Interview

Schwachstellen aufdecken

[16.11.2026] Das bayerische Landesamts für Sicherheit in der Informationstechnik (LSI) unterstützt Kommunen beim Thema Cyber-Sicherheit. LSI-Präsident Bernd Geisler spricht über das Angebot und berichtet über eine IT-Notfallübung mit der Stadt Ingolstadt.

Herr Geisler, Cyber-Angriffe auf öffentliche Verwaltungen sind längst keine Ausnahme mehr. Wie schätzen Sie die aktuelle Bedrohungslage für bayerische Kommunen ein? Welche Angriffsszenarien bereiten Ihnen derzeit die größten Sorgen?

Wie andere Sicherheitsbehörden auch, stellt das LSI eine ständig wachsende Bedrohungslage fest. Es finden täglich Angriffsversuche statt, die sich in Ihrem Schweregrad unterscheiden. Die Anzahl der Angriffe sowie deren Komplexität steigt kontinuierlich. Diese Entwicklung hat sich mit dem Einsatz von KI nochmals deutlich verstärkt. Die am häufigsten festgestellten Einfallstore sind E-Mails mit schadhaftem Inhalt, über das Internet erreichbare, nicht aktualisierte Systeme mit Schwachstellen, fehlende Multi-Faktor-Authentifizierung und abgeflossene Benutzerdaten.

Das LSI unterstützt Kommunen mit verschiedenen Beratungs- und Präventionsangeboten. Was können konkret in Anspruch nehmen?

Das LSI bietet präventive Unterstützungsleistungen auch für Kommunen an, darunter den Warn- und Informationsdienst, eine Malware Information Sharing Plattform, Handreichungen zum Notfallmanagement, das Siegel „Kommunale IT-Sicherheit“, Awarenessmaßnahmen, wie zum Beispiel Phishing-Simulationen, die Möglichkeit von Sicherheitsübungen sowie regelmäßige regionale Thementage. Ergänzend hierzu veröffentlicht das LSI praxisnahe Leitfäden, etwa zur Abwehr von DDoS-Angriffen, und baut sein Unterstützungsangebot fortlaufend aus, um den aktuellen technischen und organisatorischen Herausforderungen gerecht zu werden. Die Nachfrage nach diesen Angeboten ist anhaltend hoch und reicht teilweise über die Landesgrenzen hinaus – eine Wertschätzung der Expertise des LSI, die uns freut.

Ende September hat das LSI gemeinsam mit der Stadt Ingolstadt eine umfassende IT-Notfallübung durchgeführt (wir berichteten). Welche Ziele haben Sie damit verfolgt?

Die Übung mit der Stadt Ingolstadt war besonders umfangreich und für das LSI auch die erste Übung in dieser Größenordnung mit einer kreisfreien Stadt. Die Übung gliederte sich in zwei aufeinander abgestimmte Formate: ein moderiertes Tabletop-Szenario und eine technische Praxiseinheit. Während Führungskräfte und Verantwortliche verschiedener Organisationseinheiten im Tabletop-Format konkrete Entscheidungssituationen bewerteten und notwendige Maßnahmen abstimmten, wurden parallel technische Prozesse und Reaktionsmöglichkeiten unter möglichst realistischen Bedingungen erprobt.

> **Es finden täglich Angriffsversuche statt, die sich in Ihrem Schweregrad unterscheiden.**

Warum ist es so wichtig, bei der IT-Notfallvorsorge nicht nur die Technik, sondern auch die organisatorischen Abläufe und Entscheidungsstrukturen zu überprüfen?

Durch die Kombination beider Übungsbestandteile entsteht ein umfassendes Bild der bestehenden IT-Notfallstrukturen. Notfallpläne, Entscheidungswege und technische Abläufe konnten unter realitätsnahen Voraussetzungen erprobt werden. Gleichzeitig werden bereits gut funktionierende Strukturen bestätigt und weitere Optimierungspotenziale identifiziert. Die gewonnenen Erkenntnisse bilden damit eine wichtige Grundlage für die kontinuierliche Weiterentwicklung der Notfallvorsorge.

Um möglichst realistische Bedingungen zu schaffen, wurde in Ingolstadt nur ein kleiner Kreis vorab über die Übung informiert. Welche Erkenntnisse haben Sie dabei gewonnen?

Ein besonderer Schwerpunkt lag auf der praxisnahen Gestaltung des technischen Übungsteils. Der Kreis der vorab informierten Personen wurde bewusst klein gehalten, um ein möglichst authentisches Lagebild zu erzeugen. Dadurch konnte nicht nur die technische Bewältigung einer simulierten IT-Störung untersucht werden, sondern unter realitätsnahen Bedingungen auch die internen Informations- und Kommunikationswege, die Zusammenarbeit zwischen den beteiligten Bereichen sowie das Zusammenspiel von Verwaltung und IT-Fachkräften.

Bei solchen Übungen geht es ausdrücklich auch darum, Schwachstellen aufzudecken. Welche typischen Probleme treten bei kommunalen IT-Notfalltests zutage?

Die Gegebenheiten sind von Kommune zu Kommunen sehr unterschiedlich und damit auch die möglichen Erkenntnisse. Daher ist es wichtig, dass jede Kommune solche umfangreichen Tests oder die Tabletop-Übungen des LSI selbst durchführt, um die eigenen Verbesserungspotentiale zu ermitteln. Wichtig ist uns dabei, dass Übungen nicht als reines Thema des IT-Betriebs wahrgenommen werden. Es sollten explizit auch andere Bereiche bei den Übungen mit angesprochen werden, da in einem echten Notfall auch Führungskräfte und Mitarbeiter aus anderen Fachbereichen involviert sind. Das LSI bietet hierfür Handreichungen mit diversen Dokumenten zum IT-Notfallmanagement.

Ein Notfallplan auf dem Papier ist das eine, seine Umsetzung unter Zeitdruck das andere. Wie häufig sollten Kommunen den Ernstfall proben?

Die IT-Infrastruktur ändert sich schnell, Personal wechselt und Organisationsstrukturen ändern sich. Eine Übung pro Jahr ist daher sicher ein guter Richtwert. Die daraus gewonnen Erkenntnisse sollten in das IT-Notfallmanagement und in eine Fortschreibung des eigenen Informationssicherheitskonzepts einfließen, um zu gewährleisten, dass sie auch in den jeweiligen Prozessen ankommen.

Wichtig ist es, sich laufend über Schwachstellen in Software zu informieren.

Wie läuft Zusammenarbeit zwischen einer Kommune und dem LSI konkret ab?

Die Tabletop-Übungen des LSI sind so konzipiert, dass sie auch von kleinen Kommunen verwendet und selbst durchgeführt werden können. Es besteht aber grundsätzlich die Möglichkeit, dass das LSI die Moderation übernimmt und bei der Auswertung unterstützt. Natürlich stehen wir für alle Fragen beratend zur Verfügung. Der Aufwand für so eine Übung ist bewusst überschaubar gehalten und beträgt etwa 1,5 bis 2 Stunden. Bei einem umfassenden Übungsvorhaben wie in Ingolstadt ist dies natürlich aufwändiger.

Wenn Sie einem Bürgermeister oder einer Landrätin drei Maßnahmen empfehlen könnten, mit denen sich die Widerstandsfähigkeit der Verwaltung gegenüber Cyber-Angriffen verbessern lässt: Welche wären das?

Wichtig ist es, sich laufend über Schwachstellen in Software zu informieren. In Bayern steht dafür der kostenfreie Warn- und Informationsdienst des LSI zur Verfügung, der über aktuelle Angriffe und Sicherheitslücken informiert. Entscheidend ist, entsprechende Updates zeitnah einzuspielen. Ebenso sollten alle aus dem Internet erreichbaren Systeme im Blick behalten werden. Bayerische Kommunen können dem LSI ihre öffentlichen IP-Adressen melden, die dann in das Monitoring aufgenommen werden. So kann das LSI noch schneller und gezielter über Gefährdungen informieren. Ein weiterer wichtiger Baustein ist die regelmäßige Schulung und Sensibilisierung aller Mitarbeitenden, einschließlich der Führungskräfte, für digitale Bedrohungen und den sicheren Umgang damit. Für den Fall eines erfolgreichen Cyberangriffs sollte zudem stets ein Backup verfügbar sein, auf das Angreifer keinen Zugriff haben und das sich zuverlässig wieder einspielen lässt.

()

Das Interview erscheint in der Dezemberausgabe von Kommune21. Hier können Sie ein Einzelheft bestellen oder ein Abonnement abschließen

Stichwörter: IT-Sicherheit, Bayern, Cybersicherheit, Ingolstadt, Landesamt für Sicherheit in der Informationstechnik (LSI)