Baden-Württemberg

Cyber-Sicherheit als politische Aufgabe

[17.11.2026] Die Cybersicherheitsagentur Baden-Württemberg hat 2025 mehr Cyber-Sicherheitsvorfälle erfasst. Innenminister Manuel Hagel betont den Schutz von Behörden und kritischen Infrastrukturen als festen Bestandteil der Sicherheitspolitik. Die Agentur will ihre Prävention ausbauen.

Die Cybersicherheitsagentur Baden-Württemberg (CSBW) hat ihren Jahresbericht für 2025 vorgestellt. Daraus geht hervor, dass insbesondere Kommunen und Hochschulen im Fokus von Cybercrime-Gruppierungen standen. „Vor dem Hintergrund der aktuellen Bedrohungslage ist für uns klar, dass Cyber-Sicherheit ein fester Bestandteil unserer Sicherheitspolitik ist. Die digitale Verwundbarkeit stellt ein reales Risiko für unsere Gesellschaft, Wirtschaft und den Staat dar. Es ist ganz entscheidend, dass wir uns gegen Cyber-Angriffe abhärten und unsere Kritischen Infrastrukturen sowie Behörden vor diesen Bedrohungen schützen“, sagt der stellvertretende Ministerpräsident und Innenminister Manuel Hagel.

Was die erfassten Vorfälle zeigen

Bei Landkreisen, Städten und Gemeinden sowie kommunalen Unternehmen stieg die Zahl der erfassten Fälle gegenüber 2024 um fast 50 Prozent. An Hochschulen, Universitäten und vergleichbaren Einrichtungen nahm die Zahl der minderschweren Fälle um mehr als 160 Prozent zu. Erfolgreiche Ransomware-Angriffe auf drei Schulen und zwei Kommunen schränkten deren Arbeitsfähigkeit teilweise durch eine vollständige Verschlüsselung der Systeme stark ein. Hinzu kamen der Angriff auf den Online-Shop einer Landesinstitution und die teilweise erfolgreiche Kompromittierung eines Hochschulnetzwerks. Die CSBW führt die Entwicklung sowohl auf eine höhere Aktivität von Ransomware-Gruppierungen als auch auf verbesserte Erkennungs- und Auswertungsmöglichkeiten zurück. Zudem ist die Meldebereitschaft gestiegen. Für Kommunen und Unternehmen besteht keine generelle Pflicht, Cyber-Sicherheitsvorfälle an die Behörde zu melden. Die Fallzahlen bilden deshalb nicht ausschließlich Veränderungen der tatsächlichen Bedrohungslage ab. Die Erkenntnisse sollen in die Weiterentwicklung zielgruppengerechter Präventions- und Sensibilisierungsmaßnahmen einfließen.

Breiter Schutzauftrag

„Wir brauchen ein umfassendes Verständnis, das nicht nur die technische Sicherheit von Systemen und Netzen umfasst, sondern auch die politische, wirtschaftliche und strategische Dimension von Cyber-Angriffen in den Blick nimmt“, sagt CSBW-Präsidentin Nicole Matthöfer. Ihrem Cyber-Monitoring schreibt die Behörde für 2025 die Verhinderung potenzieller Schäden von rund 24 Millionen Euro zu. Zugleich wächst nach Angaben von Vizepräsident Björn Schemberger, dem Leiter der Abteilung Detektion und Reaktion, die Nachfrage nach Unterstützung. Schulungen, der Warn- und Informationsdienst, Sicherheitschecks für kleine und mittlere Unternehmen sowie IT-Notfallübungen würden zunehmend genutzt. Die CSBW sieht eine weitere Herausforderung im Einsatz Künstlicher Intelligenz durch Cyber-Kriminelle: KI-generierte Phishing-Mails würden häufiger und überzeugender und erhöhten die Erfolgschancen der Angreifer. Wie schnell und weitreichend sich die Möglichkeiten von KI-Modellen verändern, sei derzeit kaum abzuschätzen. Die Agentur will deshalb ihre Präventions- und

Sensibilisierungsangebote ausbauen.

(sib)

• Jahresbericht 2025 der CSBW

Stichwörter: IT-Sicherheit, Baden-Württemberg, CSBW, Politik