klimaschutz-kommune.de // News 2-3 // Keywords: Cybersicherheit, Hackerangriff

Digitalisierung, Siegen-Wittgenstein

Hackerangriff legte Kommunen in NRW lahm

Einige Kommunen in NRW können seit Monaten nur eingeschränkte Bürgerservices anbieten. Grund dafür ist ein Hackerangriff auf den IT-Dienstleister Südwestfalen-IT. Angesichts einer generell hohen Bedrohungslage fordert Bundesinnenministerin Nancy Faeser, dem Thema Cybersicherheit eine neue Priorität einzuräumen.

MargJohnsonVA@EnavtoElements

Ein Hackerangriff hatte im Oktober 2023 die öffentlichen Verwaltungen und Rathäuser von über 70 Kommunen in Nordrheinwestfalen lahmgelegt. Angriffsziel war das Netzwerk des IT-Dienstleisters Südwestfalen-IT, wie ZEIT Online berichtete. Das Unternehmen hatte einen sogenannten Erpressungstrojaner entdeckt und daraufhin die Verbindung zu den Nutzern der Software gekappt. Der Hackerangriff hatte gravierende Auswirkungen auf den Betrieb der Behörden: Bürgerbüros, Kfz-Zulassungsstellen und Ausländerbehörden mussten ihre Arbeit einstellen. Personalausweise und

Beurkundungen konnten nicht erstellt werden, Auszahlungen funktionierten oft nicht. Viele Verwaltungen in Rathäusern waren nicht erreichbar – weder per Telefon noch per E-Mail. Besonders stark betroffen war der Kreis Siegen-Wittgenstein.

Ein forensischer Bericht des Unternehmens offenbarte im Januar: der Hauptzugang des kommunalen Dienstleisters war nicht ausreichend geschützt. Über die softwarebasierte VPN-Lösung, welche nur mit einem einfachen Passwort gesichert war, konnten die Angreifer ins System eindringen. Persönliche Daten von Einwohnern seien, laut Bericht von externen Cyber-Security-Experten, nicht abgeflossen. Nichtsdestotrotz stellte IT-Experte Philipp Rothmann dem Unternehmen ein vernichtendes Zeugnis aus. Gegenüber dem WDR sagte er: „Die Südwestfalen-IT hat es den Angreifern sehr leicht gemacht." Üblich wäre hier eine „Multifaktor-Authentifizierung" gewesen, d. h. eine Abfolge von mehreren Passwörtern. Im vorliegenden Fall mussten die Hacker aber nur lang genug verschiedene Varianten durchprobieren.

Cybersicherheit muss Priorität haben

Der Hackerangriff auf NRW-Kommunen zeigt einmal mehr, wie vulnerabel IT-Systeme sind. Gleichzeitig wird offenbar, dass das Thema Cybersicherheit in Städten und Kommunen massiv unterschätzt wird. In einem Bericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) im Oktober erklärte Bundesinnenministerin Nancy Faeser: „Die Bedrohungslage ist besorgniserregend. Die Gefährdung ist sehr komplex und kann jederzeit eskalieren." Faeser forderte, dass Deutschland sich auf entsprechende Szenarien vorzubereiten habe und man Cybersicherheit eine ganz neue Priorität einräumen müsse.

Auch Claudia Plattner, BSI-Präsidentin, sagte im Gespräch mit dem WDR, dass Cybersicherheit immer noch nicht den Stellenwert habe, den es haben müsse, angesichts der Größe des Problems. Plattner verwies auf ein weiteres großes Problem im Zusammenhang mit Cybersicherheit in Deutschland: Hierfür stehe nicht genug Geld zur Verfügung: „Angesichts der Aufgaben, die auf uns zukommen, muss man definitiv sagen, das wird haushalterisch ganz, ganz schwer, wirklich diesen Job so machen zu können, wie man ihn eigentlich machen müsste", so Plattner weiter. Dazu zähle auch, dass Unternehmen und Kommunen Hackerangriffe schneller bemerken müssten. Andreas Lüning von G Data erklärte hierzu gegenüber dem WDR: Bevor es überhaupt zu einem Erpressungsversuch käme, hätten Angreifer sich i. d. R. bereits 100 bis 200 Tage im Unternehmen umgeschaut. Zeit genug, um alle möglichen Daten abzugreifen.

Bürgerservices ab Ende März wieder verfügbar

Laut Medienberichten sollen die wichtigsten Verwaltungssysteme der Südwestfalen-IT Ende März wieder normal laufen und zentrale Bürgerservices der betroffenen Kommunen wieder uneingeschränkt zur Verfügung stehen. Sicherheitslücken seien inzwischen geschlossen worden, so das Unternehmen selbst. Ein neuer Geschäftsführer soll den Vorgang in der Südwestfalen-IT nun

aufarbeiten und weitere Schwachstellen beheben. Verantwortlich für den Hackerangriff auf die NRW-Kommunen war mutmaßlich die Gruppe „Akira“. Sie gehört zu einer der fünf gefährlichsten Hackergruppen weltweit.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet Kommunen einen unkomplizierten und ressourcenschonenden Einstieg in den etablierten IT-Grundschutz an. Kommunen können hier [EXTERNER LINK: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/WIBA/Weg_in_die_Basis_Absicherung_WiBA_node.html] anhand von Checklisten mit einfachen Prüffragen und entsprechenden Hilfsmitteln die nötigsten Maßnahmen selbst identifizieren und umsetzen. Außerdem existieren vom BSI zahlreiche Informationsangebote sowie Förderprogramme zur Cybersicherheit, die Kommunen dabei unterstützen, ihre Cybersicherheit zu verbessern. [EXTERNER LINK: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/ACS_Broschuere.pdf?__blob=publicationFile&v=3]

Quellen:

- CSO: IT-Forensik-Bericht enthüllt schwere Sicherheitslücke; https://www.csoonline.com/de/a/it-forensik-bericht-enthuellt-schwere-sicherheitsluecke,3681237
- WDR: Hackerangriff: Südwestfalen-IT räumt schwere Sicherheitslücke ein https://www1.wdr.de/nachrichten/westfalen-lippe/suedwestfalen-it-raeumt-sicherheitsluecke-ein-100.html
- WDR: Hackerangriff stellt NRW-Kommunen weiter vor große Probleme; https://www1.wdr.de/nachrichten/hackerangriff-legt-kommunen-weiter-lahm100.html
- ZEIT Online: Hackerangriff legt IT-Infrastruktur von 70 Kommunen lahm; https://www.zeit.de/digital/2023-10/cybersicherheit-hackerangriff-cyberangriff-kommunen-nrw
- bsi.bund.de: Allianz für Cyber-Sicherheit; https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Allianz-fuer-Cyber-Sicherheit/Vernetzen/vernetzen_node.html