Umgang mit Lösegeldforderungen bei Angriffen mit Verschlüsselungstrojanern auf Kommunalverwaltungen

Empfehlungen der Bundesvereinigung der kommunalen Spitzenverbände, des Bundeskriminalamtes und des Bundesamtes für Sicherheit in der Informationstechnik

Weltweit kommt es immer häufiger mit Hilfe von Verschlüsselungs-Schadprogrammen (Ransomware) zu kriminell motivierten Angriffen auf die informationstechnische Infrastruktur von Kommunalverwaltungen bzw. kommunalen Einrichtungen. Diese Angriffe haben die Erlangung von Lösegeldern zum Ziel.

Jede Lösegeldzahlung macht eine Erpressung zum Erfolg für den Erpresser und motiviert diesen und andere potenzielle Angreifer zur Fortsetzung und Weiterentwicklung der Angriffe. Außerdem besteht das Risiko, dass nach einer Zahlung nicht das erhoffte Ergebnis eintritt oder weitere Forderungen erhoben werden.

Die Bundesvereinigung der kommunalen Spitzenverbände, das Bundeskriminalamt (BKA) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfehlen allen Kommunalverwaltungen,

- sich im Falle von Erpressungsversuchen grundsätzlich nicht auf Lösegeldzahlungen einzulassen,
- jeden Erpressungsversuch zur Anzeige zu bringen sowie
- das jeweilige Landes-CERT oder das BSI zu informieren (www.allianz-fuer-cybersicherheit.de/ACS/DE/Meldestelle/meldestelle.html)

Um die Auswirkungen auf Verfügbarkeit und Integrität der IT-Systeme im Falle eines Ransomware-Angriffs zu minimieren, sollten Kommunalverwaltungen Vorkehrungen für rechtzeitige systematische Präventions-, Detektions- und Reaktionsmaßnahmen sowie ein effektives Notfall- und Informationssicherheitsmanagement treffen.

Eine Liste der Zentralen Ansprechstellen Cybercrime (ZAC) der Polizeien finden Sie unter: www.allianz-fuer-cybersicherheit.de/ACS/ZACs

Informationen über geeignete Präventions- und Reaktionsmaßnahmen und über Notfallmanagement stellt das BSI auf den Webseiten der Allianz für Cyber-Sicherheit zur Verfügung: www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Themen/Ransomware/ransomware_node.html

www.allianz-fuer-cybersicherheit.de/ACS/IT-Notfallkarte

Der IT-Grundschutz des BSI bietet ausführliche Informationen und Standards für die Gestaltung von Informationssicherheit und Notfallmanagement: www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

Berlin, März 2020