KOM SG

Erkenntnisse aus den Security-Audits 2022

Im Jahr 2022 wurden wie in den Vorjahren Security-Audits im Auftrag der KOM SG bei ausgewählten Gemeinden durchgeführt. Die wichtigsten Erkenntnisse und daraus entstehende Handlungsempfehlungen werden in diesem Dokument festgehalten.

1 Aktualisierung Software

Bei vielen der überprüften Gemeinden wurde - wie auch bereits in den Vorjahren – Mängel bezüglich zeitnaher Aktualisierung von Computersoftware festgestellt. Bei den meisten Gemeinden fehlt eine regelmässige Aktualisierung von installierter Software auf den Computersystemen. Diese Software wird meist initial vom IT-Dienstleister installiert, jedoch kaum oder nur sehr selten aktualisiert.

Empfohlene Massnahmen:

- Service Level Agreements (SLA) mit IT-Dienstleistern erstellen, in welchem die regelmässigen Updates definiert sind.

2 Netzwerksicherheit

Nach wie vor treffen wir auf viele «flache» Netzwerke bei den Gemeindeverwaltungen. Sämtliche Systeme werden dabei im gleichen Netzwerk betrieben oder die unterschiedlichen Netzwerke sind transparent untereinander verbunden. Dies erlaubt es, Angreifern sich einfacher im Netzwerk auszubreiten.
Auch die neu durchgeführten Prüfungen bezüglich dem Active Directory (Verzeichnisdienst) zeigen fast bei allen Audits Mängel auf, die verbessert werden sollten. So haben viele Benutzende Zugriffsrechte (Admin-Accounts), die nicht benötigt werden.

Die aktuellen Sicherheitsvorschriften der KOM SG wurden durch den Vorstand per 1. Januar 2023 in Kraft gesetzt und tragen den oben genannten Aspekten Rechnung. Im 2. Quartal 2023 finden Online-Events zu den neuen Sicherheitsvorschriften statt. Zudem überarbeitet die KOM SG die Musterinformatikweisung für Gemeinden.

Empfohlene Massnahmen:

- Umsetzung der Massnahmen gemäss der neuen Sicherheitsvorschriften
- Durchführen von Audits und Penetrationstest
- Informatikweisung überprüfen und ggf. anpassen