IT-Sicherheit

Kehrseite der Digitalisierung

[10.01.2022] Mit fortschreitendem Digitalisierungsgrad häufen sich Cyber-Angriffe und IT-Sicherheitsvorfälle. Die jüngsten Vorkommnisse in Schwerin, Witten und Sachsen-Anhalt werfen ein Schlaglicht auf den Zustand der IT-Sicherheit in Kommunen.

Die Schlagzeilen lauten „Cyber-Angriff legt Stadtverwaltung lahm“, „Datendiebe steigen ein“, „Kein Normalbetrieb mehr in diesem Jahr“ oder „So kamen die Hacker ins Netzwerk“. Quasi im Wochentakt ist von Cyber-Angriffen, IT-Sicherheitsvorfällen, Schad-Software-Befall und Cyber-Erpressung zu erfahren. Privatleute, Unternehmen und immer häufiger auch Kommunen, Verwaltungen, selbst Schulen und Krankenhäuser sind davon betroffen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) geht in seinem jüngsten Bericht zur Lage der IT-Sicherheit in Deutschland von einer angespannten bis kritischen Sicherheitslage aus. BSI-Präsident Arne Schönbohm erklärte: „Es ist nicht nur die Anzahl von Sicherheitsvorfällen, die besorgniserregend ist, es ist auch die rasante Entwicklung neuer und angepasster Angriffsmethoden, die massenhafte Ausnutzung schwerwiegender Software-Schwachstellen und die teilweise gravierenden Folgen, die erfolgreiche Cyber-Angriffe auslösen.“
Die Zahlen sind abenteuerlich: Fast 15 Millionen kritische Meldungen übermittelte das BSI an deutsche Netzbetreiber, 144 Millionen Schadprogramm-Varianten wurden 2021 gezählt – ein Anstieg um 22 Prozent gegenüber dem Vorjahr. 44.000 Mails mit Schadprogrammen wurden allein in deutschen Regierungsnetzen abgefangen. Bei 98 Prozent wurden Schwachstellen in der Serversoftware MS Exchange festgestellt.

Verwaltungsdienste fielen wochenlang aus

So auch in Mecklenburg-Vorpommern. Zuerst betraf es Anfang Oktober 2021 die Stadtwerke Wismar, dann am 15. Oktober die kommunalen IT-Dienstleister KSM und SIS in Schwerin und schließlich das Datenverarbeitungszentrum Mecklenburg-Vorpommern. Weite Teile der Server-Systeme wurden von einer Schad-Software verschlüsselt und waren damit nicht erreichbar. Betroffen sind kommunale Unternehmen und Kommunalverwaltungen, etwa Bürgerbüros in Schwerin und im Landkreis Ludwigslust-Parchim, wo praktisch alle IT-gestützten Verwaltungsdienste – Kfz-Wesen, Passwesen, Grundsicherung – wochenlang ausfielen und teils ein analoger Notdienst eingeführt werden musste.
Die Verantwortlichen reagierten schnell. Man fuhr alle Systeme herunter und trennte sie vom Netz, schaltete IT-Forensiker des BSI ein, informierte die Staatsanwaltschaft und begann umgehend mit der Schadensanalyse. Nach Angaben von Matthias Effenberger, Geschäftsführer des Schweriner IT-Dienstleisters SIS, sind voraussichtlich keine personengebundenen Daten abgeflossen. Ein abschließender datenforensischer Bericht steht aber noch aus. Auch die Wiederherstellung der Systeme sei wieder angelaufen. „Nach aktuellem Stand gehen wir davon aus, dass sämtliche Datenbestände als Back-up verfügbar sind und zur Wiederherstellung der Systeme genutzt werden können“, erklärte Effenberger. „Hier zahlt sich unser strenges Datensicherungskonzept aus.“ Mit einem Normalbetrieb sei allerdings erst 2022 wieder zu rechnen.

Lohnen Zertifizierung und Zentralisierung?

Wie lange ein IT-Wiederaufbau nach einer derartigen Cyber-Attacke dauern kann, zeigt das Beispiel Anhalt-Bitterfeld. Dort kam es Anfang Juli 2021 zu einem so genannten Ransomware-Angriff, bei dem mehrere Server des Landkreises mit Schad-Software infiziert und sämtliche Daten verschlüsselt wurden. Die Hackergruppe Pay or Grief (Zahle oder trauere) meldete sich mit einer Lösegeldforderung, der sich das Landratsamt jedoch verweigerte, woraufhin 200 Megabyte Daten im Darknet auftauchten. Rund 1.000 PCs und Laptops mussten in den Verwaltungen „plattgemacht" werden, das heißt die Festplatten wurden von allen Daten bereinigt. Der erste Cyber-Katastrophenfall Deutschlands wurde ausgerufen, die Experten des BSI rückten an, ebenfalls die Bundeswehr, um beim Neuaufsetzen der Systeme zu helfen. Wochenlang waren die Verwaltungsstellen nur noch per Fax oder Telefon, jedoch nicht mehr elektronisch erreichbar. Banken und Sparkassen sprangen ein, um die Zahlung von Sozialhilfe, Unterhalts- und Wohngeld sicherzustellen. Noch heute ist die Wiederherstellung nicht vollständig abgeschlossen, da bei den vorhandenen Back-ups nicht ohne Weiteres davon ausgegangen werden konnte, dass sie nicht auch schon mit Schad-Code befallen waren.
Angesichts der Schwere der Vorfälle in Schwerin, Anhalt-Bitterfeld und im nordrhein-westfälischen Witten, wo die Stadtverwaltung im Oktober 2021 ebenfalls von einem Cyber-Beutezug betroffen war, entsteht der Eindruck zunehmender Verwundbarkeit. Bedrückend daran: Nicht nur solche Gemeinden oder Kreise, die ihre IT „unter dem Schreibtisch" selbst betreiben, sind betroffen, sondern offenbar auch solche, die sich einem kommunalen IT-Dienstleister angeschlossen haben. Das BSI verweist auf die eigenen IT-Grundschutzprofile für Kommunen, eine Art Basis-Absicherung für Kommunalverwaltungen, in denen Mindestsicherheitsmaßnahmen beschrieben sind. Anscheinend sind jedoch selbst BSI-zertifizierte Rechenzentren wie in Schwerin nicht vor schwerwiegenden Cyber-Attacken gefeit. Lohnt am Ende eine ebenso aufwendige wie kostspielige Zertifizierung gar nicht? Und bedeutet eine Zentralisierung der IT besseren Schutz oder – umgekehrt – eine größere Angriffsfläche?

Schwächstes Glied der Sicherheitskette: der Mensch

„Ein Angriff auf einzelne Kommunalverwaltungen oder kommunale Unternehmen hätte in der heutigen digitalen Zeit wahrscheinlich weitaus größere Schäden und langfristigere Ausfälle nach sich gezogen", ist Matthias Effenberger überzeugt. „Insofern ist die Bündelung der kommunalen IT-Ressourcen auch weiterhin die richtige Entscheidung." Sachsens Datenschutzbeauftragter Andreas Schurig rät Kommunen, sich dringend auf den Ernstfall vorzubereiten. Eine konsequente Datensicherung, ein systematischer Update- und Patch-Service, eine straff konfigurierte Firewall, Notfallpläne und Reservetechnik gehören zu den Präventionsmaßnahmen.
Aber auch Weiterbildungen für IT-Verantwortliche und Schulungen für das Personal. Neben dem Ausnutzen von Sicherheitslücken in Netzwerken und Fehlkonfigurationen der Systeme gelangen Angreifer immer noch sehr häufig über Standard-Anmeldeinformationen, allzu leichte Passwörter und unvorsichtige Mitarbeiter an die begehrten Daten. Insbesondere durch den Wechsel ins Homeoffice im Zuge der Corona-Pandemie hätten sich Kriminelle auf das schwächste Glied der Sicherheitskette, den Menschen, konzentriert, stellt eine Bitkom-Studie fest.
Darüber hinaus gilt es aber auch, die politische Awareness zu erhöhen. Die IT-Sicherheit in Kommunen ist längst nicht so gut aufgestellt, wie die des Bundes oder der Länder. Vor die Wahl gestellt, die Schultoiletten zu sanieren oder in IT-Sicherheit zu investieren, fällt vielen Bürgermeistern und Ratsmitgliedern die Entscheidung nicht schwer. Anders als marode Toiletten fällt eine diffuse Bedrohung aus dem Cyber-Raum weniger stark ins Auge. Diese Sichtweise muss sich ändern und den Kommunen genügend Gelder zur Verfügung gestellt werden, damit sie sich besser schützen können. Denn eins zeigen die Fälle auch: Die Kehrseite der zunehmenden Digitalisierung ist eine größere Verwundbarkeit insbesondere in Kommunen, wo sich die Zahl der Schnittstellen nach außen ständig erhöht.

()

Dieser Beitrag ist im Titel der Ausgabe Januar 2022 von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Cyber-Attacken