CSBW
CYBER SICHERHEITS AGENTUR
BADEN-WÜRTTEMBERG

Sichere Kommunalverwaltung

Cyberangriffe durch Ransomware[1] legen immer häufiger den digitalen Betrieb einer Kommune lahm. Die Folge sind massive Einschränkungen für die Dienstleistungen der Kommune, so dass von der Führerscheinausgabe bis hin zur Zahlung sozialer Leistungen alles blockiert sein kann.
Hinzu kommt, dass die Angreifer oft sensible Daten erbeuten.

Gefahren:

- Massive Einschränkungen des laufenden Betriebs einer Kommune bis hin zum Stillstand
- Erbeutung und Veröffentlichung sensibler Daten von Bürgern und Unternehmen
- Reputationsschaden für die Digitalisierung im Allgemeinen und für alle Beteiligte

Ursachen:

- Veraltete IT-Systeme und fehlende Patches, keine regelmäßig durchgeführten Updates
- Mangelnde Professionalität beteiligter Dienstleister und schlechte Produkt-Qualität
- Unzureichende technische Absicherungen, insbesondere keine ausreichend vor Ransomware abgesicherten Backup-Systeme
- Mangelhafte Sensibilisierung der Mitarbeiter
- Fehlendes Notfallmanagement und fehlendes Kommunikationskonzept im Krisenfall
- Zu geringe finanzielle und personelle Ausstattung im Bereich Informationssicherheit in den Kommunen
- Fehlendes Bewusstsein für die Gefahr und die Folgen von Cyberangriffen auf eine Kommune

Sichere Kommunalverwaltung

Handlungsempfehlungen für eine sichere Kommunalverwaltung:

- Informationssicherheit langfristig planen, systematisch umsetzen und finanzielle und personelle Mittel hierfür zur Verfügung stellen.
- Alle IT-Systeme müssen dem Stand der Technik entsprechen, dieser ist auch nach §16 Absatz 1 EGovG BW[2] umzusetzen.
- Externe IT-Dienstleister sollten etabliert und müssen professionell sein. Im Idealfall haben sie Erfahrung mit der kommunalen Verwaltung.
- Die Verantwortung externer IT-Dienstleister in Bezug auf die Beachtung aller notwendigen Aspekte der Informationssicherheit muss gewährleistet und vertraglich abgesichert sein.
- Systeme müssen regelmäßig aktualisiert und gepatcht werden. Veraltete Systeme können in gemeinsamen Netzen nicht geduldet werden.
- Wichtige mit dem Internet verbundene IT-Systeme und Internetanschlüsse müssen über gesonderte, besonders überwachte Systeme betrieben werden und dauerhaft überwacht 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 essenziell.
- Es muss ein Kommunikationskonzept für den Krisenfall vorliegen.
- Langfristig kann die systematische Umsetzung des IT-Grundschutzprofils *Basis-Absicherung Kommunalverwaltung*[3] helfen.
- Wenn ein Schritt der Digitalisierung einer Kommune nicht ausreichend sicher ist, darf dieser nicht gegangen werden!

Quellen und weiterführende Literatur:

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

CSBW
CYBER SICHERHEITS AGENTUR
BADEN-WÜRTTEMBERG

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

CSBW Prävention
Kontakt: schulungen@cybersicherheit.bwl.de
Stand: 05.2023