IT-Sicherheit

Interkommunales Konzept

[22.06.2017] Die Kommunale ADV-Anwendergemeinschaft West (KAAW) unterstützt ihre 39 Mitgliedskommunen bei der Erstellung eines individuellen IT-Sicherheitskonzepts. Der Zweckverband hat dafür eine eigene Vorgehensweise auf Basis des BSI-Grundschutzes entwickelt.

Mit der Digitalisierung sowie der Etablierung neuer E-Government-Prozesse nimmt auch die Computer-Kriminalität zu. Im Jahr 2016 zeigte sich die erhöhte Bedrohungslage auch im kommunalen Sektor. Zum Schutz der Daten sind hinreichende technische und organisatorische Maßnahmen festzulegen. Kommunen in Nordrhein-Westfalen müssen diese laut § 10 Absatz 2 und 3 Landesdatenschutzgesetz verpflichtend in einem dokumentierenden Sicherheitskonzept ermitteln. Dieses beschreibt die geplante Vorgehensweise zur Umsetzung jeder einzelnen Maßnahme und ist das zentrale Dokument im Sicherheitsprozess einer Behörde. Der Zweckverband Kommunale ADV-Anwendergemeinschaft West (KAAW) unterstützt seine 39 Mitgliedskommunen im Westmünsterland seit dem Jahr 2012 dabei, diese Vorgaben praktisch zu erfüllen und hat dafür eine eigene Vorgehensweise auf Basis des IT-Grundschutzes des Bundesamts für Sicherheit in der Informationstechnik (BSI) definiert. In dem 2008 gegründeten Zweckverband KAAW werden die IT-Systeme vor Ort in den Mitgliedskommunen autonom betrieben. Das stellt eine besondere Herausforderung dar, weil die IT-Sicherheitskonzepte jeweils individuell pro Kommune erstellt werden müssen. Dieser Herausforderung nimmt sich das KAAW-Team „Shared Service Center IT-Sicherheitsberatung/Datenschutz“, bestehend aus zwei Sicherheitsberatern und einem behördlichen Datenschutzbeauftragten, an. Der interkommunale, aber dennoch individuelle Weg zum eigenen Sicherheitskonzept wird dabei kontinuierlich gemäß dem PDCA-Zyklus (Plan, Do, Check, Act) verbessert. Die geplanten Maßnahmen werden bewertet und je nach Priorität und Aufwand durch die IT-Verantwortlichen in den Kommunen umgesetzt. Darauf aufbauend werden die Wirksamkeit und Effizienz der umgesetzten Verbesserungsmaßnahmen festgestellt und analysiert. Basierend auf den Analyseergebnissen werden weitere Verbesserungsmaßnahmen geplant und der Prozess beginnt von Neuem.

Basis-Check als Grundlage

Der KAAW-Basissicherheits-Check (BSC) und die daraus resultierende Risikobewertung bilden die Grundlage eines jeden Sicherheitskonzepts. In einem Abstimmungstermin zwischen Mitarbeitern der KAAW und der Mitgliedskommune hält der Sicherheitsberater die aktuellen Gegebenheiten fest. Dazu wird der Ist-Zustand zur Informationssicherheit mittels eines auf die Kommunen angepassten BSC durchgeführt. Dabei werden zwölf Themenkomplexe – Organisation, Personal, Server-Raum, Datenschutz, Dokumentation/Notfallvorsorge, Server- und Client-Umgebung, Datensicherung, Infrastruktur allgemein, Gebäude, E-Mail sowie WLAN/mobile Clients – durch die Beantwortung von mehr als 150 Fragen analysiert. Der Basissicherheits-Check des Zweckverbands KAAW wird mindestens einmal jährlich im Rahmen einer IT-Sicherheitsstrategietagung aktualisiert und liegt mittlerweile in Version 4.0 vor. Zudem wird er regelmäßig mit den Aufsichtsbehörden, in diesem Fall der Gemeindeprüfungsanstalt NRW, oder Fachexperten abgestimmt, um neue Bedrohungslagen und gesetzliche Änderungen zu berücksichtigen. Bislang wurde der KAAW-Basissicherheits-Check mehr als 40-mal durchgeführt und erprobt. Empfohlen wird, einen solchen Check alle zwei bis drei Jahre zu wiederholen.
Die aus dem BSC gewonnenen Erkenntnisse werden anschließend durch den KAAW-Sicherheitsberater

nach Priorität, dem Aufwand zur Umsetzung empfohlener Maßnahmen sowie den dazugehörigen Kosten bewertet. Die Schätzungen zu Aufwendungen (eigener Ressourceneinsatz) und externen Kosten basieren auf Erfahrungswerten der IT-Sicherheitsbeauftragten, die in ihrer Hauptfunktion Mitarbeiter in den IT-Abteilungen der Mitgliedskommunen sind. Durch diese Prognosewerte sollen IT-Verantwortliche und Hauptverwaltungsbeamte einer Kommune einen ersten Eindruck erhalten, welche Maßnahmen mit wenig Aufwand umzusetzen sind, um die IT-Sicherheit kurzfristig zu erhöhen.

Konzept wird dokumentiert

Entscheidend für die Wahrnehmung und Gestaltung des eigenen Sicherheitskonzepts sowie für das aktive Risiko-Management in der betreffenden Kommune ist das auf den Basissicherheits-Check folgende Sensibilisierungsgespräch, an dem Verwaltungsvorstand, IT-Fachverantwortlicher, IT-Sicherheits- sowie Datenschutzbeauftragter der Kommune, Kämmerer und KAAW-Sicherheitsberater teilnehmen sollten. Eine 100-prozentige IT-Sicherheit kann nie gewährleistet werden – umso wichtiger ist es, sich mit dem Risiko-Management auseinanderzusetzen, die Gefahren einzuschätzen, zu bewerten und das Restrisiko festzulegen und zu tragen. Nach der Analyse der Risiken sind unter Umständen Sofortmaßnahmen einzuleiten, aber auch mittelfristige Maßnahmen zur generellen Risikominimierung in den IT-Strategieplan sowie die Haushaltsplanung einzubringen. Die bereits umgesetzten und noch umzusetzenden Maßnahmen sind in einem dokumentierenden Sicherheitskonzept festzuhalten.
Zur Verbesserung der Kontrollmöglichkeiten übergibt die KAAW jeder Kommune einen einheitlichen IT-Sicherheits- und Datenschutzordner. Dabei soll unter anderem das Inhaltsverzeichnis – bestehend aus Sicherheitsleitlinie, Sicherheits- und Notfallvorsorgekonzept, Risikoliste, Notfallhandbuch, Wiederanlaufhandbüchern, Datensicherungskonzept, Verfahrensverzeichnissen, Auftragsdatenverarbeitungsverträgen, Dienstanweisungen sowie dem letzten KAAW Sicherheits- und Datenschutzcheck – bei der Etablierung der IT-Sicherheit unterstützen. Der Ordner wird von einem IT-Sicherheitsberater im Rahmen der Durchführung des BSC auf Vollständigkeit und Korrektheit geprüft. Sofern gewünscht, erstellt die KAAW ein Empfehlungsschreiben an den jeweiligen Verwaltungsvorstand, das bestätigt, dass die Inhalte den Vorgaben des Landesdatenschutzgesetzes NRW entsprechen und die notwendigen Freigaben – zum Beispiel der IT-Sicherheitsleitlinie – erfolgen sollten.
Abschließend bleibt festzuhalten, dass ein dokumentierendes IT-Sicherheitskonzept nur so gut und aktuell ist, wie es in der Kommune gepflegt wird. Es bildet ein wichtiges Instrument zur Sensibilisierung aller Mitarbeiter in der Verwaltung und dient zusätzlich der IT-Budget- und Maßnahmenplanung.

()

Dieser Beitrag ist in der Juni-Ausgabe von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Kommunale ADV-Anwendergemeinschaft West (KAAW)