IT-Sicherheit

Kommunen zahlen kein Lösegeld

[05.03.2020] Empfehlungen, wie sich Kommunalverwaltungen bei IT-Angriffen mit Lösegeldforderungen verhalten sollen, haben jetzt die kommunalen Spitzenverbände, das Bundeskriminalamt und das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht. Für Erpressungsversuche gilt demnach eine -Toleranz-Politik.

Gemeinsam mit dem Bundeskriminalamt (BKA) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) haben jetzt die kommunalen Spitzenverbände Empfehlungen zum Umgang mit Lösegeldforderungen bei IT-Angriffen auf Kommunalverwaltungen mit Erpressungstrojanern herausgegeben. „Wir dürfen derartigen Lösegeldforderungen nicht nachgeben“, lautet der Aufruf der Präsidenten des Deutschen Städtetages, des Deutschen Landkreistages und des Deutschen Städte- und Gemeindebundes, Oberbürgermeister Burkhard Jung (Leipzig), Landrat Reinhard Sager (Kreis Ostholstein) und des Ersten Bürgermeisters Uwe Brandl (Abensberg). „Es muss klar sein, kommunale Verwaltungen sind nicht erpressbar. Sonst werden den Kriminellen Anreize geboten, ihre Handlungen fortzusetzen. Hier muss die Haltung unserer Verwaltungen glasklar und nicht verhandelbar sein.“ Jeder Erpressungsversuch muss laut den Präsidenten zur Anzeige gebracht und verfolgt werden. Zudem sollte das jeweilige Landes-CERT oder das BSI informiert werden, heißt es in den gemeinsamen Empfehlungen mit dem BSI und dem BKA. „Für derartige Angriffe auf die Funktionsfähigkeit kommunaler Dienstleistungen, die Daten von Bürgerinnen und Bürgern und deren Steuergeld, muss eine -Toleranz-Politik gelten“, betonen die Präsidenten der kommunalen Spitzenverbände. Eine Haltung, die auch BKA-Präsident Holger Münch bekräftigt: „Betroffene Kommunen sollten niemals auf Erpressungsversuche von Cyber-Kriminellen eingehen. Denn damit unterstützen sie das Geschäftsmodell der Erpresser.“

Muster durchbrechen

Laut BKA-Präsident Münch leisten Geschädigte in vielen Fällen ihre Zahlungen umsonst. „Die Daten bleiben verschlüsselt und die Täter setzen ihre Straftaten ungehindert fort“, berichtet er. „Kommunalverwaltungen können dazu beitragen, dieses Muster zu durchbrechen: Indem sie die zuständigen Behörden alarmieren und damit die Strafverfolgung ermöglichen. Und indem sie präventive Maßnahmen ergreifen, um ihre Computer-Systeme wirksam zu schützen.“
Zu Letzterem ermuntert neben den kommunalen Spitzenverbänden auch das BSI. Konsequent umgesetzte IT-Sicherheitsmaßnahmen stellen laut BSI-Präsident Arne Schönbohm den besten Schutz vor Lösegeldforderungen durch Cyber-Kriminelle dar. „Dies ist ein kontinuierlicher Prozess, den das Bundesamt für Sicherheit in der Informationstechnik unterstützt, etwa mit dem IT-Grundschutz-Profil für Kommunen. Neben den essenziellen Präventionsmaßnahmen bietet das BSI außerdem Informationen zur Ersten Hilfe bei IT-Sicherheitsvorfällen an“, so Schönbohm weiter. „Ein effektives Notfall-Management kann die Auswirkungen eines Cyber-Angriffs entscheidend minimieren. Das BSI steht auch Kommunen hierfür gerne beratend zur Seite.“
Eine Liste der Zentralen Ansprechstellen Cybercrime (ZAC) der Polizeien finden sich auf den Websites der Allianz für Cyber-Sicherheit. Dort stellt das BSI außerdem Informationen über geeignete Präventions- und Reaktionsmaßnahmen sowie über das Notfall-Management zur Verfügung. Ausführliche Informationen und Standards für die Gestaltung von Informationssicherheit und Notfall-Management finden sich darüber hinaus auf den Websites des BSI.

(ba)

Stichwörter: IT-Sicherheit, Cyber-Sicherheit, DStGB, Deutscher Landkreistag, Deutscher Städtetag, Bundeskriminalamt (BKA), Bundesamt für Sicherheit in der Informationstechnik (BSI)