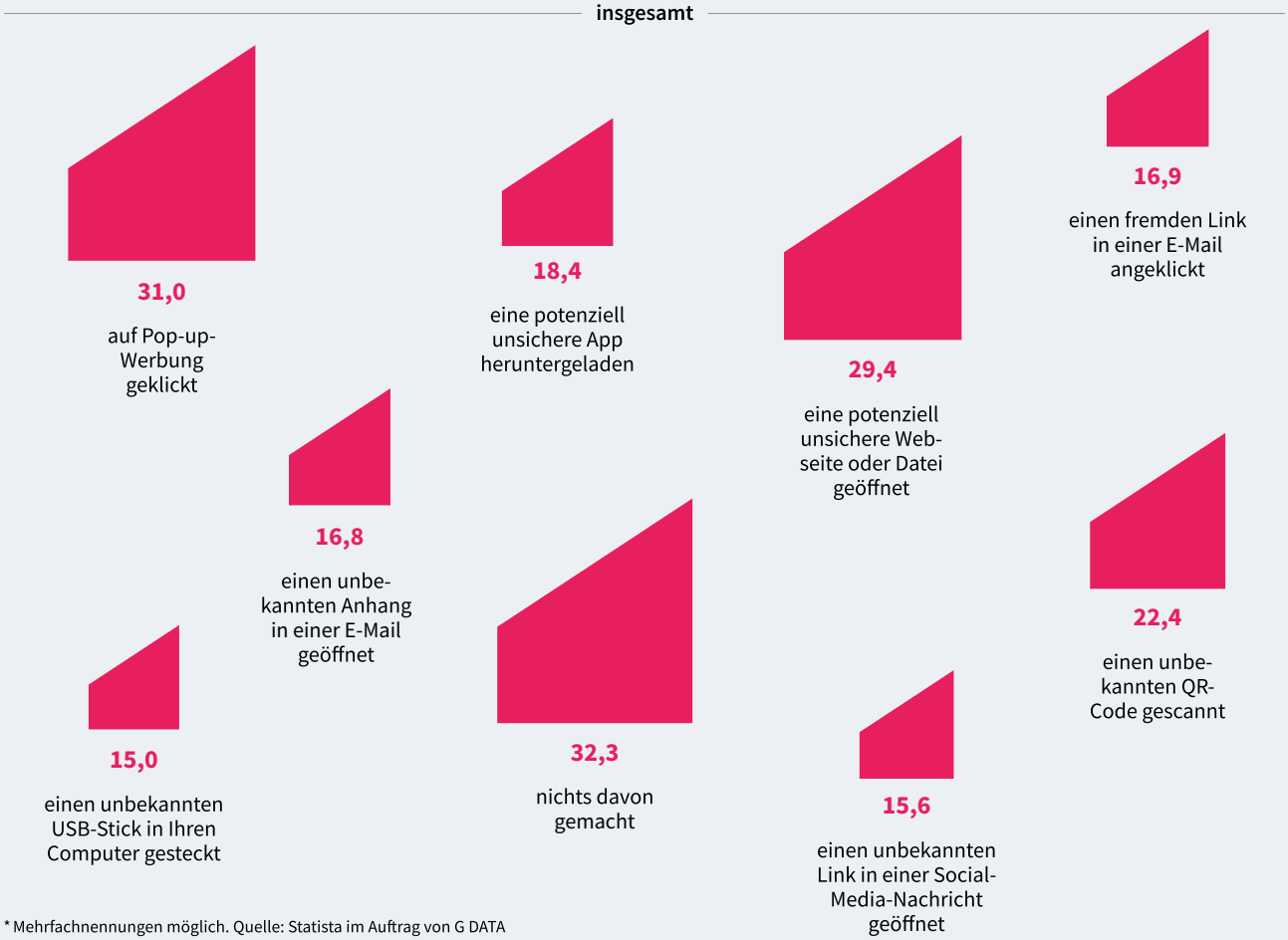
Fast 30 Prozent der Arbeitnehmenden in Deutschland haben schon einmal eine potenziell unsichere Webseite aufgerufen oder eine entsprechende Datei geöffnet.

Etwa ein Sechstel der Befragten hat bereits einen unbekannten USB-Stick in den eigenen Computer gesteckt. Dabei sollte der „alte Trick“ des angeblich verlorenen Datenträgers auf einem Parkplatz oder vergleichbare Szenarien, mit denen Kriminelle mit Schadcode präparierte USB-Sticks in Unternehmen bringen, bekannt sein.

Neugierig – und überheblich

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

„Haben Sie schon mal aus Neugier folgende Dinge gemacht?“



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

Unzureichende Maßnahmen gegen Cyberangriffe

Virenschutzlösungen sind bei deutschen Unternehmen immer noch die Schutzkomponente Nummer eins gegen Attacken. Drei von fünf Bereichs-, Abteilungs- oder Teamleitenden in der IT oder Security geben dies an. Dabei ist klassische Antiviren-Software in der Schutzwirkung begrenzt, weil diese insbesondere auf das Erkennen von Schadprogrammen spezialisiert ist. Allerdings finden viele Angriffe heute dateilos statt, beziehungsweise sie sind individualisiert. Oft nutzen die Angreifergruppen ungeschlossene Schwachstellen in Betriebssystemen oder Anwendungen aus und gelangen darüber in die IT-Infrastruktur von Unternehmen.

Die Lösung besteht in der Nutzung von Managed Security Services, zum Beispiel Managed Extended Detection and Response (MXDR), weil eine Erkennung neuartiger Angriffsmuster dank einer breit aufgestellten Sensorik erfolgt. Schädliche Aktivitäten im Netzwerk lassen sich so aufspüren und durch Gegenmaßnahmen beenden. Allerdings machen Managed Security Services gerade einmal einen Anteil von 35 Prozent aus. Dies wird sich in den kommenden Jahren verändern, weil immer mehr IT-Verantwortliche in Unternehmen erkennen, dass eine Investition in diese Art von Dienstleistungen notwendig ist.

Maßnahmen

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

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

59,1 Anti-Viren-Software

49,4 Multi-Faktor-Authentifizierung

49,0 Notfallplan und -übungen

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

42,9 regelmäßige Penetrationstests

42,5 Durchführung von Security-Awareness-Trainings

35,2 Managed Security Services

30,8 Rahmenvereinbarung mit Incident-Response-Team

0,8 keine der genannten

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

Oft bewirkt auch erst eine erfolgreiche Attacke ein Umdenken bei den Verantwortlichen. So gaben im Jahr 2023 mehr als die Hälfte (55 Prozent) der Unternehmen an, im Zuge der Bewältigung eines Angriffs zusätzliche Maßnahmen ergriffen zu haben.

In der IT-Sicherheit ist dann oft von „Lernen durch Schmerz“ die Rede. Weitere 15 Prozent der Befragten planten zum Zeitpunkt der Befragung, zusätzliche Mittel zur Steigerung des IT-Sicherheitsniveaus zu ergreifen.

Ergänzt

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

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

Quelle: TÜV-Verband

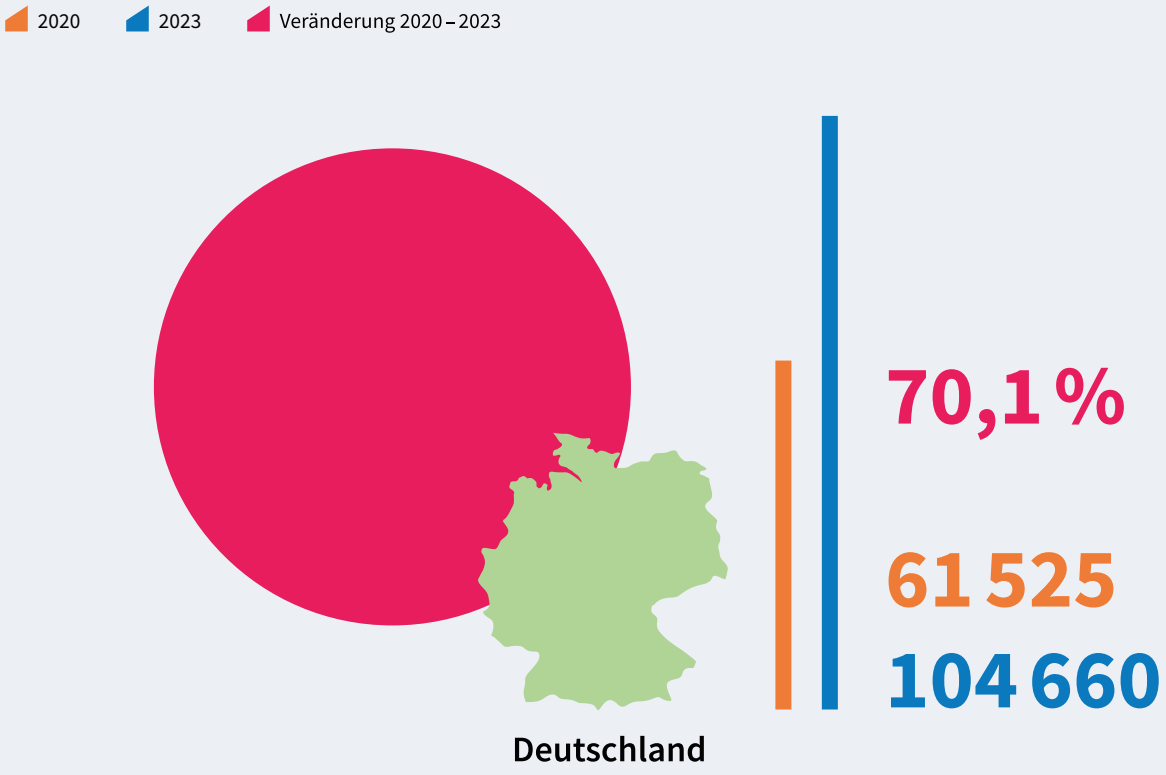
Herausforderung Personalmangel

Fachkräfte fehlen in vielen Branchen und die Entwicklung hat auch vor der IT-Sicherheit nicht Halt gemacht. 2023 fehlten in Deutschland fast 105.000 Expertinnen und Experten für Cybersicherheit.

Innerhalb von nur drei Jahren (von 2020 bis 2023) stieg der Personalmangel um siebzig Prozent an und verschärfte das Problem weiter.

Gefährliche Lücken

Fehlende Fachkräfte im Bereich Cybersicherheit; Deutschland



Quelle: (ISC)²

Nicht verwunderlich ist daher, dass 44 Prozent der Arbeitnehmerinnen und Arbeitnehmer in Deutschland den Fachkräftemangel als hoch oder sehr hoch bewerten.

Nur weniger als ein Sechstel der Befragten schätzen das Problem von fehlendem Personal niedrig oder sehr niedrig ein.

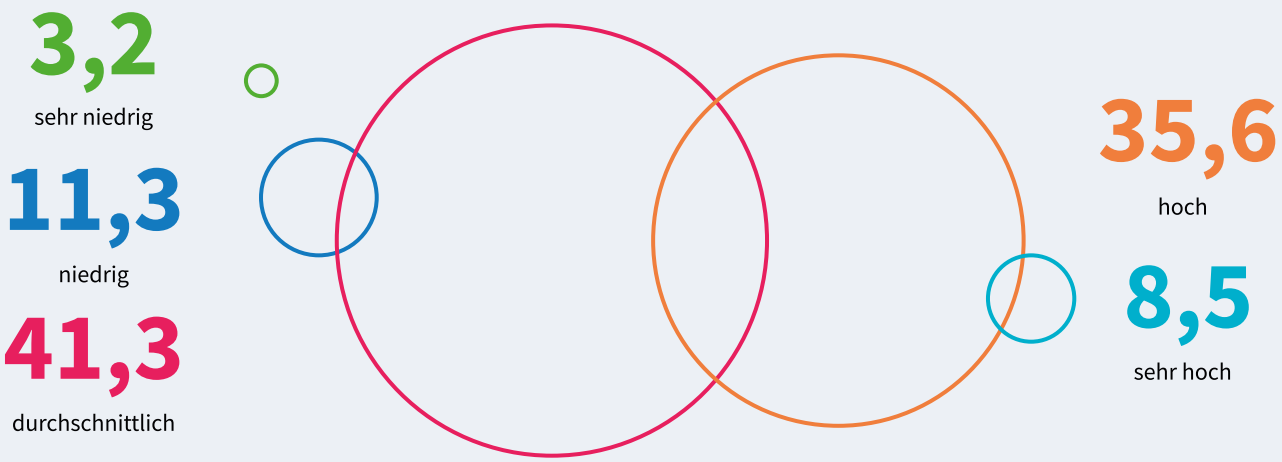
Ein sehr großer Anteil von 41 Prozent empfindet das Problem als durchschnittlich, was sicherlich daran liegt, dass (wie bereits erwähnt) in vielen Wirtschaftszweigen und Berufsgruppen dieses Problem vorzufinden ist.

Damit erscheint es vielen Angestellten fast als eine Art „Normalzustand“.

Mehr Fachkräfte

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

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



Quelle: Statista im Auftrag von G DATA

Der Mangel an Fachkräften hat ernste Konsequenzen für die betroffenen Unternehmen und wirkt sich unmittelbar auf die IT-Sicherheit aus: So haben 43 Prozent der Mitarbeitenden erlebt, dass Informationen aus Security Software und anderen Systemen, die der Cyberabwehr dienen, nur unzureichend ausgewertet werden. Viele Daten werden erst gar nicht eingesehen, so dass mögliche Hinweise auf aktuell laufende Cyberangriffe ungesehen bleiben und die Angreifergruppe ungehindert weiter im Netzwerk agieren kann. Weitere Folgen des Fachkräftemangels sind falsch konfigurierte Systeme, zu langsames Patchen von kritischen Systemen und Versäumnisse in Prozessen und Verfahren.

Die Ergebnisse zeigen, wie gravierend das Problem in Unternehmen ist, dass nicht genug Zeit für wichtige Aufgaben bleibt. IT-Administratoren sind durch das Tagesgeschäft bereits voll ausgelastet und sind daher nicht in der Lage, sich um IT-Sicherheit zu kümmern. Sie haben keine Zeit dafür, erste Anzeichen für Angriffe zu entdecken. Zudem ist es nicht möglich, die Ursachen für erfolgte Cyberangriffe zu ermitteln, um weitere Maßnahmen daraus ableiten zu können.

IT-Administratoren und ihre Teams brauchen daher die Unterstützung durch spezialisierte Security-Dienstleister.

Mehr Informationen, mehr Zeit und mehr Ressourcen

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

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

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

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

Ein weiteres Problem für Unternehmen in diesem Zusammenhang besteht darin, dass IT-Verantwortliche das Cyberrisiko nicht ausreichend bewerten können. Dabei ist dies die Basis dafür, passende Maßnahmen zu planen und dadurch eine effektive Cyberabwehr aufzustellen. Hürden für eine umfassende Analyse sind hauptsächlich der Zeitaufwand und unzureichendes Personal, wobei beide Faktoren unmittelbar zusammenhängen: Fehlen Mitarbeitende, können einige Aufgaben nur unzureichend oder überhaupt nicht erledigt werden.

Zu leichtfertig

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

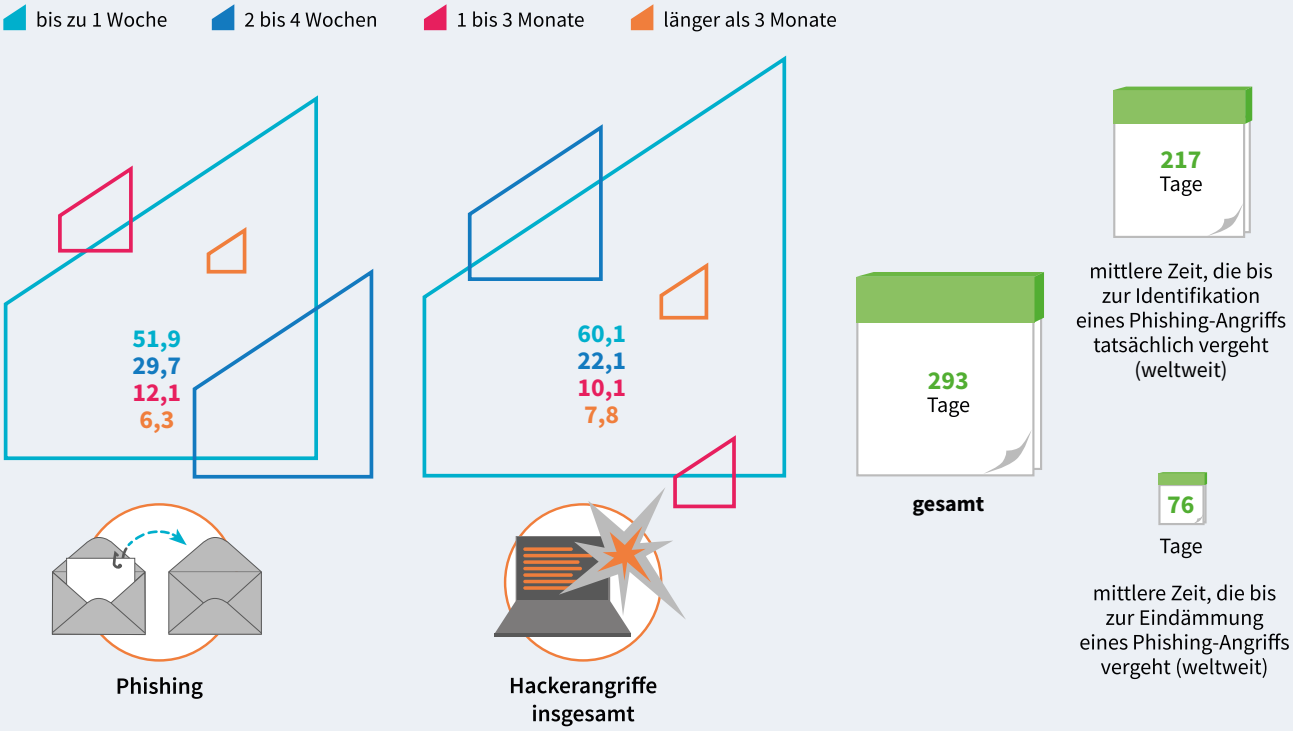
* Mehrfachnennungen möglich. Quelle: ISACA

Wie beschrieben, ist eine Folge des Personalmangels und der fehlenden Zeit für Aufgaben rund um IT-Sicherheit, dass Informationen aus den Analysesystemen oft ungelesen bleiben. Trotzdem sind die Angestellten in Unternehmen oft noch optimistisch in der Annahme, wie viel Zeit für das Entdecken einer Cyberattacke vergeht: Drei von fünf Mitarbeitende gehen davon aus, dass ein Angriff in maximal einer Woche identifiziert wird. Jeder Zehnte glaubt, dass dies in ein bis zwei Monate erfolgt und nur knapp acht Prozent der Befragten denken, dass mehr als drei Monate vergehen, bis eine Attacke aufgedeckt wird. Dies kommt der Realität zwar noch am nächsten, aber trotzdem sind die wirklichen Zahlen weitaus höher.

Das dauert

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

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



Quellen: Statista im Auftrag von G DATA, IBM

Bis eine Phishing-Attacke identifiziert ist, dauert es im Durchschnitt 217 Tage. Die Eindämmung nimmt weitere 76 Tage in Anspruch. Gestohlene oder kompromittierte Berechtigungsnachweise werden sogar erst nach 240 Tagen bemerkt und 88 Tage aufgewendet, um den Vorfall unter Kontrolle zu bringen.

Diese Zahlen zeigen, wie fatal sich eine schwache IT-Sicherheit auf das Schutzniveau eines Unternehmens auswirkt. Häufig werden Angriffe erst dann bemerkt, wenn unmittelbare Auswirkungen auftreten, zum Beispiel die Verschlüsselung der Systeme und Dateien bei einer Ransomware.

Bis dieser Punkt erreicht ist, war die Angreifergruppe allerdings schon über einen längeren Zeitraum unbemerkt in der IT-Infrastruktur des Unternehmens aktiv und ihre Aktivitäten hätten längst bemerkt und gestoppt werden können.

Ahnungslos

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

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

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

60,1 %
… bis zu 7 Tagen
unbemerkt bleibt.

22,1 %
… 14 bis 28 Tage
unbemerkt bleibt.

10,1 %
… 30 bis 90 Tage
unbemerkt bleibt.

7,8 %
… länger als 90 Tage
unbemerkt bleibt.

Quellen: IBM, Statista

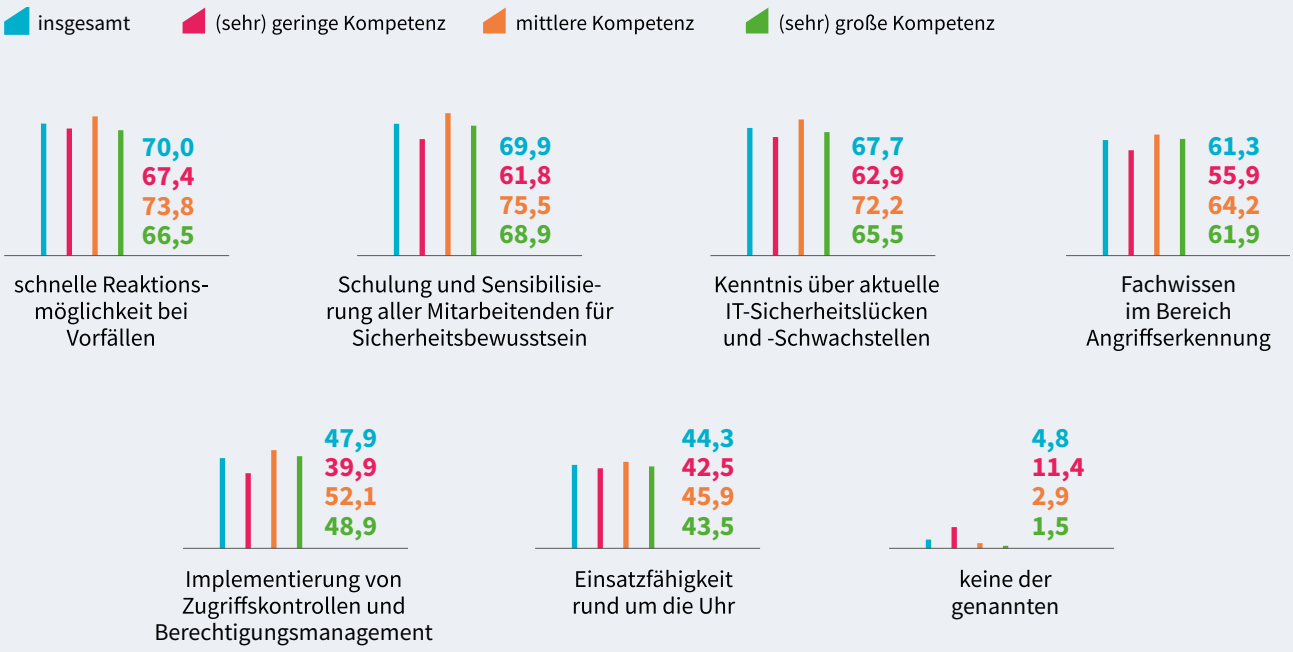
Was muss IT-Sicherheit leisten?

Unternehmen haben Anforderungen an eine effektive IT-Sicherheit. Dabei ist die schnelle Reaktionszeit bei Security-Vorfällen für sieben von zehn Mitarbeitende ein wichtiger Anspruch. Auch Kenntnisse über aktuelle IT-Sicherheitslücken und Schwachstellen sowie Fachwissen im Bereich Angriffserkennung spielen mit einem Anteil von fast 68 Prozent und 61 Prozent eine große Rolle beim geforderten Leistungsprofil.

Gut eingeschätzt?

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

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



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

Was brauchen Unternehmen?

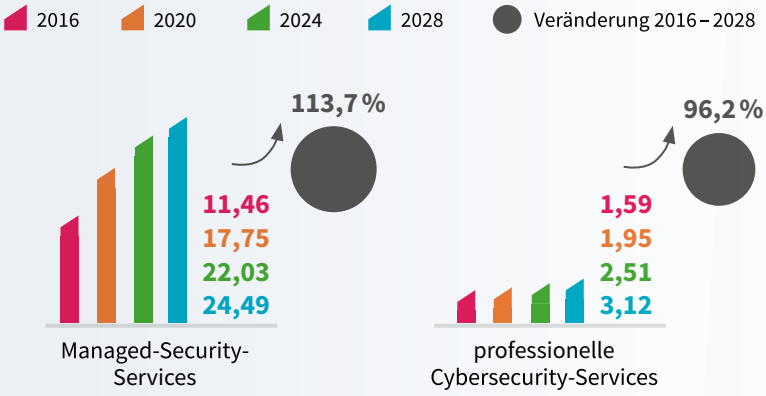
Deutlich wird, dass Firmen ihre eigene IT-Sicherheit heutzutage oft nicht mehr allein bewerkstelligen können. IT-Verantwortlichen fehlen Personal, Ressourcen und die fachliche Expertise – ohne diese Faktoren ist es nicht möglich, Unternehmen effektiv vor Cybergefahren zu schützen. Daher sind Firmen auf kompetente und auf Security spezialisierte Dienstleister angewiesen.

In den letzten Jahren ist der Markt für Managed Security Services (MSS) und für professionelle Cybersecurity-Services rasant gewachsen. Betrug im Jahr 2016 der Umsatz mit MSS weltweit noch annähernd 11,5 Milliarden Euro, wird dieser für 2028 auf fast 24,5 Milliarden Euro – also mehr als das Doppelte - prognostiziert. Das wäre eine Veränderung von fast 114 Prozent.

Bei professionellen Cybersecurity-Services, wie beispielsweise Penetration Tests, gehen Marktbeobachterinnen und -beobachter ebenfalls von einer enormen Umsatzsteigerung aus.

Prognostiziert

Umsatz mit Security-Services; weltweit; in Milliarden Euro



Quelle: Statista Market Insights

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

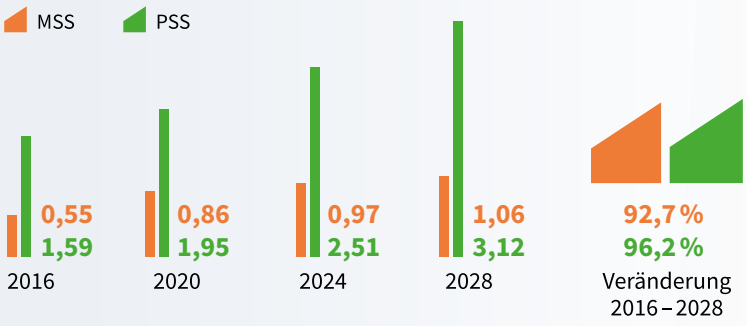
Professional Security Services (PSS) hingegen sind spezialisierte, zeitlich begrenzte Dienstleistungen, die auf spezifische Sicherheitsprojekte oder -initiativen fokussiert sind und oft tiefgehende Beratung und Expertise bieten. Beispiele: Durchführung eines Penetrationstests oder Entwicklung und Implementierung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

Ein Blick auf Deutschland zeigt, dass hier die gleiche Tendenz ablesbar ist: Managed Security Services brachten 2020 einen Umsatz von fast 900 Millionen Euro.

Im Jahr 2028 wird dieser Anteil auf mehr als eine Milliarde Euro anwachsen, was eine Steigerung von fast 93 Prozent bedeutet. Professional Security Services spielen im deutschen Markt allerdings eine größere Rolle: Ihr Umsatz wird 2028 voraussichtlich mehr als 3,1 Milliarden Euro ausmachen.

Umgesetzt

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



Quelle: Statista Market Insights

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

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

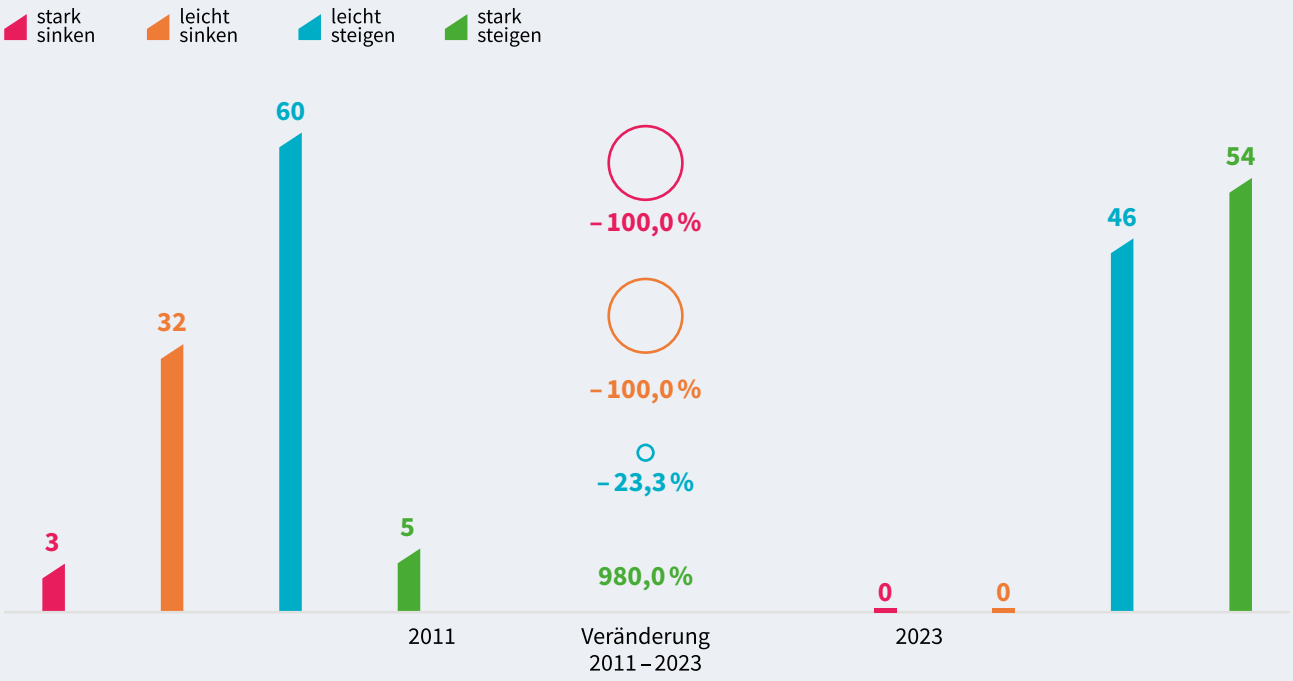
Unternehmen müssen ihre IT Security so aufstellen, dass sie nicht nur für den Moment ausreicht, sondern auch zukunftssicher ist, denn die Bedeutung von Cyberattacken und Datendiebstahl wird zukünftig weiter stark steigen.

2023 gaben dies mehr als die Hälfte (54 Prozent) der Führungskräfte in deutschen Unternehmen an. Im Vergleich zum Jahr 2011 ist dieser Anteil um 980 Prozent gestiegen und auch zukünftig wird der Stellenwert von Cyberkriminalität weiter rasant steigen.

Befürchtungen

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

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



Quelle: teleResearch

Kriterien für Security-Dienstleister

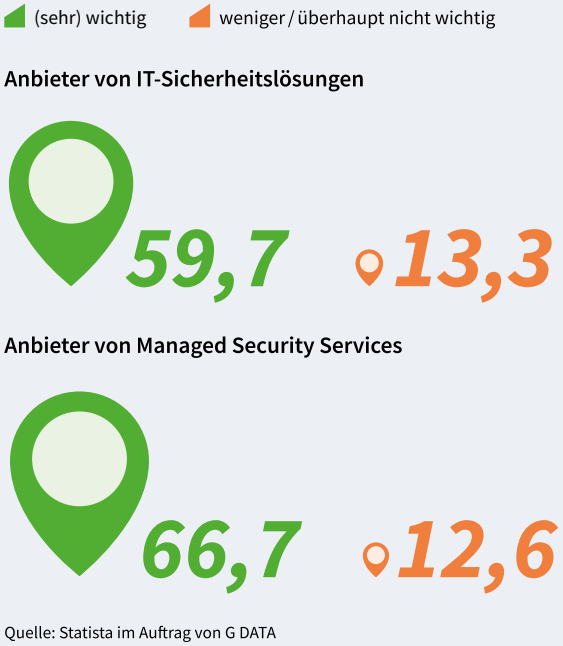
Die Standortfrage ist gerade bei Anbietern von IT-Sicherheitslösungen und Managed Security Providern von entscheidender Bedeutung. Es geht hier nicht nur um den zentralen Vertrauensaspekt, sondern auch darum, welche Datenschutzregelungen gelten. Unter diesen Gesichtspunkten verwundert es nicht, dass zwei Drittel der befragten Administratoren, Team-, Abteilungs- und Bereichsleitenden für IT-Sicherheit oder IT es wichtig oder sehr wichtig finden, wo der Unternehmenssitz des Dienstleisters von Managed Security Services ist. Zudem bevorzugt mehr als die Hälfte (fast 52 Prozent) der Befragten klar einen deutschen IT-Sicherheitsanbieter.

In Deutschland gelten besonders strenge gesetzliche Rahmenbedingungen zum Datenschutz sowie die EU-Datenschutzgrundverordnung.

Standortentscheidungen

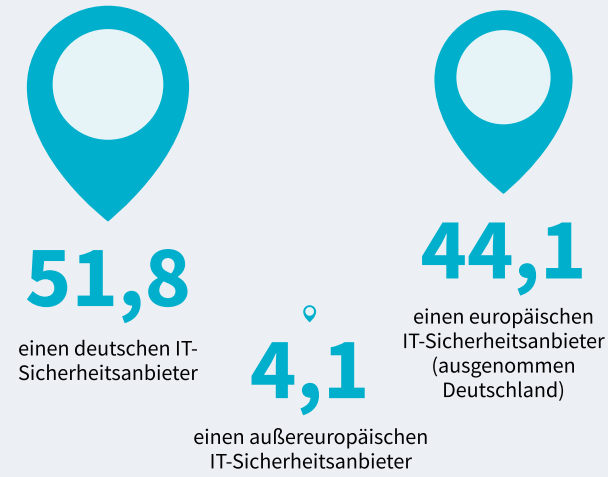
Wichtigkeit des Standorts von Anbietern für IT-Sicherheitslösungen und für Managed Security Services; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die IT-Admin in der IT Security oder IT / EDV sind oder die als Bereichsleitung, Abteilungsleitung oder Teamleitung in der IT Security oder IT / EDV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

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



Quelle: Statista im Auftrag von G DATA

Welchen IT-Sicherheitsanbieter würden Sie bevorzugen?*



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

Die Lösung: G DATA 365 | Managed Extended Detection and Response

IT-Verantwortliche in Unternehmen stehen vor großen Herausforderungen bei der Stärkung der IT-Sicherheit. Mit MXDR von G DATA CyberDefense lösen sie die Probleme des Personalmangels, der fehlenden fachlichen Expertise und den Ressourcenmangel. IT-Mitarbeitende können sich dadurch vollkommen auf ihre Kernaufgaben konzentrieren.

IT Security ist Teamplay

Cybercrime ist ein Rund-um-die-Uhr-Geschäft. Angreifergruppen kennen keinen Feierabend und attackieren auch an Wochenenden oder nachts. Ein 24/7-Schutz der IT-Systeme ist daher unerlässlich, ansonsten bleiben Attacken zu lange unbemerkt. Zudem ist ein weiterer Aspekt von entscheidender Bedeutung: Ist ein Cyberangriff erfolgreich, muss eine Reaktion darauf umgehend erfolgen, um diesen zu beenden und weiteren Schaden abzuwenden. Genau das leistet G DATA 365 | MXDR und ist daher eine lohnende Investition. Dabei überwachen spezialisierte IT-Sicherheitsexperten alle Vorgänge auf den Endgeräten und intervenieren bei Cyberangriffen zu jeder Tages- und Nachtzeit – 24 Stunden täglich und an sieben Tagen in der Woche. Sie werden so zu einem integrativen Teil des Security-Teams des Unternehmens.

G DATA CyberDefense hat die MXDR-Lösung und darin enthaltenen Technologien selbst entwickelt. Das Analystenteam ist so in der Lage, potenziell schädliche Aktivitäten im Netzwerk sicher zu deuten und richtig zu reagieren. Hierdurch kommen die Security-Software und die Response-Dienstleistung aus einer Hand.

Die Webkonsole bündelt alle relevanten Informationen an einem zentralen Punkt und ermöglicht es firmeninternen IT-Teams und Verantwortlichen, Einsicht in Sicherheitsvorfälle und ergriffene Maßnahmen zu nehmen. Hier finden sie auch fundierte und leicht verständliche Handlungsempfehlungen in deutscher Sprache zur Umsetzung. Diese basieren unter anderem auf Root-Cause-Analysen (RCA), die durchgeführt werden, um die Ursachen von Vorkommnissen herauszufinden.

Die angeratenen Maßnahmen sind dabei in unterschiedliche Schweregrade eingeteilt, so dass IT-Admins schnell erkennen, wo ihr Mitwirken dringend erforderlich ist.

G DATA als verlässlicher Anbieter

Durch die Nutzung von **G DATA 365 | MXDR** profitieren IT-Verantwortliche von der **umfangreichen Expertise** des deutschen Cyber-Defense-Spezialisten. Den Unternehmen stehen **persönliche Ansprechpartner** zur Seite und sie werden unterstützt von einem **preisgekrönten 24/7-Support in deutscher Sprache**. G DATA CyberDefense setzt auf eine direkte persönliche Betreuung und nutzt eigens entwickelte Software zur Angriffserkennung, die kontinuierlich auf **Basis von Kundenfeedback** weiterentwickelt wird.

Beim **Onboarding** berät das Cyber-Defense-Unternehmen **individuell** und thematisiert dabei aktiv das Thema **Datenschutz**. Hierbei wird unter anderem festgelegt, auf welchen Endpoints welche spezifische oder eventuell auch keine Response erfolgen soll. Das Onboarding führt G DATA entweder allein oder gemeinsam mit einem **Systemhaus** durch. Die Datenverarbeitung erfolgt ausschließlich auf **Servern in Deutschland**. Damit unterliegen die Informationen den strengen **deutschen Datenschutzrichtlinien**.

Für G DATA CyberDefense stehen sowohl der **Schutz der Kundendaten** als auch die **Cybersicherheit** an erster Stelle.

Weitere Informationen zu G DATA 365 | MXDR und die Option einer unverbindlichen Testphase auf ausgewählten Geräten sind verfügbar auf

www.gdata.de/mxdr

INFORMATION SECURITY MANAGEMENT SYSTEM
ISO 27001:2022
CERTIFIED

TRUST IN GERMAN SICHERHEIT