Cybersicherheit

Hoher Handlungsdruck

[12.11.2025] Die aktuelle Studie „Cybersicherheit in Zahlen“ von G DATA CyberDefense zeigt: Veraltete IT, Fachkräftemangel und zu geringe Budgets bremsen die Sicherheitsvorkehrungen aus. Kommunen müssen jetzt handeln und ihr Schutzniveau erhöhen.

Kommunale IT-Infrastrukturen stehen zunehmend im Fokus von Cyberkriminellen. Im Rahmen der Studie Cybersicherheit in Zahlen haben das IT-Sicherheitsunternehmen G DATA CyberDefense, Statista und brand eins über 300 Beschäftigte im öffentlichen Dienst zu ihrer Einschätzung befragt.

Trotz steigender Bedrohung stuft rund die Hälfte aller Befragten das Risiko eines Cyberangriffs als gering oder sehr gering ein. Besonders auffällig: Beschäftigte im öffentlichen Dienst zeigen die geringste Sensibilität angesichts der Gefahrenlage – 59 Prozent der kommunalen Mitarbeitenden sehen in Cyberattacken eine niedrige beziehungsweise sehr niedrige Gefahr. Zum Vergleich: Im Bereich Telekommunikation und Information sind es nur zwei von fünf Befragten, die das Angriffsrisiko für ihr Unternehmen als niedrig einschätzen. Das ist problematisch, denn jede Verwaltungseinheit, jede Behörde und jede einzelne Person kann zum Ziel werden.

Cybervorfälle sind keine Ausnahme

Es bedarf also einer Sensibilisierung der Mitarbeitenden, etwa durch Security Awareness Trainings oder Phishing-Simulationen. Ohne ein grundlegendes Verständnis für digitale Risiken lassen sich weder Strategien noch Sicherheitsmaßnahmen wirksam umsetzen. Hinzu kommt, dass Cyberkriminelle verstärkt auf Künstliche Intelligenz setzen.

Dass Cybervorfälle zum Alltag gehören und keine Ausnahme sind, unterstreicht folgende Zahl: Fast jede zweite Person berichtet, dass sie selbst oder jemand aus ihrem Kollegenkreis bereits von einem Angriff betroffen gewesen sei. Mit oft dramatischen Folgen: Kommt es zu schwerwiegenden Vorfällen, bei denen Angriffe nicht rechtzeitig erkannt oder eingedämmt werden, stehen Dienste über Wochen oder gar Monate still. Bürgerservices sind dann nur eingeschränkt arbeitsfähig und Wohngeldzahlungen oder Unterhaltsvorschüsse können nicht bearbeitet werden.

Herausforderung IT-Sicherheit

Ein zentrales Problem liegt im Zustand der IT-Infrastruktur vieler Kommunen: Nur 43 Prozent der Befragten halten die eigenen Systeme für modern und gut gepflegt. Jeder Fünfte sieht große Unterschiede je nach Bereich. Und rund 15 Prozent bezeichnen die Technik als veraltet, wenn auch funktional. Fünf Prozent der befragten Verwaltungsangestellten sprechen sogar von überholten und schwer wartbaren IT-Systemen. Gerade ältere Systeme mit bekannten Schwachstellen bieten Angriffsflächen – insbesondere, wenn Updates fehlen. Schließlich suchen Angreifergruppen gezielt nach veralteten und ungepatchten Systemen. Kommunale IT-Abteilungen stehen dabei oft vor einer komplexen Aufgabe: Heterogene Strukturen, knappe Ressourcen und ein hoher Zeitdruck erschweren eine nachhaltige IT-Strategie.

Auf dem Weg zu mehr IT-Sicherheit müssen Verantwortliche gleich mehrere Herausforderungen lösen. 22 Prozent der Befragten sehen im Fachkräftemangel die größte Hürde für mehr IT-Sicherheit. Gleich danach folgt veraltete Technik (17,5 Prozent). Auch finanzielle Mittel fehlen vielerorts: 15 Prozent nennen das begrenzte Budget als Haupthindernis. Dabei erfordert eine sichere IT-Landschaft mehr als moderne Hardware. Zusätzlich müssen Software und Betriebssysteme kontinuierlich aktualisiert werden. Weitere Probleme sind fehlendes Fachwissen sowie Zeitmangel innerhalb der Verwaltung. Ein Mangel an Zeit wirkt sich ähnlich negativ aus wie der Personalmangel oder ein zu knapp kalkulierter Etat.

Externe Partner können helfen

Immer mehr Kommunen setzen auf externe Dienstleister, um ihre Systeme abzusichern. Dieser Schritt bietet viele Vorteile. 47 Prozent der Befragten sehen in der Zusammenarbeit ein höheres Sicherheitsniveau durch professionelle Lösungen. Zwei von fünf Angestellten schätzen das Fachwissen externer Partner, das intern oft fehlt. Zeitersparnis für interne Teams spielt ebenfalls eine große Rolle. Das sehen angesichts knapper Personalressourcen 35 Prozent der Verwaltungsangestellten als Pluspunkt. Ein Viertel der Befragten fühlt sich durch externe Unterstützung zudem besser aufgestellt, um gesetzliche Anforderungen wie die Datenschutz-Grundverordnung (DSGVO) zu erfüllen.

Die Studienergebnisse machen deutlich: Kommunen müssen beim Thema IT-Sicherheit nachsteuern. Der Handlungsdruck ist hoch und die Bedrohungslage macht schnelles Handeln erforderlich. Externe Dienstleister können helfen, das Sicherheitsniveau zu erhöhen, ohne dass intern zusätzliche Ressourcen aufgebaut werden müssen. Die Verantwortlichen vor Ort sollten das Thema nicht länger aufschieben.

()

Dieser Beitrag ist in der Ausgabe November 2025 von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Cybersicherheit, G DATA CyberDefense