G DATA CyberDefense

Realitätscheck: IT-Sicherheit in Unternehmen

Umfragen zu Angriffszahlen, Herausforderungen & Strategien

Whitepaper

Inhalt

Liebe Leserinnen und Leser,

die Cybersecurity-Lage ist kritisch: Jeden Tag werden Unternehmen angegriffen und ihre Security-Architektur dabei auf die Probe gestellt. Die Attacken haben aber nicht nur in ihrer Häufigkeit zugenommen. Sie werden auch immer komplexer und sind individuell auf das Unternehmen zugeschnitten – nicht zuletzt durch den vermehrten Einsatz künstlicher Intelligenz. Jede Firma steht daher vor der großen Herausforderung, sich gegen hoch entwickelte Bedrohungen wirksam und umfassend zu schützen. Zum einen, um die wirtschaftliche Existenz zu sichern und zum anderen, um der Regulatorik (wie NIS-2) Rechnung zu tragen. Dafür braucht es mehr als Technologien. Notwendig ist ein tiefes Verständnis für Risiken, Angriffsflächen, Abhängigkeiten und die Folgen eines erfolgreichen Angriffs.

Cybersecurity ist aber nicht nur ein rein technisches Thema. Es ist heute in Zeiten einer veränderten geopolitischen Lage untrennbar mit **digitaler Souveränität** verbunden: Nur wer die Kontrolle über seine digitalen Infrastrukturen, Daten und Sicherheitsprozesse behält, kann langfristig handlungsfähig bleiben.

Als Mitgründer und Vorstand der G DATA CyberDefense AG beschäftigt mich das Thema IT-Sicherheit seit 40 Jahren. Wir verstehen uns nicht nur als Anbieter leistungsfähiger Security-Lösungen und als Dienstleister. Vielmehr sind wir ein verlässlicher Partner, der Unternehmen dabei unterstützt, eine zukunftssichere und unabhängige Sicherheitsarchitektur aufzubauen.

Auf den folgenden Seiten betrachten wir den Status quo der IT-Sicherheit in Unternehmen. Dabei werfen wir auch einen Blick auf die Herausforderungen rund um die Sicherstellung einer effektiven Cyberabwehr. Lassen Sie mich vorab verraten: Die Ergebnisse verdeutlichen eindrucksvoll, wie entscheidend ein ganzheitlicher Ansatz ist, der IT-Verantwortliche und ihre Teams entlastet und dabei für einen umfassenden Schutz sorgt.

Ich lade Sie ein, die Erkenntnisse dieses Papers zu nutzen, um die IT-Sicherheitsstrategie Ihres Unternehmens zu überprüfen und weiterzuentwickeln. Denn eines steht fest: Cybersicherheit ist heute nicht nur eine technische Disziplin, sondern vor allem eine zentrale strategische Aufgabe. Damit wird sie auch zu einem wesentlichen Baustein für die digitale Souveränität Ihrer Organisation.

Ihr Andreas Lüning

Vorstand und Mitgründer | G DATA CyberDefense AG

Ausgangslage

Täglich berichten die Medien über neue Cyberattacken auf Unternehmen und Institutionen. Daher überrascht es nicht, dass viele Menschen einen Angriff selbst erlebt haben. Fast ein Drittel (31 Prozent) der deutschen Arbeitnehmenden hat 2024 einen oder mehrere IT-Sicherheitsvorfälle im eigenen Unternehmen mitbekommen. Dem gegenüber steht eine Mehrheit, die keine Kenntnis von einem Angriff hat. Viele Vorfälle bleiben unentdeckt. Die Angreifergruppen agieren im Verborgenen. Sie nutzen zum Beispiel ungeschlossene Sicherheitslücken in Anwendungen und Betriebssystemen als „Einstieg“ in ein Unternehmensnetzwerk. Für die Schwachstellen existieren oft Updates, aber diese werden aus Zeitgründen erst mit großer Verzögerung oder auch gar nicht eingespielt. Nach dem initialen Zugang geschieht das weitere Vorgehen – zum Beispiel das Nachladen von Schadcode – möglichst unbemerkt. Oft ist ein Angriff erst dann sichtbar, wenn beispielsweise im Fall einer Ransomware die Systeme verschlüsselt sind.

Aufgrund dieser Ausgangslage ist der Einsatz eines Managed Security Operations Centers (Managed SOC) sinnvoll. Durch die kontinuierliche Überwachung der IT-Systeme und aller Aktivitäten werden schädliche Vorgänge sofort erkannt und gestoppt.

Unbemerkt

Wahrnehmung von IT-Sicherheitsvorfällen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2025; in Prozent

Haben Sie im vergangenen Jahr einen IT-Sicherheitsvorfall oder Angriff in Ihrem Unternehmen mitbekommen?

69,0 % nein

21,8 % ja, einen Vorfall oder Angriff

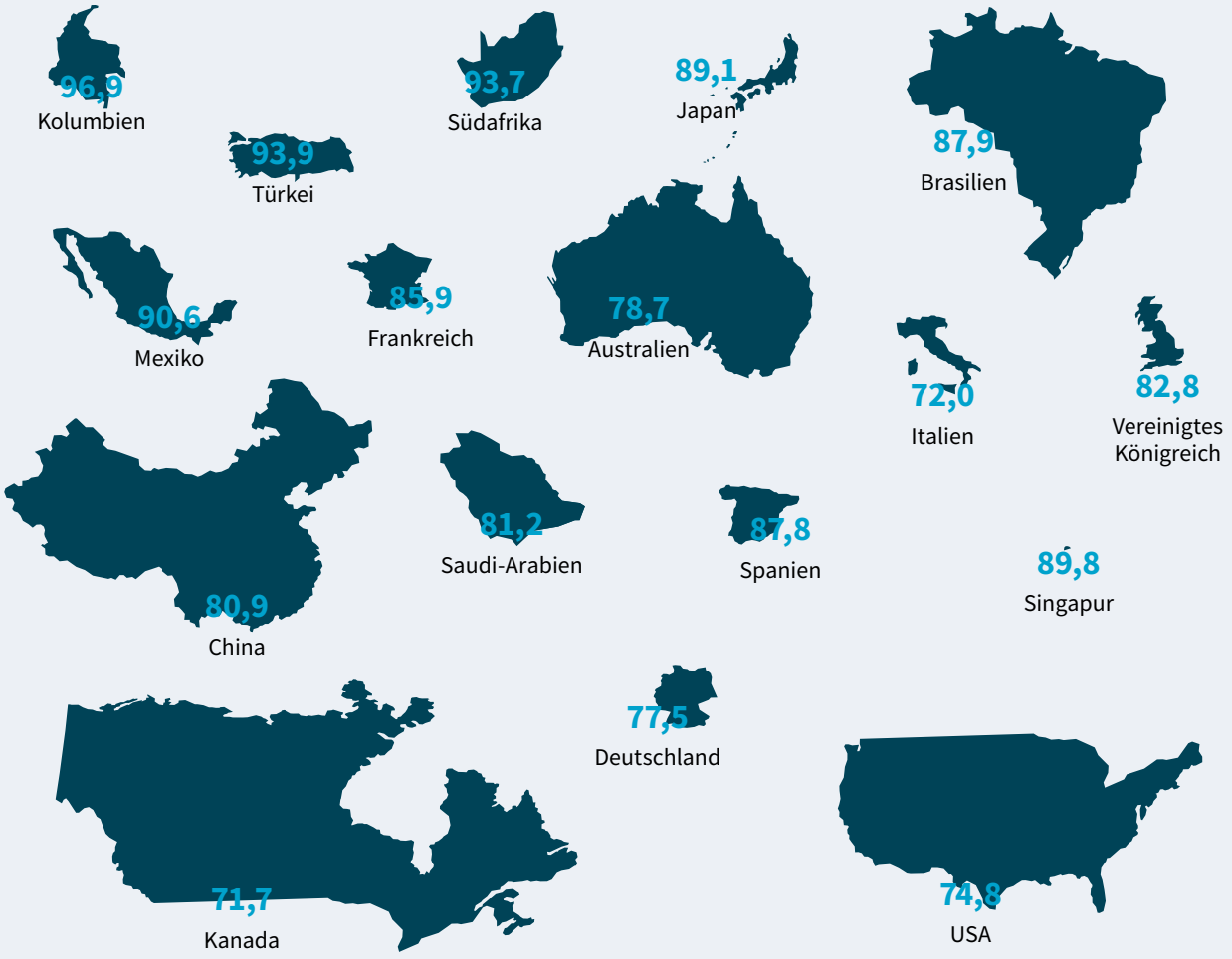
9,2 % ja, mehrere Vorfälle oder Angriffe

Quelle: Statista im Auftrag von G DATA

Die Cyber-Bedrohungslage ist ernst: Auf der ganzen Welt sind 2024 viele Unternehmen Opfer von mindestens einer erfolgreichen Cyberattacke gewesen. In Deutschland waren fast vier von fünf Firmen (78 Prozent) betroffen. Zum Vergleich: Den höchsten Wert verzeichnet Kolumbien mit annähernd 97 Prozent.

Opfer

Anteil der Unternehmen, die in den vergangenen zwölf Monaten mindestens einem erfolgreichen Cyberangriff zum Opfer fielen; IT-Entscheidungsträgerinnen und -träger (n=1.200); weltweit; 2025; in Prozent



Quelle: CyberEdge

Schwerwiegende Konsequenzen

Die Folgen eines Angriffs sind fatal. Insbesondere, wenn dieser nicht frühzeitig entdeckt und eingedämmt wird. Bei den meisten betroffenen Unternehmen – annähernd einem Drittel (32 Prozent) – kam es zu Betriebsausfällen. Für Firmen bedeuten Störungen, dass beispielsweise Güter nicht fristgerecht produziert werden können. In Zulieferbetrieben ist im schlimmsten Fall die ganze Produktionskette gestört, weil Teile fehlen, die verbaut werden müssen. Dies zieht Konventionalstrafen und weitere finanzielle Belastungen mit sich.

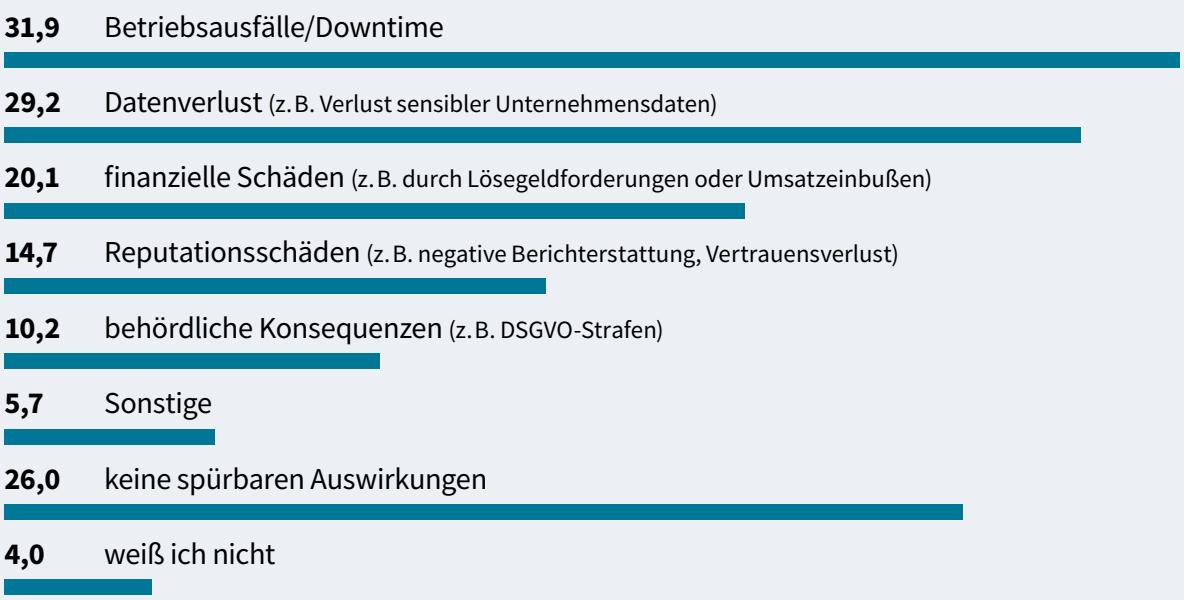
Die zweithäufigste Konsequenz war der Datenverlust, darunter auch sensible Informationen. Mit finanziellen Schäden in Folge eines Angriffs hatte eine von fünf Firmen zu kämpfen. Weitere Folgen waren Reputationsschäden oder behördliche Konsequenzen, zum Beispiel Strafzahlungen im Rahmen der EU-Datenschutzgrundverordnung.

Die Ergebnisse zeigen, wie wichtig ein frühes Eingreifen in das Angriffsgeschehen ist, um negative Folgen einzudämmen oder weitgehend zu verhindern. Ein Managed SOC leistet dies: Angriffe werden in der Anfangsphase beendet, bevor es zu weitreichenden Schäden kommt.

Unabsehbar

Wahrnehmung von IT-Sicherheitsvorfällen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die im vergangenen Jahr einen oder mehrere IT- Sicherheitsvorfälle oder Angriffe erlebt haben; 2025; in Prozent*

Welche Folgen hatte der IT-Sicherheitsvorfall oder Angriff?



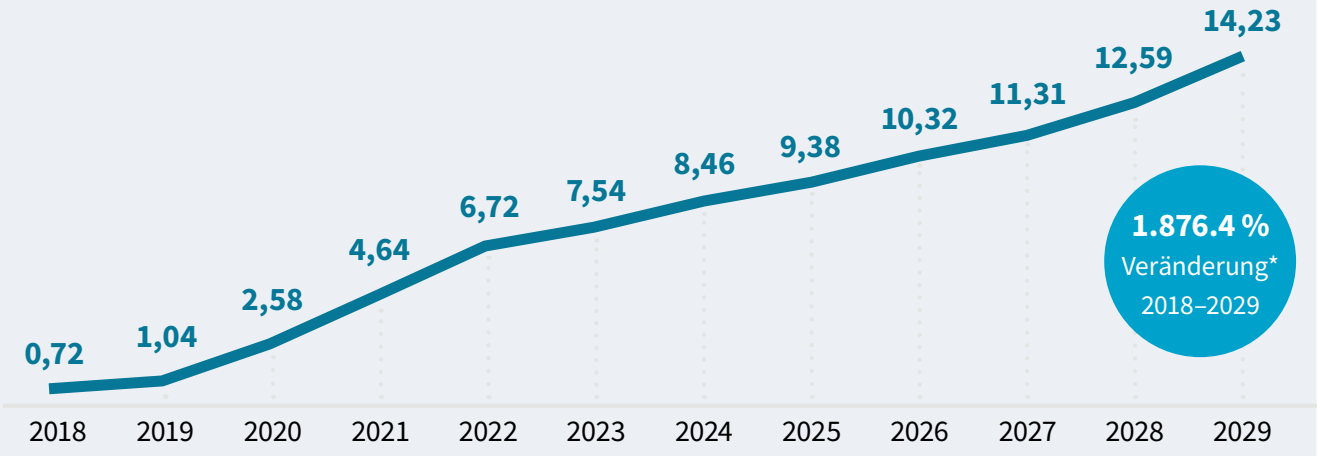
*Mehrfachnennungen möglich. Quelle: Statista im Auftrag von G DATA

Aufgrund der zunehmenden Anzahl von Angriffen steigen auch die Kosten, die Cyberkriminalität verursacht, kontinuierlich. Waren es im Jahr 2018 weltweit noch weniger als eine Billion Euro, wird für 2029 eine Summe von mehr als 14 Billionen Euro prognostiziert. Innerhalb von elf Jahren bedeutet das einen Anstieg von mehr als 1.800 Prozent. Diese Entwicklung macht deutlich, dass Cyberangriffe längst nicht mehr Einzelfälle sind, sondern ein global wachsendes, hochprofessionelles Geschäftsmodell.

Für Unternehmen bedeutet das: Klassische Schutzmaßnahmen reichen allein nicht mehr aus. Angesichts immer komplexerer Angriffsmethoden und stetig steigender Schadenssummen ist ein ganzheitlicher, kontinuierlicher Sicherheitsansatz unverzichtbar.

Kontinuierlich

Zukünftige Entwicklung der Kosten durch Cyberkriminalität; weltweit; in Billionen Euro



Quellen: Statista Market Insights, National Cyber Security Organizations, FBI, IMF

Erwartung: Verschärfung durch den Einsatz von KI

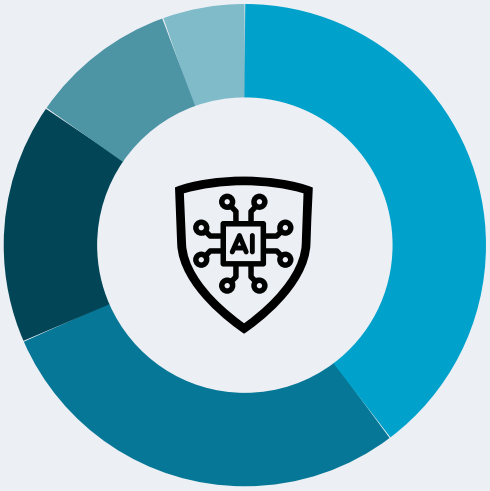
Künstliche Intelligenz (KI) ist in aller Munde – auch bei Cyberkriminellen. Daher glauben sieben von zehn Arbeitnehmenden in deutschen Unternehmen, dass sich die Bedrohungslage durch KI verschärfen wird. Der Grund: Die Angreifergruppen setzen schon heute auf KI, um Schadprogramme zu schreiben oder Phishing-Mails zu generieren. Hierdurch steigt das Gefahrenpotenzial auf ein neues gefährliches Niveau. Nur ein kleiner Teil der Befragten ist der Ansicht, dass das Risiko gleichbleiben wird (16 Prozent) oder sogar sinken könnte (5 Prozent). Die Unsicherheit ist ebenfalls nicht zu unterschätzen: Jeder Zehnte fühlt sich nicht in der Lage, die Entwicklung einzuschätzen – ein Hinweis darauf, wie dynamisch und komplex das Thema KI-Bedrohungen derzeit ist.

Für Unternehmen bedeutet dies: KI eröffnet nicht nur Chancen, sondern verstärkt zugleich die Notwendigkeit, Sicherheitsstrukturen zu modernisieren und auf ein noch höheres Professionalitätsniveau zu heben. Angriffe, die durch künstliche Intelligenz automatisiert, beschleunigt oder präziser werden, überfordern klassische Schutzsysteme zunehmend. KI spielt auch in der Cyberabwehr eine zunehmend wichtige Rolle, etwa bei der Entwicklung von Security-Technologien oder bei der Analyse großer Datenmengen in einem SOC.

Perspektivisch

Einschätzungen zum Einfluss von KI auf IT-Sicherheit; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2025; in Prozent

Erwarten Sie, dass Bedrohungen für die IT-Sicherheit durch den verstärkten Einsatz von künstlicher Intelligenz (KI) zunehmen?



39,8 %	**Ja, in bestimmten Bereichen**: Einige Angriffsszenarien werden durch KI wahrscheinlicher.
28,9 %	**Ja, deutlich**: KI wird die Bedrohungslage erheblich verschärfen.
16,1 %	**Nein, das Risiko bleibt in etwa gleich**: KI verändert die Bedrohungslage nicht wesentlich.
9,7 %	**unsicher**/kann ich nicht beurteilen
5,5 %	**Nein, das Risiko wird eher abnehmen**: KI kann helfen, Sicherheitsmaßnamen zu verbessern.

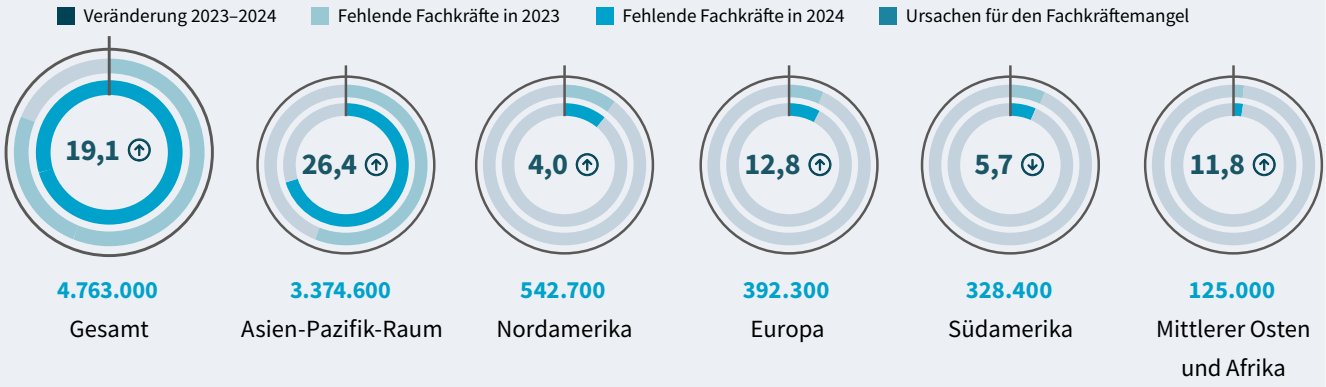
Quelle: Statista im Auftrag von G DATA

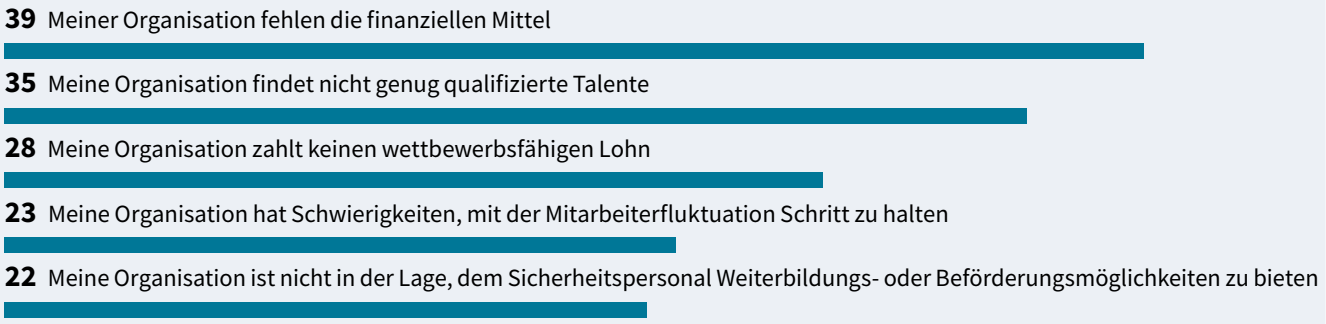
Personalmangel hemmt effektive IT-Sicherheit

2024 fehlten in Europa annähernd 400.000 Fachkräfte für IT-Sicherheit. Im Vergleich zum Vorjahr vergrößerte sich die Lücke um fast 13 Prozent. Dieser Negativtrend ist auch in der deutschen Wirtschaft deutlich wahrzunehmen. Er stellt ein Hemmnis für Security dar, wenn Unternehmen diese vollständig in Eigenregie stemmen – dies aufgrund der personellen Ausstattung aber effektiv nicht möglich ist. Dabei existiert das Problem schon seit längerer Zeit und eine Besserung der Lage ist aktuell nicht in Sicht. Im Gegenteil: Security-Fachleute sind gefragter denn je, da die Lage der Cybersicherheit immer bedrohlicher wird und Unternehmen in ihre Abwehrsysteme investieren müssen. Hierfür brauchen sie qualifiziertes Personal.

Zu wenig Experten, zu wenig Mittel, zu wenig Personal

Fehlende Fachkräfte im Bereich Cybersicherheit nach Regionen, Ursachen für den Fachkräftemangel und Einschätzung dazu; Fachleute für Cybersicherheit (n=1.868); weltweit; 2024; in Prozent





Quellen: (ISC)², ISACA

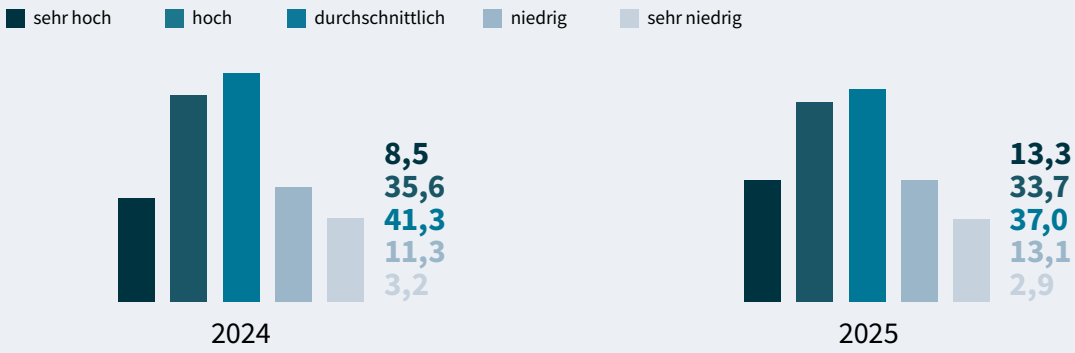
Der Fachkräftemangel in der IT-Sicherheit bleibt für Unternehmen in Deutschland ein ungelöstes und zunehmend drängendes Problem. 2025 schätzt fast die Hälfte (47 Prozent) der Arbeitnehmenden aus den Bereichen IT und IT-Sicherheit den Personalmangel im eigenen Betrieb als hoch oder sogar sehr hoch ein – im Vergleich zum Vorjahr ist das eine leichte Steigerung. Damit geht über die Hälfte der Befragten davon aus, dass sich der Wettbewerb um qualifizierte IT-Security-Expertinnen und -Experten weiter verschärft.

Der Anteil derjenigen, die den Fachkräftemangel als niedrig oder sehr niedrig wahrnehmen, bleibt mit 15 Prozent (2024) beziehungsweise 16 Prozent (2025) auf konstant niedrigem Niveau. Die Mehrheit der Unternehmen ist also dauerhaft unterbesetzt, wenn es um IT-Sicherheit geht. In einer Lage, in der Cyberbedrohungen komplexer werden und qualifizierte Fachkräfte schwer zu finden sind, braucht es Lösungen wie ein Managed SOC, um die Personalengpässe auszugleichen und trotzdem ein hohes Sicherheitsniveau zu ermöglichen.

Ungelöst

Einschätzung des Fachkräftemangels im Bereich IT-Sicherheit; 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; in Prozent

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



Quelle: Statista im Auftrag von G DATA

Aufgrund des Personalmangels haben Unternehmen konkrete Probleme bei der Sicherstellung der Cyberabwehr. Besonders häufig nennen Befragte aus den Bereichen IT und Security Versäumnisse in Prozessen und Verfahren (39 Prozent) sowie die unzureichende Auswertung sicherheitsrelevanter Informationen (38 Prozent), etwa aus Meldesystemen oder Anmeldedaten. Hier zeigt sich klar: Ohne qualifizierte Security-Fachkräfte in ausreichender Anzahl geraten wichtige Analyse- und Kontrollprozesse ins Hintertreffen.

Auch die Ausführung operativer Aufgaben leidet unter dem Personalmangel. Fast zwei von fünf Security- und IT-Fachleuten (38 Prozent) berichten von fehlenden Ressourcen für die Schulung der Belegschaft. Ein Drittel hat zu wenig Zeit für grundlegende Risikomaßnahmen. Selbst kritische Routineaufgaben wie das zeitnahe Patchen wichtiger Systeme (37 Prozent) oder der korrekte Umgang mit falschen Konfigurationen (26 Prozent) werden aufgrund fehlender Fachkräfte beeinträchtigt.

Die Zahlen machen deutlich: Der Fachkräftemangel gefährdet ganz unmittelbar die IT-Sicherheitslage von Unternehmen. Entscheidende Aufgaben bleiben liegen oder werden zu spät erkannt und behoben. Hier zeigt sich, dass IT-Verantwortliche umdenken und die Zusammenarbeit mit einem Security-Dienstleiter in Betracht ziehen sollten. Managed SOC von G DATA CyberDefense unterstützt Unternehmen mit einem erfahrenen Cyber-Defense-Team, das rund um die Uhr Bedrohungen analysiert, verifiziert und bei Bedarf sofort eingreift. Unternehmen erhalten damit eine effektive Cyberabwehr, die unabhängig von ihrem eigenen Personalstand funktioniert und sich sogar dort bewährt, wo interne Teams längst überlastet sind.

Unbefriedigend

Probleme durch einen Mangel an Cybersicherheitspersonal; 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; in Prozent*

Welche der folgenden Probleme haben Sie erlebt, die Ihrer Meinung nach durch eine ausreichende Zahl von Cybersicherheitsmitarbeitenden hätten gemildert werden können?

Versäumnisse in Prozessen und Verfahren

unzureichende Auswertung von Informationen (z. B. Meldungen von der Virenschutzlösung, Nutzeranmeldungen und -abmeldungen)

nicht genügend Ressourcen, um Personal angemessen zu schulen

langsames Patchen von kritischen Systemen

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

Luft nach oben bei der Cyberabwehr

Ein Virenschutz ist immer noch die am häufigsten genutzte Maßnahme zur Abwehr von Cyberangriffen. Mehr als zwei Drittel (68 Prozent) setzen darauf und damit auf eine Lösung, die heute nur noch einen begrenzten Schutz bietet. Der Grund: Cyberkriminelle nutzen mittlerweile verstärkt dateilose Angriffsvektoren, wie ungeschlossene Sicherheitslücken in Anwendungen. Die Erkennung eines klassischen Virenschutzes basiert allerdings auf Schadcode. Damit lässt sich kein schadcode-freier Angriff in der Frühphase aufdecken. Zudem fehlt die Möglichkeit einer Reaktion (zum Beispiel die Separierung des betroffenen Endpoints), die beispielsweise ein Managed Security Operations Center bietet.

Auf den Plätzen zwei und drei folgen Notfallpläne und -übungen (56 Prozent) sowie Security Awareness Trainings (55 Prozent). Weniger verbreitet, aber dennoch essenziell sind regelmäßige Penetrationstests (43 Prozent) sowie Managed Security Services (41 Prozent), die spezialisierte externe Expertise einbeziehen. Noch deutlich unterrepräsentiert ist der Austausch mit Incident-Response-Teams oder Rahmenvereinbarungen für Notfalleinsätze (23 Prozent), sogenannte Incident Response Retainer, obwohl gerade diese Maßnahmen Unternehmen im Ernstfall entscheidend unterstützen.

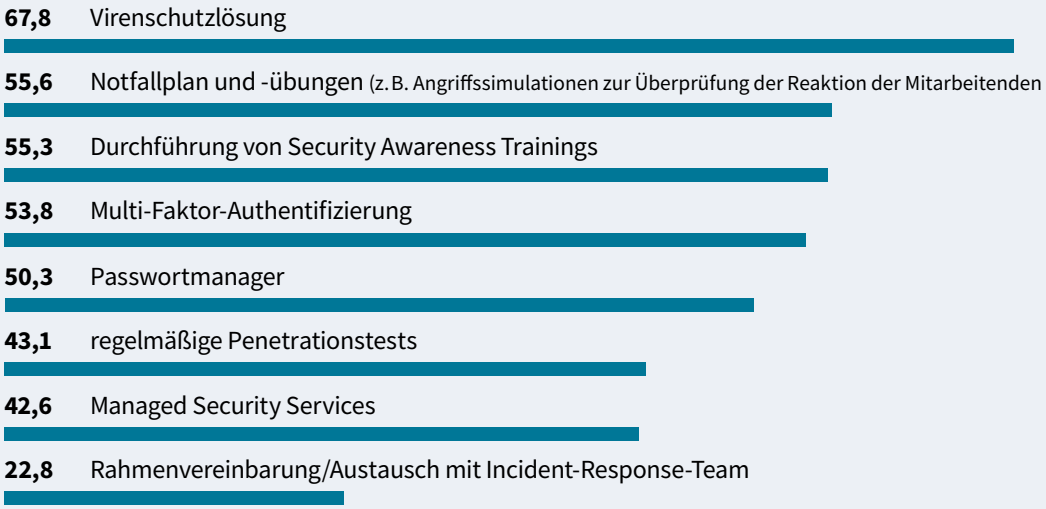
Die Zahlen machen deutlich: Viele Unternehmen investieren zwar in grundlegende Schutzmechanismen und Schulungen, doch eine tiefergehende, kontinuierliche Überwachung und professionelle Reaktion auf Angriffe ist oft nur unzureichend gewährleistet. Hier entsteht eine kritische Sicherheitslücke – vor allem angesichts zunehmend komplexer Angriffsszenarien.

Ein SOC ist für viele Unternehmen eine sinnvolle Investition, insbesondere als Managed Service. Denn der Betrieb eines Security Operations Centers in Eigenregie ist häufig nicht leistbar. Es fehlen sowohl qualifizierte Fachleute als auch das dafür nötige Know-how, um Ergebnisse richtig einzuschätzen. Zudem ist es nur in einem 24/7-Betrieb wirklich effektiv und hiermit ist wieder ein entsprechender Personalaufwand von mehreren Mitarbeitenden notwendig.

Abwehrmaßnahmen

Maßnahmen zur Vorbereitung auf Cyberangriffe; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die als Bereichsleitung, Abteilungsleitung oder Teamleitung in der IT-Security oder IT/EDV arbeiten; 2025; in Prozent*

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



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

Schnelligkeit entscheidet

Bei einem Cyberangriff kommt es auf Schnelligkeit an: Je schneller die Attacke gestoppt wird, desto kleiner fällt der Schaden aus. Erfolgt eine Reaktion zu spät, besteht die Gefahr, dass im schlimmsten Fall die gesamte IT-Infrastruktur lahmgelegt ist und das Unternehmen nicht mehr arbeitsfähig ist. Vergeht mehr Zeit, ist der finanzielle Schaden größer.

Zwar geben 28 Prozent der IT- und Security-Spezialistinnen und -Spezialisten an, innerhalb von Minuten reagieren zu können. Der Großteil benötigt aber deutlich länger. Fast die Hälfte (48 Prozent) der Befragten schafft es erst innerhalb von Stunden. 17 Prozent benötigen sogar einen ganzen Tag, bevor erste Maßnahmen eingeleitet werden können.

Besorgniserregend: 6 Prozent der Unternehmen brauchen mehrere Tage, um auf einen Vorfall zu reagieren. In der Realität können Angriffe jedoch bereits nach wenigen Minuten massiven Schaden anrichten.

Die Zahlen machen deutlich: Reaktionsgeschwindigkeit ist einer der entscheidenden Faktoren für erfolgreiche Cyberabwehr – doch viele Unternehmen können diese Geschwindigkeit aus eigenen Ressourcen nicht sicherstellen. Hohe Arbeitslast, Personalmangel und fehlende 24/7-Überwachung führen dazu, dass Vorfälle oft zu spät erkannt oder bewertet werden.

Wesentliche Geschwindigkeiten

Reaktionsgeschwindigkeit bei IT-Sicherheitsvorfällen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die als Bereichsleitung, Abteilungsleitung oder Teamleitung in der IT-Security oder IT/EDV arbeiten; 2025; in Prozent

Wie schnell reagiert Ihr Unternehmen in der Regel auf einen IT-Sicherheitsvorfall?

Quelle: Statista im Auftrag von G DATA

Regulatorik sorgt für weiteren Druck

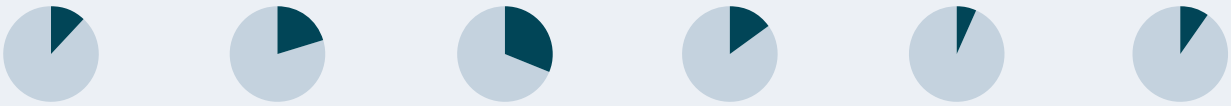
Die Netz-und-Informationssicherheit-2-Richtline (NIS-2) sorgt für einheitliche Sicherheitsstandards und ein höheres Security-Niveau. Die Umsetzung ist für Unternehmen allerdings mit erheblichem Aufwand verbunden. Zum Zeitpunkt der Befragung hat weniger als ein Achtel der Firmen (12 Prozent) NIS-2 vollständig implementiert. Damit ist die Anwendung für einen großen Teil der betroffenen Unternehmen weder abgeschlossen noch ausreichend fortgeschritten. Dabei ist das deutsche Umsetzungsgesetz der EU-Richtlinie mittlerweile beschlossen und gilt seit dem 6. Dezember 2025. Der Druck ist damit immens, denn bei Nichteinhaltung der geforderten Maßnahmen und Regelungen drohen empfindliche Strafen.

Kurz vor dem Abschluss des Prozesses steht eines von fünf Unternehmen. Weniger als ein Drittel der Befragten (31 Prozent) gibt an, mitten in der Umsetzung zu stecken – hier ist deutlich mehr Tempo notwendig. Unerlässlich ist häufig auch eine Umplanung der Security-Architektur, die unter anderem die kontinuierliche Überwachung der IT-Infrastruktur, die Erkennung und Analyse von Sicherheitsvorfällen und die Reaktion darauf vorschreibt.

Gefährlich

Umsetzung der NIS-2-Richtlinie; 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 oder Geschäftsführung/Vorstand sind; 2025; in Prozent

Wie weit ist Ihr Unternehmen mit der Umsetzung der Anforderungen der NIS-2-Richtlinie?



12,1	20,4	31,3	17,9	7,3	11,1
bereits vollständig umgesetzt	in der finalen Umsetzungs-phase	mitten in der Umsetzung	erste Planungen gestartet	noch nicht gestartet	nicht betroffen/ keine Angabe

Quelle: Statista im Auftrag von G DATA

Warum Unternehmen einen Security-Partner brauchen

Der bereits dargestellte Mangel an IT-Sicherheitspersonal ist ein wesentliches Argument für die Zusammenarbeit mit einem Dienstleister. Zudem bringt dieser die benötigte fachliche Expertise mit.

Bei der Auswahl des richtigen Security-Partners legen Unternehmen mehrere Kriterien zugrunde: Am wichtigsten ist das Thema Datenschutz. Dabei ist zu beachten, wo der Anbieter seinen Sitz hat und wo die nötige IT-Infrastruktur gehostet wird. In Europa und besonders in Deutschland gelten strenge Datenschutzgesetze. Daher ist es von Vorteil, wenn der Dienstleister dort sitzt. Genauso wichtig sind den Befragten aus den Bereichen IT und Security die Themen Zertifizierungen und Compliance. Darunter fallen beispielsweise die Konformität mit der EU-Datenschutzgrundverordnung (EU-DSGVO) oder die ISO 27001. Auf dem dritten Platz folgt der Punkt „fortschrittliche Technologie“. Dies ist absolut notwendig, damit die Cyberabwehr mit den Angreifergruppen Schritt hält. Wichtig ist aber nicht nur die technische Ebene. Von entscheidender Bedeutung sind das Fachwissen und die Erfahrung der Spezialistinnen und Spezialisten, welche die Dienstleistung erbringen. Bei einem Managed SOC sind das die Analyse und Einschätzung von potenziellen Vorfällen und die richtige Reaktion im Fall eines Angriffs. Ein Full-Response-SOC lässt sich ansonsten von einem Anbieter nicht effektiv betreiben.

Wesentliche Kriterien

Kriterien für die Zusammenarbeit mit IT-Security-Dienstleistern; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die als Bereichsleitung, Abteilungsleitung oder Teamleitung in der IT-Security oder IT/EDV arbeiten; 2025; Durchschnittsrang (Rang 1 = höchste Priorität)

Welche Kriterien sind Ihnen bei der Zusammenarbeit mit einem IT-Security-Dienstleister am wichtigsten?

2,74

Datenschutz

2,74

Zertifizierungen & Compliance (z. B. ISO 27001, DSGVO-Konformität)

2,81

fortschrittliche Technologie

Quelle: Statista im Auftrag von G DATA

Analystenteam und KI als ideales Match

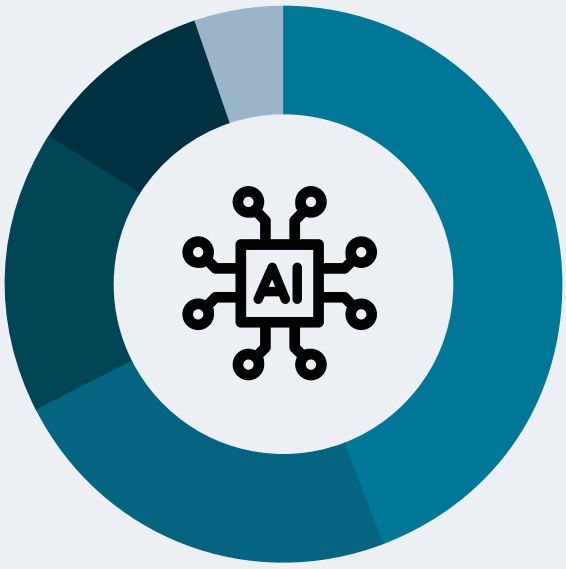
Nicht nur Cyberkriminelle setzen auf künstliche Intelligenz. Sie ist auch auf der anderen Seite der IT-Sicherheit nicht mehr wegzudenken. Die Mehrheit der Arbeitnehmenden in Deutschland (45 Prozent) bevorzugt allerdings eine Kombination aus einem Team und KI. Und das ist genau das, was das SOC-Team von G DATA CyberDefense ausmacht. Generell lassen sich Analystinnen und Analysten nicht vollständig von einer KI ersetzen. Vielmehr ist künstliche Intelligenz eine perfekte Ergänzung, die dafür sorgt, dass entdeckte, potenziell schädliche Aktionen geclustert und vorab eingeschätzt werden. Gerade bei der Überprüfung großer Datenmengen entlastet KI, da sie die „Spreu vom Weizen trennt“ und den Blick auf die kritischen Fälle lenkt. Das macht es den SOC-Spezialistinnen und -Spezialisten einfacher, eine Einschätzung vorzunehmen. Die Reaktion muss zum Unternehmen passen, daher bleibt diese dem Menschen überlassen.

Ausschließlich auf Fachleute setzen zwei von fünf Arbeitnehmende in Deutschland. Nur ein Achtel der Mitarbeitenden (16 Prozent) fühlt sich von einer KI eher oder eindeutig geschützt.

Gemeinschaftlich

Schutzgefühl bei KI vs. Team aus Sicherheitsfachleuten; Arbeitnehmerinnen und Arbeitnehmer in Deutschland; 2025; in Prozent

Würden Sie sich durch eine künstliche Intelligenz besser geschützt fühlen oder durch ein Team aus IT-Sicherheitsfachleuten?



44,5	eine Kombination aus beidem
23,5	eher durch IT-Sicherheitsexperten
16,2	eindeutig durch IT-Sicherheitsexperten
10,8	eher durch KI
5,1	eindeutig durch KI

Quelle: Statista im Auftrag von G DATA

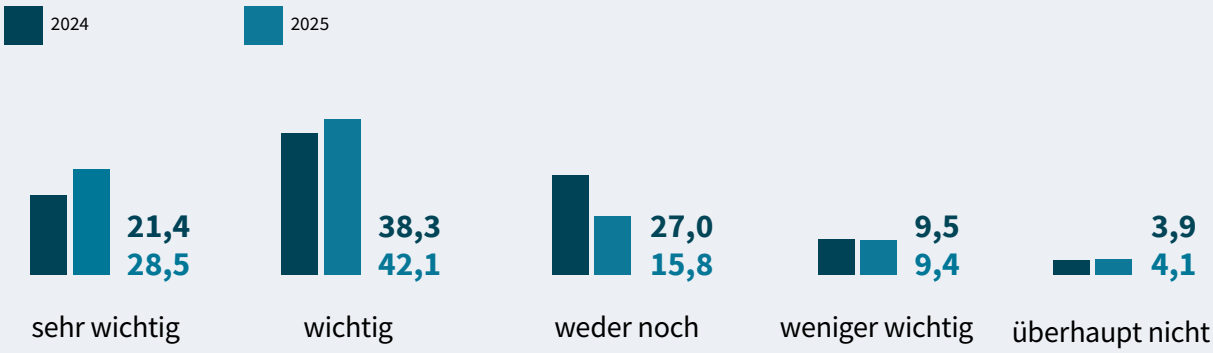
Standort entscheidet

Für Unternehmen spielt der Standort des IT-Security-Anbieters eine entscheidende Rolle. Sieben von zehn Befragten (71 Prozent) aus IT und Security positionieren sich klar. Es ist wichtig oder sogar sehr wichtig, wo der Unternehmenssitz ist. Der Trend ist eindeutig: Die Bedeutung des Standorts steigt kontinuierlich. So vergrößerte sich der Anteil innerhalb eines Jahres um 10 Prozent. Das zeigt, dass IT-Verantwortliche in Firmen genau wissen möchten, wo die Security-Dienstleistungen herkommen und wie wichtig die Themen Vertrauen, Transparenz und rechtliche Rahmenbedingungen sind.

Gute Lage

Wichtigkeit des Standorts von Anbietern für IT-Sicherheitslösungen; 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; in Prozent

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



* Alle Befragten. Quelle: Statista im Auftrag von G DATA

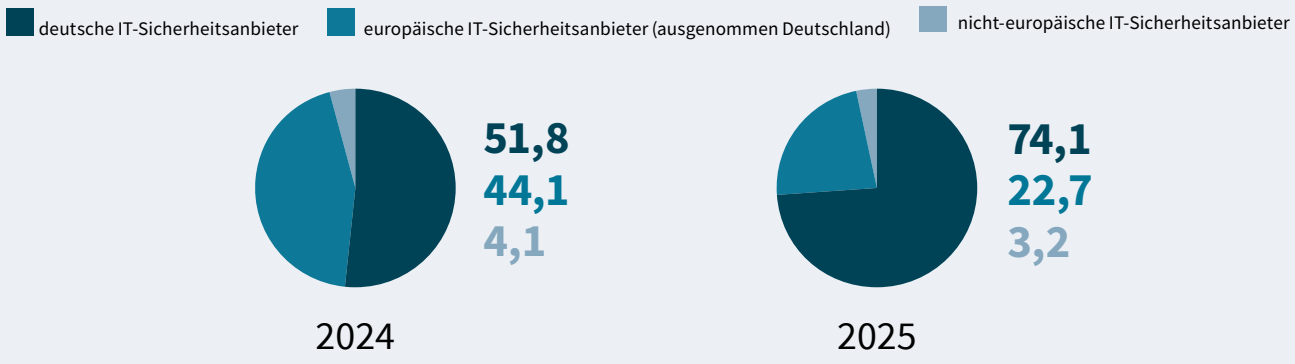
Bei der konkreten Frage, welcher Anbieter bevorzugt wird, zeigt sich: Drei Viertel der Arbeitnehmenden (74 Prozent) mit IT- und Security-Bezug spricht sich für einen deutschen Dienstleister aus. Im Vergleich zum Vorjahr ist dies ein Anstieg um mehr als 20 Prozent. Der Anteil der Befragten, die einen europäischen IT-Sicherheitsanbieter vorziehen, hat sich innerhalb eines Jahres fast halbiert auf jetzt 23 Prozent. Nur wenige Unternehmen ziehen einen nicht-europäischen Dienstleister vor.

Das unterstreicht die große und wachsende Bedeutung des strategischen Themas digitale Souveränität. Warum? Unternehmen können sich heute nicht mehr uneingeschränkt auf außereuropäische Anbieter verlassen. US-amerikanische Dienstleister werden zunehmend von politischen Vorgaben ihrer Regierung beeinflusst und schrecken im Zweifelsfall nicht davor zurück, ihre Dienste einzuschränken. Daher gewinnen gerade die Themen Vertrauen und Souveränität bei der Wahl des passenden Security-Anbieters enorm an Relevanz. Zu prüfen ist dabei, wo dieser den Unternehmenssitz hat und sich die nötigen Serverkapazitäten befinden. Sind diese vollständig in Deutschland, unterliegen sie somit auch dem deutschen Datenschutz.

Gute Entscheidung

Wichtigkeit des Standorts von Anbietern für IT-Sicherheitslösungen; 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 und denen der Standort sehr wichtig oder wichtig ist; in Prozent

Welche IT-Sicherheitsanbieter würden Sie bevorzugen?



* Alle Befragten, denen der Standort sehr wichtig oder wichtig ist. Quelle: Statista im Auftrag von G DATA

Die Lösung: G DATA 365 | MXDR

Das Full-Response-Security-Operations-Center (SOC) von G DATA CyberDefense ist die passende Antwort für Unternehmen auf immer weiter zunehmende Cyberattacken und den zunehmenden regulatorischen Druck.

24/7-Full-Response

Ein erfahrenes Analystenteam überwacht bei G DATA 365 | MXDR das Netzwerk – und das rund um die Uhr. Die Expertinnen und Experten sind vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert. Sie haben alle Vorgänge im Blick und analysieren verdächtig wirkende Aktivitäten, um Unregelmäßigkeiten und schädliche Handlungen aufzudecken. Zeigt die Überprüfung eines Vorganges, dass es sich um eine Attacke handelt, erfolgt sofort und ohne Verzögerung eine passende Reaktion – zum Beispiel die Separierung des betroffenen Endpoints. Dies passiert an 365 Tagen im Jahr. Hierdurch sind Angriffe gestoppt, bevor der Schaden groß ist. Dabei greift das SOC-Team auf fundiertes Fachwissen und langjährige Erfahrung zurück.

Gut informiert

G DATA CyberDefense informiert seine Kundinnen und Kunden persönlich und versorgt sie mit allen relevanten Details. Über leicht verständliche Handlungsempfehlungen in deutscher Sprache über aufgedeckte Vorfälle sorgen die SOC-Spezialistinnen und -Spezialisten für weitere Sicherheit, indem die Ursachen für den Vorfall behoben werden.

Durch die Nutzung von G DATA 365 | MXDR profitieren IT-Verantwortliche von der umfangreichen langjährigen Expertise des deutschen Cyber-Defense-Unternehmens. Der Einsatz der Managed-SOC-Lösung ist für Firmen daher sehr kosteneffizient. Sie müssen keine neuen Fachkräfte einstellen und sind trotzdem in der Lage, rund um die Uhr eine nachhaltige und effektive Cybersecurity sicherzustellen. IT-Verantwortliche benötigen keine weiteren Ressourcen. Durch Managed SOC erweitern sie ihr Security-Team durch die Expertinnen und Experten des Bochumer Cyber-Defense-Spezialisten. Diese sind durch den Austausch mit der internationalen Security-Fachwelt und kontinuierliche Weiterbildungen immer auf dem neuesten Stand in Bezug auf Cybercrime-Strategien. Dieses Wissen bringen sie auch bei der Analyse und Reaktion auf Sicherheitsvorfälle ein.

NIS-2 konform mit G DATA

Die Managed-SOC-Lösung von G DATA unterstützt IT-Verantwortliche in Unternehmen maßgeblich dabei, die Anforderungen der NIS-2-Richtline zu erfüllen. Die EU-Direktive verpflichtet Firmen dazu, ein angemessenes Niveau an Cybersecurity sicherzustellen. Dazu gehören unter anderem Risikomanagement-Maßnahmen. Dank G DATA 365 | MXDR sind die IT-Systeme 24/7 überwacht und die Reaktion auf Security-Vorfälle gewährleistet – wie es NIS-2 vorschreibt. Des Weiteren unterstützt die Lösung im Fall von Cyberangriffen bei den Reportingpflichten und sorgt durch Handlungsanweisungen proaktiv für mehr Resilienz.

Verlässlicher Partner

Kundinnen und Kunden stehen persönliche Ansprechpartner zur Seite, unterstützt von einem preisgekrönten 24/7-Support in deutscher Sprache, der zu G DATA gehört. Der Cyber-Defense-Spezialist verzichtet auf externe Call-Center und fluktuierende „Follow-the-Sun"-Arbeitsweisen. Damit ist eine qualitativ hochwertige, direkte und persönliche Betreuung möglich – auch am Wochenende oder an Feiertagen.

Beim Onboarding berät das Cyber-Defense-Unternehmen individuell und thematisiert dabei aktiv das Thema Datenschutz. Dabei wird unter anderem festgelegt, auf welchen Endpoints welche spezifische Response durchgeführt werden soll. Das Onboarding erfolgt wahlweise durch G DATA oder gemeinsam mit einem IT-Security-Dienstleister.

Digitale Souveränität

G DATA hat seinen Sitz in Bochum, dem Hotspot der IT-Sicherheit, und unterliegt damit dem deutschen Datenschutz. Beim Cyber-Defense-Spezialisten erfolgt die Datenverarbeitung ausschließlich auf Servern, die in Deutschland stehen.

Zudem gilt das Gebot der Sparsamkeit. Es werden nur die Informationen erhoben, die zur Analyse und Behebung von Vorfällen erforderlich sind. Dieser Aspekt ist für IT-Verantwortliche äußerst wichtig, denn ein Managed SOC erfordert grundsätzlich, dass Anbieter vollen Einblick in die firmeneigenen Daten erhalten. G DATA wurde bereits für den vertrauensvollen Umgang mit Kundendaten ausgezeichnet. Sowohl der Schutz sensibler Daten als auch der Schutz vor Cyberbedrohungen stehen für G DATA CyberDefense an oberster 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