Dataport

Prävention und Gefahrenabwehr

[10.02.2022] Die Cyber-Attacken auf Kommunen nehmen seit Jahren zu. Beim „Digital News Club“, einer neuen virtuellen Veranstaltungsreihe des IT-Dienstleisters Dataport, standen am Mittwoch die aktuellen Entwicklungen in der Cyber-Kriminalität in Deutschland zur Debatte.

Im Februar 2016 wurde die Stadtverwaltung Dettelbach in Bayern mit einem Trojaner infiziert und aufgefordert, ein Lösegeld in Höhe von 1,3 Bitcoin zu zahlen. Das waren damals 500 Euro, wären im November 2021 jedoch annähernd 70.000 Euro gewesen. Im selben Jahr fällt die Stadt Rheine einem Cyber-Angriff zum Opfer, der die gesamte Stadtverwaltung lahmlegt. 2017 betraf es die Netzinfrastruktur im Landtag von Sachsen-Anhalt. 2018 kam es zu einem Angriff auf die Anmeldeserver des Landesamtes für Besoldung und Versorgung in Fellbach, ebenfalls 2018 infizierte sich die Stadtverwaltung von Bad Homburg mit dem Emotet-Trojaner. Im Jahr 2020 betraf es die Landeshauptstadt Brandenburg und das Stahnsdorfer Rathaus, bevor dann 2021 Wackersdorf, Bitterfeld, Schwerin und Pirmasens folgten. Wie die Abteilungsleiterin Haya Shulman vom Fraunhofer-Institut für Sichere Informationstechnologie (SIT) berichtet, stellen diese Beispiele ein großes Problem für die weitere Digitalisierung der Kommunen dar. Die Angreifer sind bandenmäßig organisiert und nennen sich Revil, Avaddon, Conti oder Darkside. Sie agieren wie richtige Firmen mit Partnernetzwerken, Herstellern, Verkäufern und sogar Callcenter für den Support. Und sie sind international aufgestellt und damit schwer zu fassen. Carsten Meywirth, Leiter der Abteilung Cybercrime beim Bundeskriminalamt (BKA), erkennt darin eine „Underground-Economy“, die hochgradig professionell agiert und Schadprogramme wie Software als Franchise-Produkte vertreibt. Der Polizeistatistik zufolge hat sich die Zahl der Cyber-Straftaten seit 2015 verdoppelt, wobei ein sehr großes Dunkelfeld existiert. Nur jede zehnte Straftat in diesem Bereich wird zur Anzeige gebracht. Der Schaden allein durch Ransomware betrug 24,3 Milliarden Euro im Jahr 2021, zwei Jahre zuvor waren es noch etwas mehr als fünf Milliarden Euro. Für Meywirth gab die Corona-Pandemie den Startschuss: „Cyberkriminelle haben die Situation für sich adaptiert. Und auch nach der Pandemie wird das, was wir jetzt erleben, das neue Normal sein.“

Verwundbare Infrastrukturen

Warum trifft es vermehrt Kommunen? Darauf haben die Experten keine eindeutige Antwort. Man sollte meinen, dass bei Kommunen nicht das meiste Lösegeld zu holen ist. Allerdings ist dies auch schon Teil des Problems: Viele Kommunen sitzen auf völlig veralteten IT-Systemen, was sowohl die Hardware als auch die Software anbelangt. „Die Architekturen sind oft so verwundbar, dass man sie gar nicht mehr patchen kann“, sagt Haya Shulman. Das Budget für IT-Sicherheit ist, falls überhaupt vorhanden, äußerst niedrig. Zudem mangelt es an Expertise, die erst eingekauft werden müsste. Hier konkurrieren auch wohlhabende Kommunen mit der Privatwirtschaft, die meist bessere Gehälter und Honorare zahlt.
Ein weiterer Teil des Problems sind fehlende bundesweite einheitliche Vorgaben für die IT-Sicherheit. Teilweise gebe es länderbezogene Vorgaben, die sich etwa aus der Datenschutz-Grundverordnung ableiten, doch auch die seien „oft rudimentärer Natur“, berichtet Christian Stuffrein, Referent für Digitalisierung beim Deutschen Landkreistag. Die Länder scheuen die finanzielle Belastung, wenn sie ein hohes Sicherheitsniveau festlegen. Immerhin haben sich die Kommunalen Spitzenverbände zusammen mit IT-Dienstleistern und IT-Sicherheitsexperten aus Kommunen für ein IT-Grundschutzprofil Basisabsicherung starkgemacht, das man aber im Vergleich zu anderen IT-Sicherheitsstandards des

Bundesamtes für Sicherheit in der Informationstechnik (BSI) nicht anders als rudimentär bezeichnen kann. Noch nicht einmal eine Meldepflicht für den kommunalen Raum ist vorgeschrieben, sodass sich auch kein Lagebild bestimmen lässt, zu welchem Zeitpunkt sich wo welche Vorfälle zugetragen haben.

IT-Sicherheit hat noch nicht erforderliche Priorität

Festzustellen ist, dass das Thema IT-Sicherheit offenbar auf der Leitungsebene noch nicht die erforderliche Priorität eingenommen hat, sonst würde es nicht zu so vielen Vorfällen kommen. Die nötigen Maßnahmen sind bekannt: Verantwortliche benennen, Prozesse definieren, Situationen einüben, ein kontinuierliches Sicherheitsmonitoring betreiben und immer wieder die Systeme mittels Backups, Patches und Updates auf dem aktuellen Stand halten. Kleine Kommunen sind damit überfordert. Bei 30 bis 40 Arbeitsplätzen entfällt dort oftmals nur eine halbe Stelle auf die IT. Uwe Störmer, Leiter Kommunale Infrastrukturen bei dataport.kommunal, berichtete vom Pilotprojekt „dITBetrieb“ im Kreis Steinburg, bei dem sich vier Ämter aus Schleswig Holstein zusammentun wollten, um die IT gemeinsam zu betreiben. Das Pilotprojekt entwickelte sich zu einem Konsolidierungsprojekt, an dessen Ende die Gesamtverantwortung für die IT an Dataport überging, die strategischen Entscheidungen aber weiterhin bei den Ämtern verblieben.
Solche Konsolidierungsprojekte, wie es sie nicht nur in Norddeutschland gibt, sind wohl das Mindeste, was Kommunen unternehmen sollten, um der verspäteten Erkenntnis, dass IT-Sicherheit erst im Ernstfall wertvoll ist, vorauszugreifen. Darüber hinaus könnten sich aus dieser Erkenntnis auch politische Folgerungen ergeben: beispielsweise die Einstufung von Kommunen als Kritische Infrastruktur und ein BSI-Grundschutz als bundeseinheitlicher Standard. Doch so weit sind wir wohl noch nicht.

()

Stichwörter: IT-Sicherheit, Digital News Club