Märkischer Kreis

IT-Sicherheitskonzept in der Praxis

[15.09.2023] Die Cyber-Sicherheitslage bleibt angespannt. Und immer öfter ist der Public Sector von Angriffen betroffen. Dies belegen aktuelle Studien ebenso wie die Fälle der jüngsten Zeit. Wie sich eine Verwaltung – bisher erfolgreich – absichern kann, zeigt beispielhaft der Märkische Kreis.

Im Märkischen Kreis in Südwestfalen trat der Ausschuss für Digitalisierung und E-Government zusammen, um den aktuellen Bericht zur IT-Sicherheitslage zu erörtern. „Aktuell ist die Kreisverwaltung sehr gut durch unsere Systeme vor Cyber-Angriffen geschützt. Eine Ausschreibung für die kommende Generation von Firewalls bereiten wir aber bereits vor“, so der Fachdienstleiter Digitalisierung und IT, Andreas Lüsebrink. Dennoch sei eine kontinuierliche Anpassung aller Sicherheitssysteme und Software an die aktuelle Gefahrenlage eine dringende Aufgabe der Kommunen, wie der IT-Sicherheitsbeauftragte Sören Hendrich darstellte. Hendrich verwies auf den Bericht des Bundesamts für Sicherheit in der Informationstechnik (BSI), wonach sich in Deutschland die bisher schon angespannte Lage in der IT-Sicherheit im Jahr 2022 weiter zuspitzte (wir berichteten). Zwar stünden insbesondere Großkonzerne im Fokus der Cyber-Kriminellen. Doch dass es auch Verwaltungen treffe, die zur wesentlichen Infrastruktur gezählt werden, zeigten jüngste Vorfälle. Als Beispiel nannte Hendrich den Kreis Anhalt-Bitterfeld, der 2022 als erster digitaler Katastrophenfall in Deutschland Schlagzeilen machte. 207 Tage konnten nach einem Ransomware-Angriff kein Elterngeld, kein Arbeitslosen- und Sozialgeld ausgezahlt werden. Auch Kfz-Anmeldungen und andere bürgernahe Dienstleistungen konnten nicht erbracht werden. In der Nachbarschaft des Märkischen Kreises wurde im Oktober 2022 die Stadt Witten Opfer von IT-Angriffen (wir berichteten). Weitere prominente Beispiele sind der Rhein-Pfalz-Kreis (wir berichteten) und die brandenburgische Landeshauptstadt Potsdam (wir berichteten).
Die Hauptbedrohung gehe von Erpresser-Software aus, so genannter Ransomware, resümierte Hendrich. Zunehmend wurden auch Schwachstellen in Software-Produkten ausgenutzt. Eine Zunahme sei zudem bei den Angriffen auf Perimeter-Systeme wie zum Beispiel Firewalls oder Router zu beobachten. Hinzu kamen verschiedene Bedrohungen im Zusammenhang mit dem russischen Angriffskrieg auf die Ukraine, zum Beispiel durch Hacktivismus und Kollateralschäden bei Cyber-Sabotage-Angriffen im Rahmen des Krieges.

Zahlreiche Normen und Auflagen

Konkret betroffen war die Verwaltung des Märkischen Kreises insbesondere durch die Schwachstellen in den Software-Paketen von Microsoft sowie dem Java-Framework Log4j, da sich diese in vielen Software-Bausteinen befand und eine große Angriffsfläche bot. 284 Aufträge zur kontinuierlichen Sicherheitsanpassung bearbeitete die IT der Kreisverwaltung in diesem Zusammenhang von Mai 2022 bis heute. Zudem musste das Antivirensystem des russischen Anbieters Kaspersky von einem anderen Sicherheitssystem abgelöst werden. Das BSI hatte im März 2022 vor dem Einsatz dieser Virenschutz-Software gewarnt.
Damit war die To-Do-Liste für die IT-Sicherheit aber noch lange nicht abgearbeitet, wie Hendrich darstellte. So setze das IT-Team der Kreisverwaltung das Informationssicherheits-Management-System (ISMS) nach dem IT-Grundschutzprofil des BSI konsequent um. Zudem treibt der Kreis auf Grundlage des IT-Sicherheitskonzepts Öffentlicher Gesundheitsdienste (ÖGD) auch die Digitalisierung des Gesundheitsamts weiter voran. Für Betreiber Kritischer Infrastrukturen (KRITIS) legt darüber hinaus die NIS2-Richtlinie

Cyber Security weitere Mindeststandards in der EU fest, die es umzusetzen gilt. Bis 2024 müssen EU-Mitgliedsstaaten NIS2 in lokale Gesetzgebung überführen und nationale Betreiber mit Cybersecurity regulieren. Das Rechnungsprüfungsamt fordert in seinem Bericht vom Mai 2023 unter anderem die Erstellung eines Notfallhandbuchs und die Einstellung eines Notfallbeauftragten bis Oktober 2024.
Im Märkischen Kreis gibt es trotz der zahlreichen zu erfüllenden Verpflichtungen und Aufgaben zunächst eine gute Nachricht: Für die Umsetzung der bisherigen IT-Sicherheitsmaßnahmen stellt der Bericht des Gemeinde-Prüfungsamts 2022/23 den Kommunen ein gutes Zeugnis aus und bestätigt einen Erfüllungsgrad von 85,6 Prozent.
Das IT-Sicherheitskonzept der Kreisverwaltung nimmt nicht nur die technischen Komponenten in den Blick. Auch die Sensibilisierung der Beschäftigten beim Märkischen Kreis spielt eine zentrale Rolle, so finden etwa Schulungen von Auszubildenden, IT-Sicherheitstrainings und eine breite Informationsbereitstellung statt. Dabei rückt auch E-Learning immer mehr in den Vordergrund.

(sib)

Stichwörter: IT-Sicherheit, Märkischer Kreis, BSI, Grundschutz, KRITIS, NIS2