G DATA CyberDefense

Realitätscheck: IT-Sicherheit im öffentlichen Sektor 2025

Umfragen zu Angriffszahlen, Herausforderungen & Strategien

Whitepaper

Inhalt

Liebe Leserinnen und Leser,

was verbindet Städte und Landkreise in ganz Deutschland – unabhängig von Größe, Struktur oder Bundesland? Eine Gemeinsamkeit, die auf den ersten Blick unsichtbar ist, aber große Wirkung entfaltet: Sie wurden Opfer gezielter Cyberangriffe.

Diese Vorfälle sind längst keine Ausnahmen mehr. Die steigende Zahl betroffener kommunaler Einrichtungen zeigt deutlich: Es kann jede öffentliche Institution treffen. Der Grund ist ebenso einfach wie alarmierend – Cyberkriminelle agieren strategisch und gewinnorientiert. Sie suchen gezielt nach Schwachstellen, bei denen sich mit geringem Aufwand ein hoher Schaden oder Profit erzielen lässt. Kommunale IT-Strukturen geraten dabei zunehmend ins Visier, da sie vielerorts als besonders angreifbar gelten.

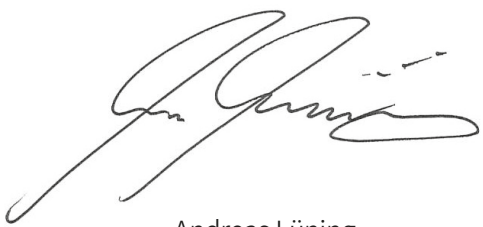
Doch Cyberangriffe gefährden nicht nur technische Systeme – sie untergraben das Vertrauen der Bürgerinnen und Bürger in die Leistungsfähigkeit digitaler Verwaltungsprozesse. Wenn digitale Dienste ausfallen oder personenbezogene Daten gefährdet sind, entsteht schnell der Eindruck, dass öffentliche Stellen digitalen Herausforderungen nicht gewachsen sind. Eine robuste Cybersicherheit ist daher unerlässlich, um das Vertrauen in moderne und verlässliche Verwaltung zu sichern.

Digitale Souveränität bedeutet in diesem Kontext vor allem eines: handlungsfähig bleiben – auch im Krisenfall. Kommunen müssen wissen, auf wen sie sich verlassen können. Wie stabil und unabhängig sind eingesetzte Sicherheitslösungen in einer sich geopolitisch verändernden Welt? Die Antworten auf diese Fragen sind komplex – und doch entscheidend für unsere Zukunftsfähigkeit. Es braucht ein gemeinsames Kraftpaket: verlässliche politische Rahmenbedingungen, gezielte Fördermaßnahmen sowie mehr Mut zu langfristigen, strategischen Investitionen in sichere IT-Infrastrukturen.

Wie es um die digitale Widerstandskraft von Städten, Landkreisen und öffentlichen Einrichtungen steht, zeigt eine repräsentative Studie, die wir gemeinsam mit brand eins und Statista durchgeführt haben. Die Ergebnisse bieten nicht nur eine umfassende Standortbestimmung, sondern auch wertvolle Impulse: vom Umgang mit Fachkräftemangel und knappen Budgets bis hin zu konkreten Lösungsansätzen für mehr Sicherheit im kommunalen Raum.

Ich lade Sie herzlich ein, sich mit den Erkenntnissen dieser Publikation auseinanderzusetzen – und mit uns in den Dialog zu treten. Lassen Sie uns gemeinsam daran arbeiten, die digitale Zukunft sicher, souverän und vertrauenswürdig zu gestalten.

Herzliche Grüße,



Andreas Lüning

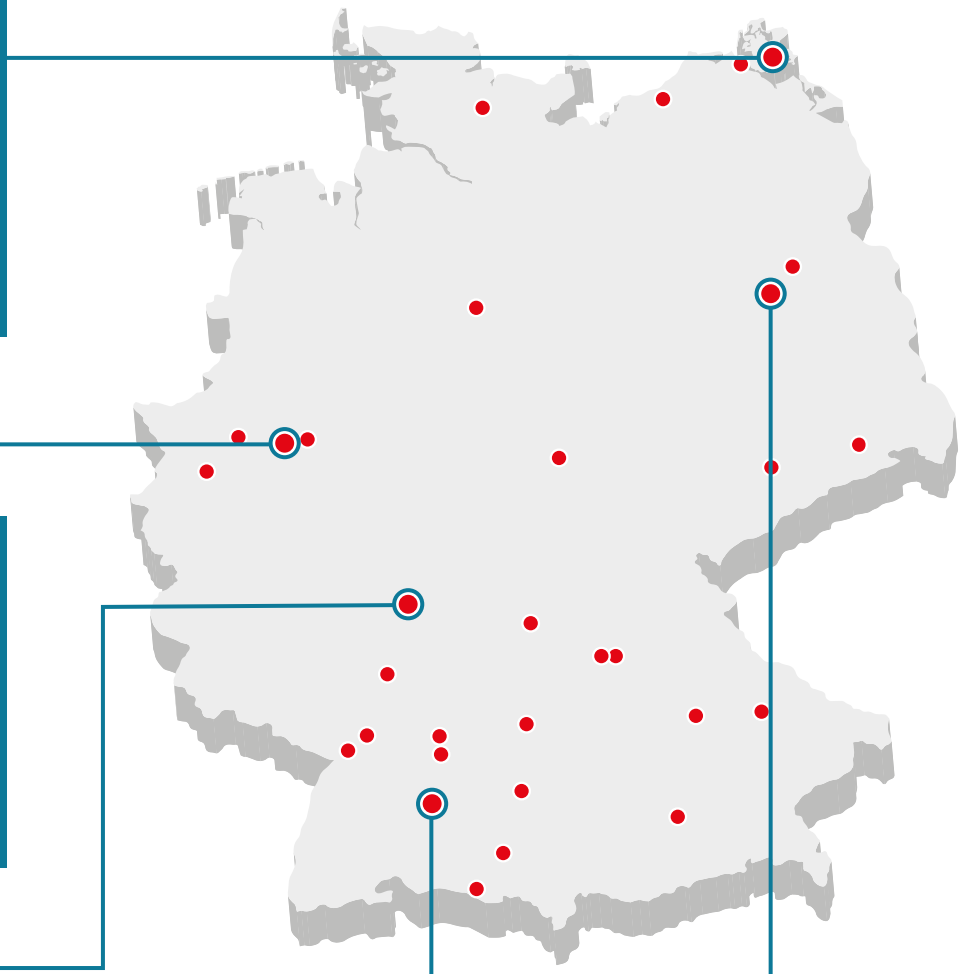
Vorstand und Mitgründer | G DATA CyberDefense AG

Cyberangriffe auf Kommunen und kommunale Betriebe 2023–2025

Darstellung von öffentlich bekannten Fällen mit weitreichenden Folgen für die Kommunen.
Es ist jedoch von einer hohen Dunkelziffer auszugehen, da nicht alle Vorfälle gemeldet werden.

Rügen, 2024

Nach einer Ransomware-Attacke konnte die Amtsverwaltung Rügen nur eingeschränkt arbeiten. Vermutlich war geplant, ein Lösegeld zu erpressen. Die Verwaltung öffnete aber aus Sicherheitsgründen den Link nicht. Die Wiederherstellung der IT-Systeme verzögerte sich, da die vorgezogene Bundestagswahl Priorität hatte.



Schwerte, 2024

Ein Cyberangriff auf die Stadtwerke Schwerte legte die internen Dienste und das Kundenportal lahm. Die Stadt Schwerte musste ihre Verbindung zu den Stadtwerken und ihrem Dienstleister Südwestfalen-IT trennen. So fielen viele kommunale Dienste, wie Pass- und Meldewesen, aus.

Rodgau, 2023

Die Stadt Rodgau samt Stadtwerken wurde durch einen Ransomware-Angriff mittels einer E-Mail lahmgelegt. Die Angreifer zogen ca. ein Terabyte an Daten ab. Eine Lösegeldzahlung erfolgte laut Stadt nicht. Die Kosten für den Wiederaufbau der IT-Systeme werden im 7-stelligen Bereich geschätzt.

Mössingen, 2023

Als die Stadt Mössingen einen Cyberangriff bemerkte, unterbrach sie die Internetverbindung. Online-Dienste fielen aus, nur Telefon ging. Erste Behelfslösungen wurden rund zwei Wochen später eingerichtet, etwa für Zahlungsverkehr. Laut LKA verlief die Reaktion dank eines guten Notfallplans erfolgreich.

Potsdam, 2023

Nach einer Angriffswarnung musste die Stadt Potsdam ihre Internetverbindungen kappen. Auch Stadtwerke und Klinikum gingen offline. Beim Neustart wurde weiterhin Schadsoftware entdeckt. E-Mails, Wohngeldanträge, Kfz-Anmeldungen und mehr fiel aus. Die Wiederherstellung dauerte über ein Jahr.

Quelle: Heinrich-Böll-Stiftung, KommunalWiki (2025)

Zwischen Realität und Risikowahrnehmung

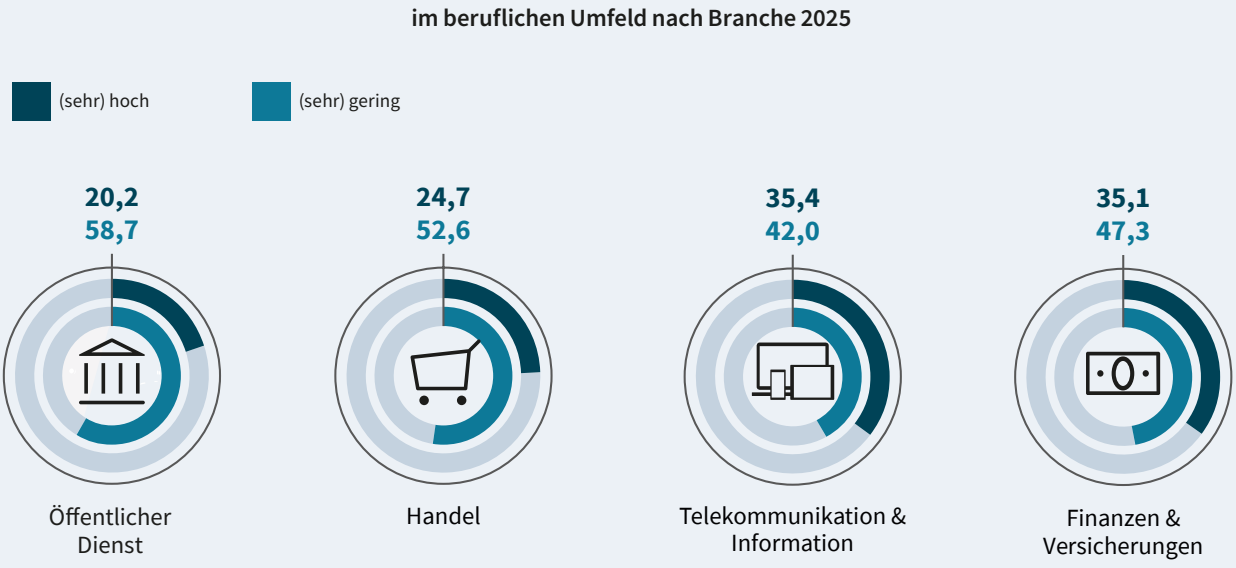
Täglich werden erfolgreiche Cyberangriffe mit weitreichenden Auswirkungen bekannt. Die Deutschlandkarte zeigt, wie sehr auch der öffentliche Sektor davon betroffen ist. Das Ganze belegt: Die Cyberbedrohungslage ist hoch und damit auch die Wahrscheinlichkeit, ein Angriffsopfer zu werden. Trotz dieser Ausgangslage schätzt die Hälfte der Arbeitnehmenden in Deutschland das Risiko als gering oder sogar sehr gering ein. Nur etwas mehr als ein Viertel (27,4 Prozent) glaubt an eine hohe oder sehr hohe Gefahr und liegt damit richtig. Generell ist jede Mitarbeiterin, jeder Mitarbeiter, jedes Unternehmen und auch jede Stadt beziehungsweise jede kommunale Einrichtung ein lohnendes Angriffsziel für Cyberkriminelle.

Ein Blick auf die Branchen zeigt, dass die Beschäftigten des öffentlichen Dienstes am wenigsten sensibel für die Gefahrenlage sind: Drei von fünf kommunalen Angestellten (59 Prozent) sind davon überzeugt, nur einem geringen Gefahrenpotenzial durch Cyberkriminalität ausgesetzt zu sein. Nur 20 Prozent glauben an ein hohes Risiko. Ähnlich sieht es beim Handel aus. In den Branchen „Telekommunikation und Information“ und „Finanzen und Versicherungen“ ist der Anteil der gefahrenbewussten Mitarbeitenden mit jeweils 35 Prozent am höchsten.

Die Zahlen belegen, dass die IT-Verantwortlichen der Städte und anderen Einrichtungen des öffentlichen Dienstes noch viel in die Security Awareness der Mitarbeitenden investieren und zu einer realistischen Risikoeinschätzung und -bewertung kommen müssen. Nur auf dieser Basis ist es möglich, die richtige Cyberabwehr-Strategie zu planen und die nötigen Maßnahmen umzusetzen, um das Risiko durch Angriffe beherrschen zu können.

Befürchtungen

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



Quelle: Statista im Auftrag von G DATA

Wahrnehmung von Cyberangriffen

Im Bereich öffentliche Verwaltung waren bereits fast die Hälfte der Befragten (45 Prozent) von einer Cyberattacke betroffen oder hatten davon im Kollegenkreis gehört. Das zeigt, dass die Wahrnehmung der verschärften Bedrohungslage und zunehmenden Anzahl von Angriffen grundsätzlich vorhanden ist. Annähernd ein Drittel der kommunalen Mitarbeitenden kennt Fälle durch den Austausch mit Kolleginnen und Kollegen.

Häufig ist ein schwerwiegender Angriff, der nicht frühzeitig erkannt oder rechtzeitig eingedämmt wurde, mit weitreichenden und schwerwiegenden Systemausfällen verbunden. Auf der kommunalen Ebene bedeutet das, dass gerade Bürgerservices nicht funktionstüchtig sind und beispielsweise Wohngeld oder Unterhaltszuschüsse nicht ausgezahlt werden können. Die IT-Infrastruktur ist wochenlang, häufig sogar über Monate nicht funktionsfähig. Anschließend arbeiten die Systeme zunächst nur eingeschränkt. Bis eine erfolgreiche Attacke vollständig bewältigt ist, dauert es oft eine lange Zeit. Nur auf dieser Basis ist es möglich, die richtige Cyberabwehr-Strategie zu planen und die nötigen Maßnahmen umzusetzen, um das Risiko durch Angriffe beherrschen zu können.

Schon mal erlebt

Persönliche Erfahrung mit Cyberangriffen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die im öffentlichen Dienst arbeiten; 2025; in Prozent

Haben Sie schon einmal einen Cyberangriff in Ihrer Verwaltung miterlebt – oder davon in Ihrer Verwaltung gehört?

12,7 % ja, persönlich erlebt

31,9 % ja, im Kollegenkreis gehört

55,4 % nein, bisher nicht

Quelle: Statista im Auftrag von G DATA

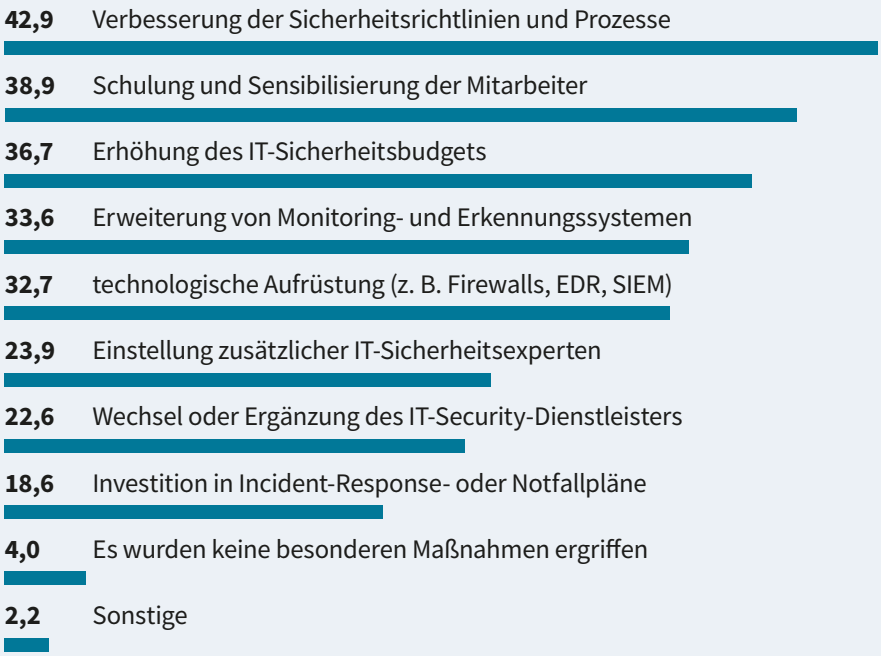
Maßnahmen infolge von Attacken

In der Folge eines erfolgreichen Cyberangriffs ergreifen IT- und Security-Verantwortliche im Regelfall weitere Maßnahmen, um einen erneuten Vorfall zu verhindern. Befragte in Leitungspositionen, die in den letzten Jahren eine oder mehrere Attacken zu bewältigen hatten, setzten mehrheitlich (43 Prozent) auf die Verbesserung der Sicherheitsrichtlinien und -prozesse. Dies deutet auf strukturelle Probleme in der Organisationsstruktur hin. 37 Prozent erhöhte das IT-Sicherheitsbudget. Ein Drittel investierte in die Erweiterung von Monitoring- und Erkennungssysteme. Darunter fällt beispielsweise ein Managed Security Operations Center (Managed SOC). Damit ist die Security-Architektur technisch auf einem höheren Sicherheitsniveau als sie es vorher war. Knapp 24 Prozent stellte zusätzliche IT-Sicherheitsexperten ein. Diese Maßnahme ist für Städte, Landkreise und andere Einrichtungen oft nur schwer umsetzbar. Zum einen herrscht akuter Fachkräftemangel – speziell in der IT-Sicherheit. Zum anderen ist der öffentliche Dienst kein attraktiver Arbeitgeber für Spezialistinnen und Spezialisten. Sie können hohe Gehälter für ihre Arbeit verlangen, die sich nicht in der starren öffentlichen Tarifstruktur (TVöD/TV-L) von Kommunen wiederfinden lassen. In der freien Wirtschaft können Security-Spezialistinnen und -Spezialisten Löhne, Zusatzleistungen und Bonuszahlungen verhandeln. IT-Leitenden im kommunalen Umfeld sind hier die Hände gebunden, sodass sie freie Stellen (wenn diese überhaupt ausgeschrieben sind) kaum besetzen können. IT-Sicherheit lässt sich so aus eigener Kraft nicht bewerkstelligen.

Ungenügend

Konsequenzen aus IT-Sicherheitsvorfällen; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die als Bereichsleitung, Abteilungsleitung oder Teamleitung in der IT-Security oder IT / EDV arbeiten und die im letzten Jahr einen oder mehrere IT-Sicherheitsvorfälle oder Angriffe erlebt haben; 2025; in Prozent *

Welche Konsequenzen wurden aus dem IT-Sicherheitsvorfall oder Angriff gezogen?



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

KI verschärft Gefahrenlage

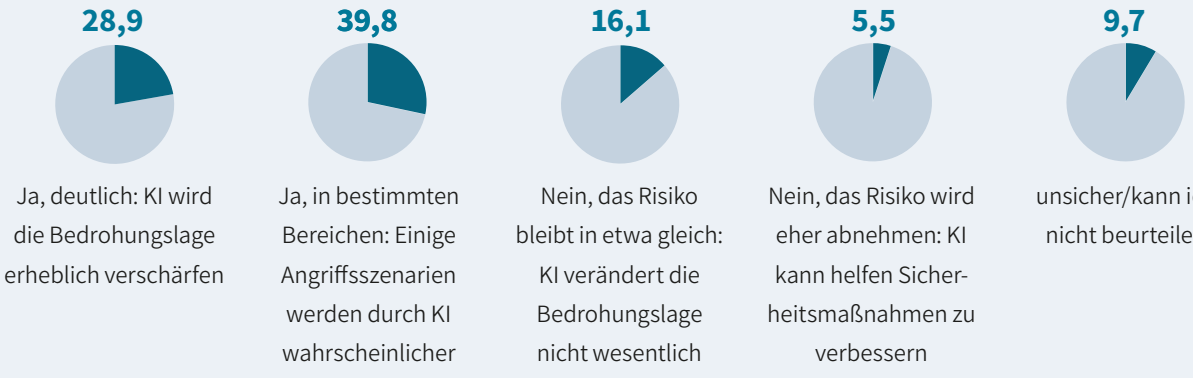
Künstliche Intelligenz (KI) birgt Kommunen viele Vorteile. Sie steigert die Effizienz und die Qualität von Arbeitsabläufen und Prozessen. Daher ist KI aus der Arbeitswelt nicht mehr wegzudenken. Diesen Nutzen haben auch Cyberkriminelle für sich entdeckt und nutzen Künstliche Intelligenz für Angriffe. Daher blicken fast 30 Prozent der Arbeitnehmenden eher pessimistisch in die Zukunft und gehen davon aus, dass sich die Gefahrenlage durch KI erheblich verschärfen wird. Zwei von fünf Befragten (40 Prozent) erwartet eine Verschlimmerung von Angriffen in einzelnen Bereichen. Zusätzlich gehen sie davon aus, dass hierdurch Angriffsszenarien wahrscheinlicher werden, die mithilfe von Künstlicher Intelligenz aus Sicht der Kriminellen effektiver sind.

Cyber-Defense-Expertinnen und -Experten beobachten schon heute, dass Angreifergruppen KI nutzen, um beispielsweise die Erstellung von Schadprogrammen oder das Aufspüren von Schwachstellen in IT-Systemen zu automatisieren. Social Engineering, zum Beispiel in Form von Phishing, ist durch KI schwerer zu erkennen. Die Mails sind hierdurch zielgerichteter und wirken realistischer, da sie beispielsweise ohne Rechtschreibfehler auskommen. Das zeigt: Eine zukunftsträchtige IT-Sicherheit, die auch beim Einsatz von Künstlicher Intelligenz effektiv funktioniert, ist essenziell.

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?



Quelle: Statista im Auftrag von G DATA

„Die größten Schwachstellen sind falsche Priorisierungen und fehlende Prozesse“

Ein Interview mit Jan Leitzgen, IT Security Consultant bei G DATA Advanced Analytics, über Cyberangriffe auf Kommunen, strukturelle Schwächen und pragmatische Sofortmaßnahmen.

Warum erkennen viele IT-Verantwortliche Cyberangriffe auf Städte und Kommunen zu spät? Stehen sie besonders im Fokus von Cyberkriminellen?

Jan Leitzgen: *„Die typischen Einfallstore sind schwache Passwörter, nicht gepatchte Systeme sowie fehlende Zwei-Faktor-Authentifizierung bei VPN-Zugängen. Hinzu kommt: Häufig ist die IT personell unterbesetzt und da bleibt kaum Luft für Prävention wie das Auswerten des Monitorings. Zudem fehlt den Angestellten Awareness, um überhaupt verdächtige Aktionen zu erkennen. Und es mangelt dann auch an Prozessen, um Phishing zu melden.*

Kommunen sind selten gezielt im Visier, aber sie sind eine leichte Beute für Cyberkriminelle. Es fehlt an grundlegenden Sicherheitsmaßnahmen: klare Prozesse, Notfallpläne oder Security Awareness unter Mitarbeitenden. Wenn dann eine Phishing-Mail eintrifft oder ein veralteter Dienst offen zum Internet exponiert ist, haben Angreifergruppen leichtes Spiel. Ein weiteres Sicherheitsrisiko, das sehr verbreitet ist: Nutzt ein IT-Admin ein und dasselbe Passwort für sein persönliches Profil und den Admin-Zugang, die dann auch nicht zusätzlich mit einer Zwei-Faktor-Authentifizierung abgesichert sind, können sich die Täter ungehindert im Netz bewegen, Daten ausleiten und Systeme verschlüsseln.“

Was passiert, wenn ein Angriff erfolgreich ist? Welche konkreten Auswirkungen hat das auf die Verwaltung und die Bürgerinnen und Bürger?

Jan Leitzgen: *„Wenn Cyberkriminelle Daten und Systeme verschlüsselt haben, kommt der Geschäftsbetrieb zum Erliegen. Bürgerbüros, Ausweisstellen, Kfz-Zulassungen – nichts funktioniert mehr. Sozialleistungen werden nicht ausgezahlt und die Kommunikation zwischen Fachbereichen bricht ab.*

Wer jetzt keine Notfallpläne und keinen Überblick über die Systemlandschaft hat, ist zunächst hilflos und verliert wertvolle Zeit. Dabei sind die ersten Stunden besonders wichtig, um etwa einen Notbetrieb vorzubereiten. Dafür muss aber definiert sein, welche Systeme priorisiert wieder hochgefahren werden müssen. Besonders kritisch wird es, wenn keine klare Kommunikationsstrategie existiert. Ohne einen Notfallplan geraten viele Verwaltungen in einen Panikmodus, den wir den „Headless Chicken Mode“ nennen.“

Wie lange dauert es aus deiner Erfahrung, bis eine betroffene Kommune wieder arbeitsfähig ist? Und wann ist der Normalbetrieb wiederhergestellt?

Jan Leitzgen: *„In den ersten Tagen befinden sich IT und Krisenstab im Ausnahmezustand – 12-Stunden-Tage, auch am Wochenende. Bis sukzessive ein stabiler Notbetrieb steht, vergehen in der Regel sechs bis acht Wochen. Erst dann ist eine geregelte Kommunikation wieder möglich und Verwaltungsleistungen sind wieder abrufbar.*

Den Normalbetrieb erreichen Kommunen oft nach sechs bis neun Monaten. Aber „Normalbetrieb“ heißt nicht: Alles ist jetzt sicher. Es bedeutet, dass die ausgenutzten Schwachstellen mitigiert wurden – meist mit überschaubaren Ressourcen. Eine langfristige Steigerung der IT-Sicherheit erfordert mehr Budget, mehr Zeit und vor allem mehr Personal. Und genau daran hapert es leider.“

Was können Kommunen sofort tun, um ihre IT-Sicherheit zu verbessern – auch mit knappen Mitteln?

Jan Leitzgen: *„Erstens: Sichtbarkeit schaffen. Ohne Monitoring bleiben verdächtige Aktivitäten unsichtbar. Wer weiß schon, was im eigenen Netzwerk passiert? Tools wie XDRs (Extended Detection and Response) können eine große Hilfe sein – vor allem, wenn externe Dienstleister mit an Bord sind.*

Zweitens: Die Reaktionsfähigkeit erhöhen. Ein Notfallplan, also eine Handlungsanleitung für den Ernstfall, hilft enorm. Es muss nicht perfekt sein, aber realistisch: Wer macht was, wenn jemand auf einen Phishing-Link klickt? Welche Accounts müssen sofort gesperrt werden? Wer informiert wen? Und das Wichtigste: Wer darf welche Entscheidungen treffen?

Und drittens: Passwörter und Perimeter prüfen. Exponierte Dienste sollten zwingend mit einer Zwei-Faktor-Authentifizierung abgesichert sein. Schwache Passwörter gehören abgeschafft – auch wenn das unbequem ist. Es geht hier nicht um „gängeln“, sondern um das digitale Überleben.“

Frage: Was rätst du Kommunen, die wenig Personal haben und trotzdem etwas bewegen wollen?

Jan Leitzgen: *„Sie sollten sich Hilfe holen und mit dem Machbaren anfangen. Es geht nicht darum, morgen alles perfekt zu machen. Es geht darum, den ersten Schritt zu gehen. Wer seine größten Schwachstellen kennt und einen Plan hat, bewegt sich vom reaktiven Krisenmodus hin zur souveränen Sicherheitskultur. Und ja, auch das geht im öffentlichen Sektor.“*

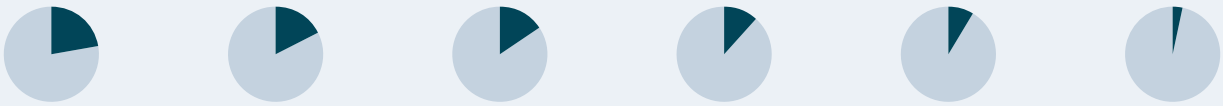
Herausforderung IT-Sicherheit in Kommunen

IT-Verantwortliche in Verwaltungen und kommunalen Unternehmen haben große Probleme, eine effektive IT-Sicherheit zu gewährleisten. Vier von fünf Arbeitnehmenden in Deutschland (82 Prozent) haben mit Herausforderungen zu kämpfen. Die größte Schwierigkeit besteht für mehr als ein Fünftel der Befragten (22 Prozent) darin, genug Fachpersonal zur Verfügung zu haben. Auf Platz zwei folgt eine veraltete Technik, was einen Investitionsstau offenbart. Eine moderne IT-Sicherheitsinfrastruktur ist die Basis für eine funktionierende Security-Architektur. Darunter fallen nicht nur Hardware, sondern auch Software und Betriebssysteme – alle Systeme sind grundsätzlich auf einem aktuellen Stand zu halten und müssen gegebenenfalls durch neue Komponenten ersetzt werden. Damit einhergehend ist auch die Budgethöhe eine häufige Herausforderung – etwa einem Sechstel stehen nicht genügend finanzielle Mittel zur Verfügung. Dabei sollte Verantwortlichen ein ausreichendes Budget für IT-Sicherheit zur Verfügung stehen, um die richtigen Maßnahmen finanzieren zu können. Ein weiteres Problem ist der Mangel an Fachwissen, der sich genauso negativ auf Security auswirkt, wie zu wenig Personal und ein zu knapp bemessener Etat.

Herausfordernd

Größte Herausforderung in der IT-Sicherheit; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die im öffentlichen Dienst arbeiten; 2025; in Prozent

Was halten Sie für die größte Herausforderung, um IT-Sicherheit in Ihrer Verwaltung zu gewährleisten?



22,3	17,5	15,7	11,7	8,7	3,6
zu wenig Personal	veraltete Technik	zu wenig Budget	zu wenig Fachwissen	Zeitmangel	zu wenig externe Unterstützung

Quelle: Statista im Auftrag von G DATA

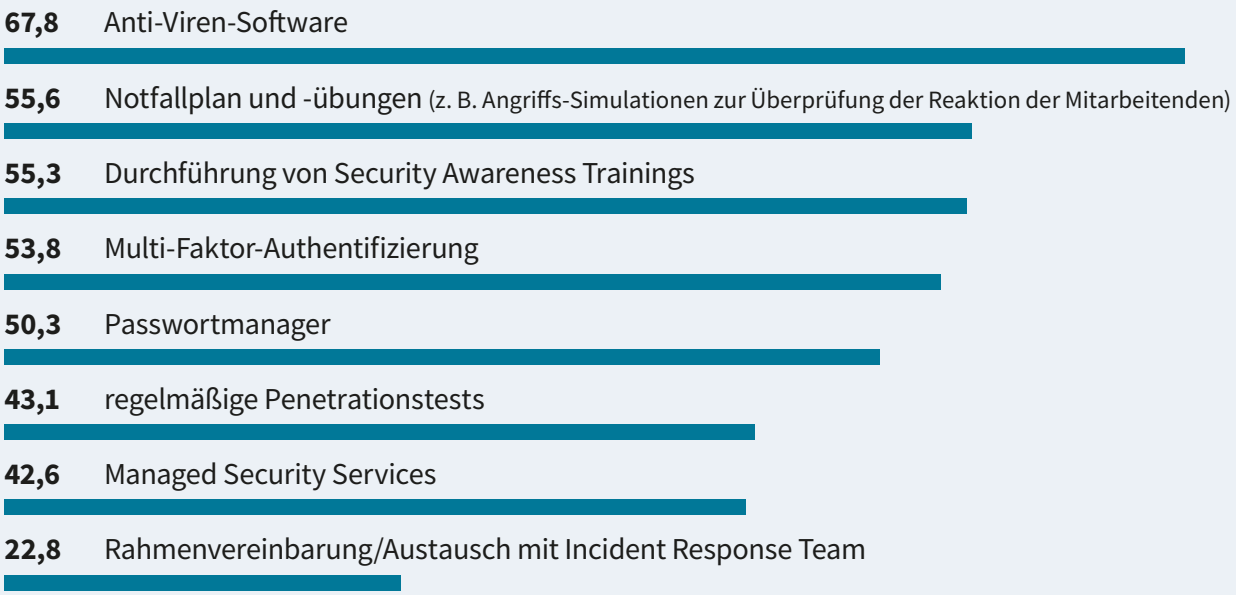
Antiviren-Software ist bei IT-Leitenden die Nummer eins

Ein Blick auf die Maßnahmen zum Schutz vor Cyberangriffen zeigt, dass der klassische Virenschutz bei vielen Verantwortlichen im Bereich IT und IT-Sicherheit immer noch am stärksten verbreitet ist – fast 68 Prozent setzen darauf. Diese Art von Security-Lösung ist heute nur noch eingeschränkt effektiv, da Angreifergruppen vermehrt auf dateilose Attacken setzen. Sie nutzen Schwachstellen in Anwendungen aus oder gelangen durch Phishing an Zugangsdaten für die IT-Systeme. Nötig ist daher eine Rund-um-die-Uhr-Überwachung des Netzwerkes in Verbindung mit der Option, jederzeit auf Vorfälle reagieren zu können. Eine Möglichkeit, dies zu gewährleisten, sind Managed Security Services – ein klassischer Virenschutz leistet dies nicht. Hierauf setzen nur fast 43 Prozent der Befragten, dabei steigert Managed Security, zum Beispiel ein Managed SOC, das Schutzniveau ungemein. Mehr als die Hälfte der IT- und Security-Verantwortlichen bereiten sich aber wenigstens mithilfe von Notfallplänen und -übungen auf den Ernstfall vor.

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

IT-Sicherheit mit externer Expertise

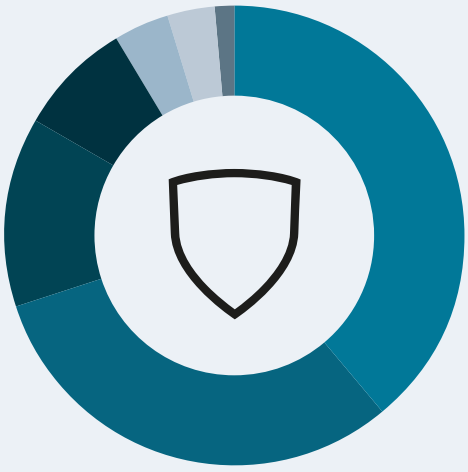
Für die kontinuierliche Überwachung der IT-Infrastruktur setzen vier von fünf Befragten in leitender Position in den Bereichen IT oder IT-Sicherheit (83 Prozent) auf ein internes Team, einen externen Dienstleister oder eine Kombination aus beidem. Fast ein Drittel (31 Prozent) favorisiert die Zusammenarbeit aus eigenen Mitarbeitenden und einem Servicepartner. Hierdurch kombinieren sie die fachliche Expertise sowie Erfahrung mit tiefgreifendem Wissen der Systeme. Fast 40 Prozent der Verantwortlichen lässt die Infrastruktur ausschließlich durch ein internes Team überwachen. Für Kommunen, Landkreise und Verwaltungen ist es im Regelfall nicht möglich, eine kontinuierliche Überwachung in Eigenregie zu gewährleisten, weil der Personalaufwand hoch ist. Benötigt werden mindestens acht Expertinnen und Experten, um den nötigen Schichtbetrieb für eine 24/7-Abdeckung zu betreiben.

In der Praxis ist die Überwachung in Nachtzeiten oder Wochenenden nur eingeschränkt, wenn interne Mitarbeitende dies übernehmen. Oft besteht die Tätigkeit darin, dass ein Teammitglied ein Bereitschaftstelefon verwaltet und vielleicht ab und zu auf die Systeme schaut. Passiert etwas, wird dies nur sehr zeitverzögert bemerkt. Jedoch ist die sofortige Reaktionsmöglichkeit essenziell, um schädliche Vorfälle zu beenden und damit Cyberkriminelle auszubremsen. Nicht immer sind Angriffe auf den ersten Blick zu erkennen, da sie häufig mit scheinbar harmlosen Aktionen starten, zum Beispiel Änderungen bei der Rechteverwaltung für Nutzerinnen und Nutzer. Eine dauerhafte und effektive Überwachung kann oft nur ein erfahrener Dienstleister sicherstellen. Dieser kommt bei 13 Prozent der Teilnehmenden allein zum Einsatz. Andere IT- oder Security-Verantwortliche setzen nur auf eine zeitweise externe Unterstützung. Dies ist aber oft ungeeignet und sorgt für keine effektive Abwehr von Cyberangriffen, wenn keine 24/7-Abdeckung stattfindet.

Gut bewacht

Kontinuierliche Überwachung von IT-Systemen; 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; 2025; in Prozent

Werden Ihre IT-Systeme kontinuierlich (24/7) von internen oder externen Sicherheitsexperten auf Angriffe bzw.deren Anzeichen überwacht?



39,0 %	ja, durch ein internes Team
31,0 %	ja, durch eine Kombination aus internem und externem Dienstleister
13,3 %	ja, durch einen externen Dienstleister
8,0 %	nein, nur zeitweise durch ein internes Team
4,1 %	nein, nur zeitweise durch einen externen Dienstleister
3,3 %	nein, nur zeitweise aus einer Kombination aus internem Team und externem Diensleister
1,2 %	nein, die weden gar nicht überwacht

Quelle: Statista im Auftrag von G DATA

„Digitale Resilienz ist kein Ziel, sondern ein Weg“

Ein Gespräch mit Thomas Rüby, IT-Leiter im Landratsamt Dachau, über IT-Sicherheit, Souveränität und realistische Wege zur Cyberresilienz im öffentlichen Sektor.

Herr Rüby, was sind derzeit die größten Herausforderungen für Kommunen bei der IT-Sicherheit? Und wie erleben Sie die aktuelle Bedrohungslage?

Thomas Rüby: *„Die größte Herausforderung ist die Breite des Aufgabenfeldes bei gleichzeitiger Ressourcenknappheit. Wir sind als IT-Team im Landratsamt Dachau für über 400 unterschiedliche IT-Services zuständig – von der Ausländerbehörde bis zum Veterinäramt. Dazu kommen über 750 mobile Arbeitsplätze, zwei kleine Rechenzentren und viele Fachverfahren. Unser Team besteht aus zwölf Personen, das bedeutet: Wir sind Generalisten, keine IT-Security-Spezialisten.*

Die Bedrohungslage hat sich aus unserer Sicht spürbar verschärft. Früher lief der Virenschutz „nebenbei”. Heute wissen wir: IT-Sicherheit ist ein eigenständiges Fachgebiet, das man nicht nebenher schafft. Die Angriffe sind gezielter, raffinierter, persistenter. Gleichzeitig ist die Erwartungshaltung an uns als Behörde hoch: Die Verwaltung soll digitaler werden – aber bitte auch absolut ausfallsicher und krisenfest. Dieses Spannungsfeld prägt unseren Alltag.“

Welche Auswirkungen hätte ein erfolgreicher Cyberangriff auf Ihre IT-Systeme?

Thomas Rüby: *„Ein Angriff ist mehr als ein technischer Zwischenfall – er hätte direkte Auswirkungen auf das Leben der Menschen in unserem Landkreis. Ob Führerschein, Ausländerwesen oder Sozialleistungen: Wenn unsere IT ausfällt, steht die Verwaltung und damit ist der Staat auf Landkreisebene deutlich eingeschränkt.*

Vorfälle wie im Landkreis Anhalt-Bitterfeld oder in der Stadt Witten haben uns vor Augen geführt: Wenn tagelang nichts mehr geht, leidet nicht nur der Service. Es schadet auch dem Vertrauen in die Verwaltung – und damit in die Demokratie insgesamt. Genau deshalb ist digitale Resilienz für uns kein abstrakter Begriff, sondern eine tägliche Aufgabe.“

Digitale Souveränität ist ein viel diskutiertes Thema. Welche Rolle spielt sie in Ihrem IT-Sicherheitskonzept?

Thomas Rüby: *„Eine sehr konkrete Rolle. Wir haben uns bewusst für einen deutschen Anbieter mit Rechenzentren in Deutschland entschieden. Nicht, weil wir dogmatisch wären – sondern weil wir technische Unabhängigkeit als strategisches Ziel sehen. Die geopolitische Lage zeigt: Man sollte wissen, mit wem man in der Krise reden kann. Wir brauchen Partner, die greifbar sind – im Zweifel auch auf Deutsch, ohne Callcenter in Übersee.*

Außerdem gilt: Wenn öffentliche Verwaltungen digitale Souveränität nicht einfordern – wer dann? Wir sind mit Steuergeld finanziert. Es ist unsere Verantwortung, diese Mittel klug, nachhaltig und rechtssicher einzusetzen.“

Sie sprechen den deutschsprachigen Support an. Ist das im Ernstfall ein entscheidendes Kriterium?

Thomas Rüby: *„Unbedingt. Im Ernstfall zählt jede Minute und jedes Missverständnis kann teuer werden. IT-Fachjargon in Stresssituationen in einer Fremdsprache zu klären, ist kein theoretisches Risiko, sondern gelebte Realität. Deshalb war für uns klar: Wir wollen rund um die Uhr einen deutschsprachigen Service mit Menschen, die unsere Infrastruktur verstehen.“*

Was würden Sie Kolleginnen und Kollegen in anderen Kommunalverwaltungen mit auf den Weg geben?

Thomas Rüby: *„Drei Dinge. Erstens: IT-Sicherheit darf nicht „nebenbei“ laufen. Wer immer nur reagiert, verliert irgendwann den Überblick. Deshalb setzen wir auf Managed Extended Detection and Response von G DATA. Und damit auf einen Dienstleister mit Erfahrung, der uns entlastet und unser Sicherheitsniveau hebt.*

Zweitens: Souveränität entsteht durch Zusammenarbeit. Ob mit einem Hersteller, mit Landesbehörden oder mit anderen kommunalen Organisationen – wir müssen voneinander lernen und gemeinsam Standards schaffen. Denn: Jeder Angriff auf eine Kommune ist auch ein Angriff auf das Vertrauen in die öffentliche Hand.

Und noch ein dritter Punkt: Digitalisierung ist kein Sprint, sondern ein Marathon. Digitale Resilienz ist kein Ziel, das man einmal erreicht – sondern ein Weg, den man konsequent gehen muss. Mit Verstand, mit Partnern und mit einem klaren Blick auf das, was wirklich zählt.“

Fachwissen, KI und Digitale Souveränität als Erfolgsfaktoren für IT-Sicherheit

Verwaltungen kommen im Regelfall nicht ohne externe Dienstleister aus, um eine effektive Cyberabwehr sicherzustellen. Die Zusammenarbeit bringt Städten, Landkreisen und anderen kommunalen Organisationen viele Vorteile. Die Mehrheit der Befragten (fast 47 Prozent) sieht in der Kooperation mit Dienstleistern die Möglichkeit, ein höheres Sicherheitsniveau zu erreichen. Oft bringt ein Servicepartner erst das nötige Fachwissen mit ein, über das kommunale IT-Teams ansonsten nicht verfügen – zwei von fünf Arbeitnehmenden im öffentlichen Dienst vertreten diese Ansicht. Dabei sind gerade das Know-how und die Erfahrung wichtige Faktoren für die Erkennung und Einschätzung von Cyberangriffen – und als Folge die passende Reaktion darauf. 35 Prozent der Studienteilnehmenden sehen den Faktor Zeitersparnis als Vorteil in der Zusammenarbeit mit einem Dienstleister. Gerade durch den bereits dargestellten Fachkräftemängel sind die zeitlichen Ressourcen für die oft umfangreichen Aufgaben in IT-Teams knapp.

Die Mitarbeitenden sind oft für den Betrieb einer Vielzahl von IT-Diensten zuständig. Ein Viertel sieht sich durch externe Security-Expertinnen und -Experten zudem bei der Einhaltung von gesetzlichen Vorschriften unterstützt.

Idealerweise hat der Dienstleister seinen Hauptsitz in Deutschland und bietet Kommunikation in deutscher Sprache an. Dies ist gerade in Krisenzeiten ein sehr großer Vorteil: Läuft gerade eine Cyberattacke und das mitten in der Nacht, ist eine einfache Kommunikation unabdingbar. Diese funktioniert für deutsche Mitarbeitende am besten in der eigenen Muttersprache, weil in dieser Situation alles Wichtige schnell besprochen werden muss. Partner stellen Kommunen zudem feste Ansprechpartner zur Seite, die ihre Kunden gut kennen und gut bei der Arbeit unterstützen können. Das schafft Vertrauen und ist die Grundlage einer guten IT-Sicherheit.

Mehr Professionalität, mehr Wissen, mehr Zeit

Vorteile durch den Einsatz von externen IT-Sicherheits-Fachleuten; Arbeitnehmerinnen und Arbeitnehmer in Deutschland, die im öffentlichen Dienst arbeiten; 2025; in Prozent *

Worin würden Sie Vorteile sehen, wenn IT-Sicherheit teilweise durch externe Fachleute unterstützt wird?

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

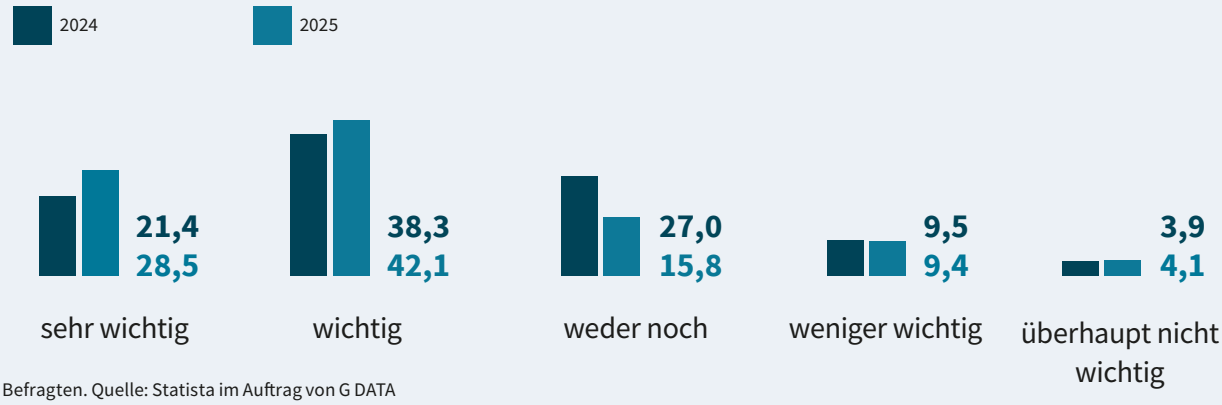
Augen auf bei der Anbieterwahl

Wenn sich Verantwortliche für ein Managed Security Operations Center entscheiden, geht es nicht um die passende Lösung auf Basis von technischen Eigenschaften. Essenziell ist dabei auch der Faktor Digitale Souveränität – und damit die Frage, wo der Anbieter den Unternehmenssitz hat. Das ist sieben von zehn Verantwortlichen wichtig oder sogar sehr wichtig. Im Vergleich zum Vorjahr hat der Wert 2025 um zehn Prozentpunkte zugenommen. Das zeigt, dass die Bedeutung steigt, denn es geht bei dieser Frage darum, welche gesetzliche Grundlage bei der Zusammenarbeit gilt. Die europäischen und deutschen Datenschutzgesetze sind weitaus strenger als beispielsweise die US-amerikanischen. Zudem ist die geopolitische Lage in den USA derzeit äußerst schwierig, was sich natürlich auch auf die Zusammenarbeit mit US-Anbietern auswirkt. Sie bieten durch die Entscheidungen im Weißen Haus keinen verlässlichen Service mehr an, was in diesem Fall zu einer erheblichen Minderung des Schutzniveaus führt. Zudem ist die US-Regierung grundsätzlich in der Lage, Daten mitzulesen und so auch an vertrauliche Informationen zu gelangen. In den USA wird grundsätzlich sogar darüber nachgedacht, den Datenschutz auszuhebeln – dies ist in Deutschland undenkbar.

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

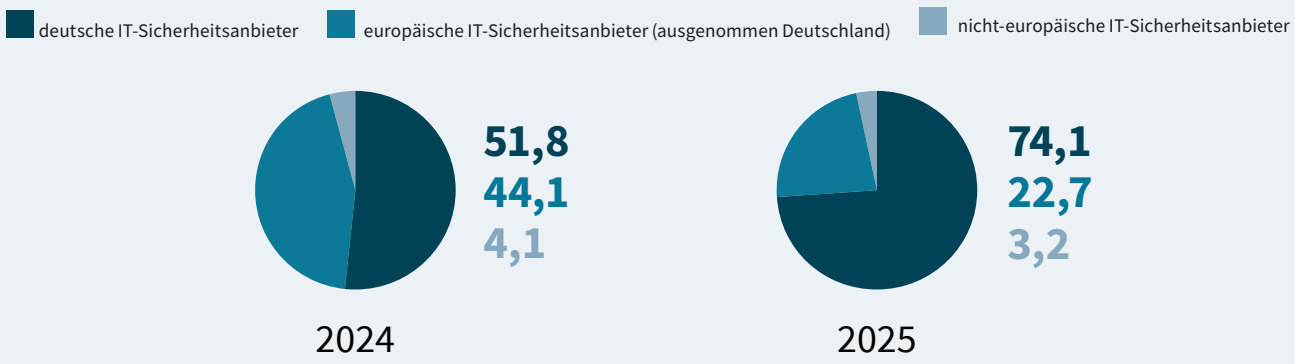
Drei Viertel der IT- oder IT-Sicherheits-Verantwortlichen bevorzugen einen deutschen Security-Anbieter. Der Anteil stieg innerhalb eines Jahres massiv - um mehr als zwanzig Prozent. Das Ergebnis unterstreicht abermals die große Bedeutung der Digitalen Souveränität und zeigt, dass deutsche IT-Sicherheit ein sehr hohes Vertrauen genießt. Bei einem Managed SOC ist dieser Aspekt sehr wichtig, denn Leitende vertrauen ihre Sicherheit einem Dienstleister an. Dazu erhält der Anbieter eine detaillierte Einsicht in die IT-Systeme seines Kunden. Bei deutschen Dienstleistern gilt dabei das Gebot der Datensparsamkeit, das bedeutet: Es werden nur die Daten eingesehen, die für die Arbeit unerlässlich sind. Alle weiteren bleiben unangetastet. Dies ist bei US-Anbietern nicht gewährleistet. Zudem bieten deutsche Dienstleister einen deutschsprachigen Kundenservice an. Hierdurch werden Verständigungsprobleme vermieden. Dies ist gerade in einer Notfallsituation wie einem aktuellen Cyberangriff von großem Vorteil.

Für Städte und kommunale Einrichtungen ist es entscheidend, in eine heimische IT-Sicherheitsinfrastruktur mit deutschen Komponenten und Dienstleistern zu investieren. Sie bleiben so unabhängig von gravierenden politischen Entscheidungen und können sich auf eine verlässliche Gesetzgebung mit einem starken Datenschutz und hohen Sicherheitsstandards verlassen. Eine Investition in die heimische IT-Wirtschaft ist daher ein wichtiger und nötiger Schritt.

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

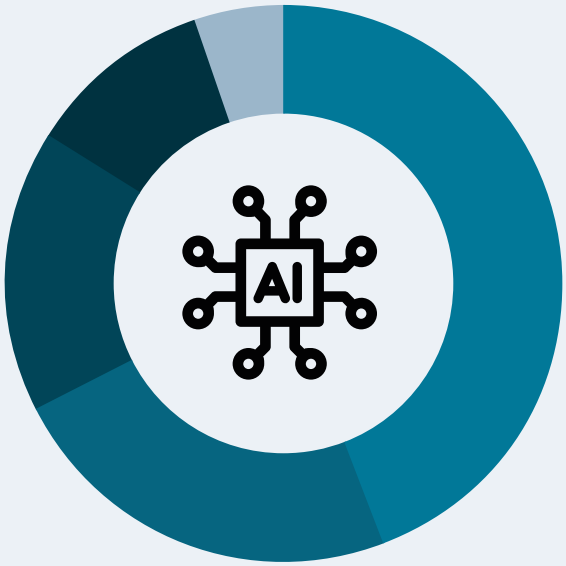
KI und Mensch als Sicherheitsduo

Künstliche Intelligenz spielt nicht nur bei Cyberkriminellen, sondern auch bei der Cyberabwehr eine große Rolle, zum Beispiel bei KI-basierten Security-Technologien. 45 Prozent der Befragten sehen die Vorteile von KI insbesondere in Kombination mit IT-Sicherheitsfachleuten und fühlen sich so gut geschützt. In der Praxis wird ein Managed-SOC-Analystenteam durch Künstliche Intelligenz ideal unterstützt. In den Analysesystemen läuft oft eine Fülle von Informationen und Meldungen auf. KI-gestützte Systeme sortieren die Daten vor, clustern diese und erleichtern die Prüfung der Vorgänge. Die Flut an Informationen wäre für die Analystinnen und Analysten, ohne die Hilfe von Künstlicher Intelligenz nur schwer zu bewältigen. Weniger als ein Viertel der Mitarbeitenden fühlt sich eher durch IT-Sicherheitsexperten, also durch Menschen, besser vor Cybergefahren geschützt. Auf KI setzen dagegen 16 Prozent.

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

Ihr Managed SOC aus Deutschland – für mehr **digitale Souveränität**

Als IT-Verantwortliche im öffentlichen Sektor stehen Sie vor großen Herausforderungen bei der Stärkung der IT-Sicherheit. Mit dem Managed SOC des deutschen IT-Sicherheitsspezialisten G DATA lösen Sie die Probleme des Personalmangels, der fehlenden fachlichen Expertise und den Ressourcenmangel. G DATA 365 | Managed Extended Detection and Response ermöglicht Ihrem IT-Team, sich vollkommen auf seine Kernaufgaben zu 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. Mit dem Managed SOC 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 KI-gestützten Technologien selbst entwickelt – komplett in Deutschland. 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 Ihren eigenen 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 Partner aus Deutschland

Durch G DATA 365 | MXDR profitieren IT-Verantwortliche im öffentlichen Sektor von der **umfangreichen Expertise** des deutschen Cyber-Defense-Spezialisten. Ihnen stehen **persönliche Ansprechpartner** zur Seite und Sie werden unterstützt von einem **preisgekrönten 24/7-Support in deutscher Sprache**. Ihre Ansprechpartner nehmen sich immer Zeit für Sie – und zwar die Zeit, die es braucht.

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 Reaktion erfolgen soll. Das Onboarding führt G DATA entweder allein oder gemeinsam mit einem **Systemhaus** durch. Wir sehen Daten nur in Verdachtsfällen ein und nur, soweit Sie es uns beim Onboarding gestatten. Die Datenverarbeitung erfolgt ausschließlich auf **Servern in Deutschland**. Damit unterliegen die Informationen den strengen **deutschen Datenschutzrichtlinien**.

Das Managed SOC von G DATA ist somit ideal für alle, die ihre IT-Sicherheit und gleichzeitig ihre digitale Souveränität stärken wollen.

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