BSI-Lagebericht 2026

Kommunen sind besonders verwundbar

[20.11.2026] Die Bedrohung durch Cyber-Angriffe nimmt weiter zu. Das Bundesamt für Sicherheit in der Informationstechnik stuft die Lage in Deutschland inzwischen als „angespannt bis kritisch“ ein. Besonders gefährdet sind nach Einschätzung der Behörde weiterhin Städte, Gemeinden und kleinere Unternehmen.

Die Digitalisierung der öffentlichen Verwaltung schafft neue Möglichkeiten für effizientere Verfahren und bessere Dienstleistungen. Gleichzeitig wächst die Abhängigkeit von funktionierenden IT-Systemen. Werden kommunale Netze durch Cyber-Angriffe lahmgelegt, können Bürgerämter, Zulassungsstellen, Sozialverwaltungen und andere öffentliche Einrichtungen ihre Aufgaben unter Umständen nicht mehr oder nur eingeschränkt erfüllen.

Wie ernst die Bedrohung inzwischen ist, zeigt der am 19. November 2026 veröffentlichte Jahreslagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Die Behörde stellt eine weitere Verschärfung der Cyber-Sicherheitslage fest. Verantwortlich dafür sind neben geopolitischen Spannungen insbesondere die zunehmenden Möglichkeiten Künstlicher Intelligenz, mit der sich Cyber-Angriffe automatisieren und beschleunigen lassen. Erstmals veröffentlicht das BSI einen eigenen Cyber Index, der verschiedene Risikofaktoren zusammenfasst. Mit durchschnittlich 170 Punkten liegt dieser um 50 Prozent über dem Wert des vorherigen Berichtszeitraums.

Angreifer nutzen Sicherheitslücken immer schneller aus

Besonders deutlich wird die Entwicklung bei der Ausnutzung von Sicherheitslücken. Im Berichtszeitraum wurden täglich durchschnittlich 160 neue Schwachstellen in IT-Systemen bekannt – 35 Prozent mehr als im Vorjahr. Zugleich verkürzt sich die Zeit zwischen dem Bekanntwerden einer Schwachstelle und ihrer ersten beobachteten Ausnutzung erheblich. Während sie im vorherigen Berichtszeitraum noch durchschnittlich 53 Tage betrug, waren es im aktuellen Zeitraum 25 Tage. Im zweiten Quartal 2026 sank dieser Wert auf nur noch acht Tage.

Für Behörden bedeutet dies, dass etablierte Prozesse zur Prüfung und Installation von Sicherheitsupdates zunehmend unter Zeitdruck geraten. Besonders problematisch ist das für Kommunen mit kleinen IT-Abteilungen, begrenzten personellen Ressourcen und komplexen Systemlandschaften. „Wir haben es mit Werkzeugen zu tun, die Cyber-Angriffe in bisher unbekannten Mengen und Geschwindigkeiten ermöglichen“, warnt BSI-Präsidentin Claudia Plattner. Cyber-Sicherheit müsse deshalb in einem dynamischen Umfeld ständig neu hergestellt werden.

Kommunen als besonders gefährdete Angriffsziele

Das BSI hebt Kommunen ausdrücklich als besonders verwundbare Ziele hervor. Dabei müssen Angreifer nicht zwangsläufig besonders aufwendige Methoden einsetzen. Häufig genügt es, bekannte Sicherheitslücken oder unzureichend geschützte Zugänge auszunutzen. Die kommunale Verwaltung steht dabei vor besonderen strukturellen Herausforderungen. Unterschiedliche Fachverfahren, historisch

gewachsene IT-Landschaften und die Zusammenarbeit mit externen Dienstleistern erschweren eine einheitliche Sicherheitsarchitektur. Hinzu kommen knappe Haushaltsmittel und der Fachkräftemangel.

Der Deutsche Städte- und Gemeindebund (DStGB) hatte bereits Anfang 2026 auf diese Probleme hingewiesen. Nach Einschätzung des kommunalen Spitzenverbandes erfüllen bislang nur wenige, überwiegend größere Städte die Anforderungen des IT-Grundschutzprofils des BSI. Für viele kleinere Kommunen übersteigen die notwendigen Maßnahmen die verfügbaren personellen, technischen und finanziellen Möglichkeiten. Der DStGB fordert deshalb eine bundesweit koordinierte Cyber-Sicherheitsarchitektur mit einheitlichen Mindeststandards, ausreichender Finanzierung und regionalen Computer Emergency Response Teams (CERTs), die Kommunen bei Sicherheitsvorfällen unterstützen können.

Wenn das Rathaus offline ist

Die Folgen eines erfolgreichen Cyber-Angriffs reichen weit über die betroffene IT-Abteilung hinaus. Können Fachverfahren nicht mehr genutzt werden, geraten zentrale Verwaltungsleistungen ins Stocken. Dazu gehören beispielsweise die Auszahlung von Sozialleistungen, die Ausstellung von Ausweisdokumenten oder die Bearbeitung von Kfz-Zulassungen. Neben der technischen Absicherung wird deshalb die Fähigkeit zum Notbetrieb immer wichtiger. Verwaltungen müssen festlegen, welche Dienstleistungen bei einem längerfristigen IT-Ausfall aufrechterhalten werden müssen und wie dies ohne die regulären digitalen Systeme möglich ist.

Eine im Oktober 2026 veröffentlichte Untersuchung des Brandenburgischen Instituts für Gesellschaft und Sicherheit (BIGS) zeigt allerdings erhebliche Defizite bei der Vorbereitung auf solche Krisen. Demnach fehlt es in kommunalen Verwaltungen häufig an etablierten Meldeketten für IT-Sicherheitsvorfälle und alternativen Kommunikationswegen für den Fall, dass reguläre IT-Systeme ausfallen. Die Untersuchung empfiehlt unter anderem klar definierte Zuständigkeiten, redundante Alarmierungsstrukturen und eine frühzeitige Einbindung der Öffentlichkeitsarbeit in kommunale Krisenstäbe.

Cyber-Sicherheit wird zur Führungsaufgabe

Aus der verschärften Bedrohungslage ergibt sich für Behörden ein wachsender Handlungsbedarf. Neben technischen Schutzmaßnahmen wie regelmäßigen Sicherheitsupdates, Mehrfaktor-Authentifizierung und Datensicherungen gewinnen organisatorische Vorkehrungen an Bedeutung. Dazu zählen insbesondere ein systematisches Schwachstellenmanagement, regelmäßig getestete Notfallpläne und die Schulung der Beschäftigten. Auch die Zusammenarbeit mit kommunalen IT-Dienstleistern und den Sicherheitsbehörden der Länder muss klar geregelt sein.

Das BSI unterstützt Kommunen unter anderem mit dem IT-Grundschutzprofil „Basis-Absicherung Kommunalverwaltung“ und dem niedrigschwelligen Einstiegskonzept „Weg in die Basis-Absicherung“ (WiBA). Damit sollen auch Verwaltungen mit begrenzten Ressourcen schrittweise ein angemessenes Sicherheitsniveau erreichen können. Entscheidend ist dabei, Informationssicherheit nicht allein als Aufgabe der IT-Abteilung zu verstehen. Sie muss vielmehr Bestandteil der Verwaltungssteuerung und der kommunalen Haushalts- und Personalplanung werden.

Stärkung der Cyber-Sicherheit

Der BSI-Lagebericht macht deutlich, dass der Ausbau digitaler Verwaltungsangebote mit einer entsprechenden Stärkung der Cyber-Sicherheit einhergehen muss. Je mehr Verwaltungsleistungen ausschließlich digital erbracht werden, desto gravierender können die Folgen eines Systemausfalls sein. Dabei geht es nicht nur um die Abwehr von Angriffen. Auch die Abhängigkeit von einzelnen IT-Dienstleistern, Cloud-Plattformen und zentralen Infrastrukturen wird zu einer strategischen Frage. Behörden müssen sicherstellen, dass sie bei technischen Störungen oder Sicherheitsvorfällen zumindest ihre wichtigsten Aufgaben weiter erfüllen können.

Die Herausforderung ist damit nicht allein technischer Natur. Gerade auf kommunaler Ebene wird Cyber-Sicherheit zunehmend zu einer Frage staatlicher Handlungsfähigkeit. Der aktuelle BSI-Bericht unterstreicht die Dringlichkeit, Sicherheitsstandards nicht nur zu definieren, sondern sie auch flächendeckend umzusetzen. Dafür benötigen Städte, Gemeinden und Landkreise neben klaren Vorgaben vor allem verlässliche Unterstützung durch Bund und Länder.

()

BSI-Lagebericht 2026 (PDF)
Das Titelthema der Dezember-Ausgabe von Kommune21 lautet: "IT-Sicherheit - Wappnen für die Attacke". Hier können Sie ein Einzelheft bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, BSI-Lagebericht, Bundesamt für Sicherheit in der Informationstechnik (BSI), Cybersicherheit