Baden-Württemberg

Jahresbericht zur Cybersicherheit 2024

[21.05.2025] Die CSBW hat 2024 rund 30 Prozent mehr IT-Sicherheitsvorfälle bearbeitet. Kommunen wurden ähnlich häufig unterstützt wie im Vorjahr, neue Präventionsangebote, Notfallübungen und ein Schwachstellenscan richten sich teils gezielt an sie.

Die Cybersicherheitsagentur Baden-Württemberg (CSBW) hat ihren Jahresbericht 2024 veröffentlicht. Im dritten Jahr ihres Bestehens baute sie ihre Unterstützungsangebote weiter aus – mit neuen Schulungen, Pilotprojekten und technischen Diensten. Auch die Zahl der bearbeiteten Vorfälle nahm erneut deutlich zu. „Wir verzeichnen mehr Gefahren, aber auch mehr Bewusstsein. Prävention, Detektion und Reaktion greifen immer stärker ineinander – das ist ein Fortschritt“, sagte Nicole Matthöfer, die seit Mai 2024 die CSBW als Präsidentin führt (wir berichteten).

Unterstützte Kommunen auf Vorjahresniveau

Im Jahr 2024 erfasste die CSBW demnach 517 Fälle mit Bezug zur Cybersicherheit – rund 30 Prozent mehr als im Vorjahr. Das gesamte Spektrum war vertreten: von falsch-positiven Virenscanner-Meldungen über Phishing-Angriffe, kompromittierten Zugangsdaten, ungepatchten Systemen bis hin zu Ransomware-Fällen mit Vollverschlüsselung. Drei Einsätze übernahm das Mobile Incident Response Team (MIRT) vor Ort. Die Anzahl der unterstützten Kommunen – Landkreise, Städte, Gemeinden sowie Unternehmen in kommunaler Trägerschaft – blieb mit 49 Fällen etwa auf dem Niveau des Vorjahres (54 Fälle). Zusätzlich beriet die CSBW Hochschulen und vergleichbare Einrichtungen in 110 Fällen (Vorjahr: 38 Fälle) und war in einem Fall auch dort mit dem MIRT im Einsatz. Die Landesverwaltung wurde in 183 Fällen unterstützt (Vorjahr: 170 Fälle).

Mehr gezielte Prävention

Im Bereich Prävention hat die CSBW ihre Aktivitäten deutlich erweitert. Insgesamt wurden über 120 Schulungen durchgeführt – nahezu eine alle drei Tage. Die Themen reichten von Passwortsicherheit über Aufbauschulungen zur Prävention im Arbeitsalltag bis hin zu zielgruppenspezifischen Formaten für Verwaltungen. Über 4.250 Personen wurden erreicht, darunter auch zahlreiche Beschäftigte der kommunalen Ebene. Um das Angebot dauerhaft und systematisch zugänglich zu machen, hat die Behörde ein Learning-Management-System eingeführt (wir berichteten). Dort waren bis Jahresende über 1.369 Nutzerinnen und Nutzer registriert, 3.091 Teilnahmezertifikate wurden vergeben. Ein neues Pilotprojekt richtete sich gezielt an Kommunen: In fünf Verwaltungen wurde 2024 ein IT-Notfall simuliert, um bestehende Abläufe im Krisenfall zu testen. Die CSBW will das Angebot 2025 weiterentwickeln.

Angriffsflächen und Angreifer schneller finden

Technisch ergänzte die Behörde ihr Portfolio um Schwachstellenscans. Seit Ende 2024 können öffentliche Stellen dieses Instrument nutzen, um potenzielle Angriffsflächen zu identifizieren und frühzeitig Gegenmaßnahmen zu treffen. Auch der Warn- und Informationsdienst wurde ausgebaut: Über eine neue Plattform stellt die CSBW sicherheitsrelevante Informationen nun in Echtzeit bereit – individualisiert und

exklusiv erreichbar aus den Netzen von Land und Kommunen. Über dieselbe Plattform können Sicherheitsvorfälle direkt gemeldet und bestehende Meldeketten in Gang gesetzt werden. Ein weiteres Instrument der CSBW ist das Monitoring des Cyberraums – auch im Darknet. 2024 informierte die Behörde in 90 Fällen betroffene Unternehmen, Kommunen sowie wissenschaftliche Einrichtungen über sicherheitsrelevante Funde. Die Zahl der Meldungen hat sich unter anderem durch erweiterte Analysemethoden erhöht, mit denen die CSBW das digitale Dunkelfeld gezielter beobachten kann.

(sib)

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