CSBW | CYBER SICHERHEITS AGENTUR Baden-Württemberg

CSBW-Factsheet: Cybersecurity-Wissen kompakt

SICHERE KOMMUNALVERWALTUNG

IT-Systeme von Kommunen geraten immer häufiger in den Fokus von Cyberkriminellen.

Cyberangriffe durch Ransomware[1] legen immer häufiger den Betrieb von Kommunen lahm. Die Folge sind massive Einschränkungen bei der Aufgabenerfüllung einer Kommune, so dass vom Ausweisantrag bis hin zur Zahlung sozialer Leistungen alles blockiert sein kann. Hinzu kommt, dass die Cyberkriminellen oft sensible Daten erbeuten.

Mögliche Gefahren von Cyberangriffen:

- Massive Einschränkungen des laufenden Betriebs einer Kommune bis hin zum Stillstand.
- Erbeutung und Veröffentlichung sensibler Daten von Bürgerinnen und Bürgern, Verwaltung und Wirtschaft.
- Vertrauensverlust in die Digitalisierung und Reputationsschaden für alle Beteiligten.
- Missbrauch der gestohlenen Daten, etwa zum Zahlungsbetrug.

Ursachen:

- Veraltete IT-Systeme und fehlende oder unregelmäßige Software-Aktualisierungen.
- Mangelnde Professionalität beteiligter Dienstleister.
- Einsatz mangelhafter Software-Produkte.
- Unzureichende technische Absicherungen, insbesondere keine ausreichend vor Ransomware abgesicherten Backup-Systeme.
- Fehlendes Bewusstsein für die Gefahr und die Folgen von Cyberangriffen auf eine Kommune.
- Mangelhafte Sensibilisierung der Mitarbeitenden.
- Fehlendes Notfallmanagement und fehlendes Kommunikationskonzept im Krisenfall.
- Zu geringe finanzielle und personelle Ausstattung im Bereich Informations-sicherheit.

[1] **Ransomware** sind Schadprogramme, die komplette IT-Systeme lahmlegen und deren Daten verschlüsseln. Die Angreifer fordern dabei ein Lösegeld (Englisch: *ransom*) für die Entschlüsselung. Zusätzlich drohen sie oft unter Fristsetzung mit der Veröffentlichung der (häufig sensiblen) Daten.

[2] **E-Government-Gesetz BW,** Gesetz zur Förderung der elektronischen Verwaltung des Landes Baden-Württemberg

[3] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunalverwaltung.html

Weitere Factsheets und Informationen finden Sie unter: www.cybersicherheit-bw.de.

Handlungsempfehlungen für eine sichere Kommunalverwaltung:

- Informationssicherheit langfristig planen, systematisch umsetzen sowie ausreichend finanzielle und personelle Mittel hierfür zur Verfügung stellen.
- Alle IT-Systeme müssen dem aktuellen Stand der Technik entsprechen, dieser ist auch nach § 16 Absatz 1 EGovG BW[2] umzusetzen. Nicht dem Stand der Technik entspricht z. B. der Einsatz von veralteter Software, für die keine Sicherheitspatches mehr bereitgestellt werden, wie z. B. Windows 7.
- Systeme müssen regelmäßig und möglichst automatisch aktualisiert werden. Veraltete Systeme können in gemeinsamen Netzen nicht geduldet werden.
- Externe IT-Dienstleister müssen professionell sein und sollten möglichst viel Erfahrung mit der kommunalen Verwaltung haben. Im Idealfall sind sie nach ISO/IEC 27001 zertifiziert, wie dies z. B. bei der Komm.ONE der Fall ist.
- Jede Kommune ist selbst dafür verantwortlich, dass ihre IT-Systeme sicher sind. Die Verantwortung externer Dienstleister in Bezug auf die Beachtung aller notwendigen Aspekte der Informationssicherheit muss gewährleistet und vertraglich abgesichert sein.
- Mit dem Internet verbundene IT-Systeme und Internetanschlüsse müssen über gesonderte, dauerhaft besonders überwachte Systeme betrieben werden. Das gilt insbesondere für Mailserver.
- Es müssen redundante Offline-Backup-Systeme eingerichtet sein, die sicher vor Ransomware-Angriffen sind. Im Fall eines Cybernotfalls ist eine professionell durchgeführte Wiederherstellung der Systeme mithilfe nicht kompromittierter Datensicherungen essentiell. Die CSBW berät hierzu gerne, denn nicht alle IT-Dienstleister verfügen über die notwendigen Erfahrungen.
- Für den Krisenfall müssen ein Notfallplan und Konzepte für die interne und externe Kommunikation vorliegen.
- Die CSBW empfiehlt Kommunen die systematische Umsetzung des IT-Grundschutzprofils *Basis-Absicherung Kommunalverwaltung*[3].
- Eine Kommune darf ein digitales Angebot erst dann bereitstellen, wenn es ausreichend abgesichert ist!