Cyber-Sicherheit

Kommunen sind leichte Beute

[12.05.2026] Wie Städte und Kreise ihre IT trotz Fachkräftemangel wirksam vor Cyber-Kriminellen schützen können, erläutern im Interview Kira Groß-Bölting und Jan Leitzgen vom Computer Security Incident Response Team (CSIRT) des Unternehmens G DATA Advanced Analytics.

Frau Groß-Bölting, Herr Leitzgen, stehen Kommunen mittlerweile besonders im Fokus von Cyber-Kriminellen?

Kira Groß-Bölting: Kommunen sind eine leichte Beute für Cyber-Kriminelle. Ihre IT ist häufig schwach abgesichert. Ransomware-Gruppen gehen opportunistisch vor und greifen da an, wo es am leichtesten ist. Empathie oder Schonung für öffentliche Einrichtungen sehen wir kaum noch.

Warum erkennen viele kommunale IT-Verantwortliche zu spät, dass ein Cyber-Angriff erfolgt?

Jan Leitzgen: Es fehlt an grundlegenden Sicherheitsmaßnahmen: klare Prozesse, Notfallpläne oder Security Awareness unter Mitarbeitenden. Viele Verwaltungen haben zudem kein durchgängiges Logging- und Monitoring-Konzept. Ereignisse werden nur punktuell geloggt und wichtige Event-IDs fehlen. Damit sind frühe Warnzeichen deutlich schwerer zu erkennen. Hinzu kommen schlechte Meldewege. Die Mitarbeitenden wissen im Zweifel nicht, was zu tun ist, wenn sie zum Beispiel auf eine Phishing-Mail hereingefallen sind.

Groß-Bölting: Viele IT-Teams sind außerdem dünn besetzt, und Kommunen mit einem IT-Leiter und einem Auszubildenden leider immer noch der Normalfall. Bei so wenig Personal reicht es nur für das Nötigste im Tagesgeschäft. Wichtige Themen wie Prävention, Awareness Trainings und saubere Prozesse fallen oft unter den Tisch.

Was sind typische Angriffsmuster?

Leitzgen: Klassische Einfallstore sind schwache Passwörter, nicht gepatchte Systeme sowie eine fehlende Zwei-Faktor-Authentifizierung bei VPN-Zugängen. Ein weiteres, sehr verbreitetes Sicherheitsrisiko: 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.

Groß-Bölting: Wir begegnen immer wieder sehr laschen Passwort-Richtlinien. Ein Beispiel: Wird mehrfach versucht, sich mit einem fehlerhaften Passwort anzumelden, erfolgt nach Zeit X die automatische Entsperrung. Mit der Begründung: Damit der Helpdesk weniger Tickets hat. Das ist faktisch eine Einladung für Angreifergruppen.

Welche Fallstricke können bei der Aufarbeitung eines erfolgreichen Angriffs aufkommen?

Leitzgen: Ohne Notfallkonzepte dauert schon die Aufklärung über die aktuelle Lage lange. Zusätzlich bricht die Kommunikation zwischen Außenstellen weg und die IT kämpft parallel mit Krisenkommunikation, Forensik und Wiederaufbau.

Groß-Bölting: Viele unterschätzen die bestehenden Abhängigkeiten. Erst ein Cyber-Sicherheitsvorfall zeigt, welche Dienste miteinander verknüpft sind – vom Identitäts- und Zugriffsmanagement bis hin zu den Fachverfahren. Wer seine Kritikalitäten nicht vorher bewertet hat, muss unter Stress priorisieren und verliert dabei wertvolle Zeit.

Welche Auswirkungen hat das auf Verwaltung und Bürger?

Leitzgen: Haben Cyber-Kriminelle Daten und Systeme verschlüsselt, kommt der Geschäftsbetrieb zum Erliegen. Bürgerbüros, Ausweisstellen, Kfz-Zulassungen – nichts funktioniert mehr. Sozialleistungen werden nicht ausgezahlt und die Kommunikation zwischen Fachbereichen bricht ab. Was analog abfangbar ist, hängt vom Reifegrad der Vorbereitung ab.

Groß-Bölting: Die ersten Stunden sind besonders wichtig, um einen Notbetrieb vorzubereiten. Dafür muss aber definiert sein, welche Systeme priorisiert benötigt werden. Besonders kritisch ist es, wenn keine klare Kommunikationsstrategie existiert. Ohne einen Notfallplan geraten viele Verwaltungen in einen Panikmodus.

„Wir begegnen immer wieder sehr laschen Passwort-Richtlinien."

Wie lange dauert es Ihrer Erfahrung nach, bis eine betroffene Kommune wieder arbeitsfähig ist?

Groß-Bölting: Bis sukzessive ein stabiler Notbetrieb steht, vergehen in der Regel vier bis sechs Wochen. Erst dann ist wieder eine geregelte Kommunikation möglich und wichtige Verwaltungsleistungen sind wieder abrufbar. Nach sechs bis neun Monaten schaffen es Kommunen mit externer Unterstützung, den Normalbetrieb wiederherzustellen. Dann sind zentrale Projekte umgesetzt und der Notbetrieb abgelöst. Das ist aus unserer Sicht aber noch lange kein Endzustand, sondern eine spürbar gehärtete Basis, auf die weiter aufgebaut werden muss.

Leitzgen: Normalbetrieb heißt also nicht: Alles ist jetzt sicher. Es bedeutet, dass die ausgenutzten Schwachstellen geschlossen wurden – meist mit überschaubaren Ressourcen. Eine langfristige Steigerung des IT-Sicherheitsniveaus erfordert jedoch mehr Budget, mehr Zeit und vor allem mehr Personal. Und genau daran hapert es leider.

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

Leitzgen: Erstens: Sichtbarkeit schaffen. Ohne Monitoring bleiben verdächtige Aktivitäten unsichtbar. Tools wie XDR (Extended Detection and Response) oder ein Security Operation Center (SOC) 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. Das 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.

Groß-Bölting: Kommunen sollten Passwort-Richtlinien mit Vorgaben der Länge und Komplexität verbindlich einführen und privilegierte Konten besonders schützen. Jeder Log-in sollte einer bestimmten Person zugeordnet sein – so bleiben Änderungen nachvollziehbar. Zudem sollten externe Zugänge mit einem automatischen Lock-out versehen sein, der die Anmeldung nach einer definierten Anzahl von

Fehlversuchen für eine gewisse Zeit blockiert. Das sind günstige, sofort wirksame Stellschrauben.

Leitzgen: Mein Rat: Kommunen sollten sich Hilfe holen und mit dem Machbaren anfangen. Das wichtigste ist, den ersten Schritt zu gehen. Wer seine größten Schwachstellen kennt und einen Plan hat, bewegt sich vom reaktiven Krisenmodus hin zur souveränen Sicherheitskultur.

()

Dieses Interview ist in der Ausgabe Mai 2026 von Kommune21 im Schwerpunkt Cyber-Sicherheit erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, G Data, Cyber-Abwehr, Cyber-Sicherheit