IT-Sicherheit

Gut gewappnet

[21.09.2015] Für Behörden empfiehlt sich ein hohes Sicherheitsniveau gemäß BSI-Grundschutz oder ISO-27001-Standard. IT-Security muss als kontinuierlicher Management-Prozess mit den Hauptkomponenten Analyse, Planung, Umsetzung und Revision betrachtet werden.

Nicht nur der ständig wachsende IT-Einfluss auf die Verwaltungsprozesse erfordert neue Sicherheitsmaßnahmen. Auch die Gefahren der wachsenden Cyber-Kriminalität oder gesetzliche Anforderungen und Richtlinien zwingen dazu, angemessene Standards einzuführen. Neben potenziellen Angriffen von außen, ergeben sich weitere Sicherheitsrisiken unter anderem aus dem digitalisierten Datenaustausch mit Bürgern sowie Unternehmen. Wie aktuelle prominente Beispiele – etwa der Angriff auf das IT-System des Bundestags – zeigen, werden sich Einrichtungen des Themas manchmal erst bewusst, wenn sie von Sicherheitsvorfällen direkt betroffen sind. Spätestens dann müssen sie feststellen, dass der Schutz der IT-Systeme besser organisiert werden muss.

Diszipliniertes Vorgehen nach Plan

Besonderes Augenmerk sollte auf der Verarbeitung personenbezogener Daten sowie der Gefahr von Datenverlusten und -missbrauch liegen. Hier kommt zusätzlich das Bundesdatenschutzgesetz, perspektivisch die EU-Datenschutzgrundverordnung zur Anwendung. Um die speziellen Anforderungen aus dem IT-Sicherheitsgesetz zu erfüllen, sind Zertifizierungen nach dem Grundschutz, DIN ISO 27001 des Bundesamts für Sicherheit in der Informationstechnik (BSI) notwendig. Noch ist die genaue Definition der so genannten Betreiber kritischer Infrastrukturen im Detail nicht getroffen. Trotzdem lässt sich aus der übergeordneten Festlegung in öffentliche Einrichtungen, Energieversorger und Gesundheitswesen eine erste Indikation treffen. Selbst dann, wenn eine direkte Zertifizierung nicht notwendig erscheint, ist für eine hohe IT-Sicherheit ein Vorgehen nach den genannten Sicherheitsstandards sinnvoll. Um geeignete und vor allem sinnvolle Maßnahmen zur Verbesserung der IT-Sicherheit ergreifen zu können, sind zunächst die Schutzziele in den Teilbereichen Verfügbarkeit, Authentizität, Vertraulichkeit sowie Integrität zu bestimmen. Die eingesetzten IT-Systeme und Dienste müssen daraufhin analysiert, der Schutzbedarf festgestellt sowie notwendige Maßnahmen abgeleitet werden. Der erreichte Stand ist zu dokumentieren und kontinuierlich fortzuschreiben. Dieser Prozess der Analyse, Planung, Umsetzung und Revision lässt sich als Informationssicherheits-Management-System (ISMS) beschreiben. Um dieses Kontinuum in Gang zu setzen, bedarf es eines Projekts zur Einführung von IT-Sicherheitsstandards und einer disziplinierten Dokumentation. Generell gilt: Wer gut dokumentiert, ist auch beim Thema IT-Sicherheit auf dem richtigen Weg. Nur so lässt sich aus zuvor erhobenen und dokumentierten Richtlinien und Konfigurationsdaten eine IT-Sicherheitsrichtlinie und ein Sicherheitskonzept erstellen.

Umsetzung nach Standards ist ratsam

Bei der Erarbeitung und schrittweisen Einführung der IT-Sicherheitsrichtlinie gemäß BSI- oder ISO-Vorgaben müssen bestehende Prozesse geprüft und eingebunden werden. Zum Handwerkszeug gehört es, vorhandene Dokumente wie Rechte-Rollen-Konzepte oder Handbücher zu sichten. Analysierte Komponenten müssen sich im Dokumentationswerkzeug erfassen lassen. Neben den notwendigen Maßnahmen für das erforderliche Sicherheitsniveau, muss der gesamte Verbund der eingesetzten IT-

Systeme elektronisch modelliert werden. Damit ist die Basis für die Dokumentation der Betriebsumgebung und die Modellierung von IT-Service-Management-Daten geschaffen. Durch die elektronische Verfügbarkeit des Informationssicherheits-Management-Systems können verantwortliche Mitarbeiter – vom Administrator bis zum IT-Sicherheitsverantwortlichen – den aktuellen Stand ihres Informationsverbunds ständig überwachen. Sie können auf veränderte Rahmenbedingungen, unerwartete Sicherheitsvorfälle oder auf bisher unbekannte Gefährdungen schnell und flexibel reagieren. Unabhängig von der Notwendigkeit einer Zertifizierung ist eine hohe Informationssicherheit für Einrichtungen des öffentlichen Dienstes nach den Standards ISO-27001 oder BSI-Grundschutz anzuraten. Die IT-Sicherheit ist als fortlaufender Prozess zu betrachten, der sowohl durch geeignete Werkzeuge als auch organisatorisch gemanagt werden muss. Eine seriöse Betrachtung des Gesamtaufwands ist nur nach einer erfolgten Erstanalyse möglich. Sinnvoll ist diese, wenn die Balance zwischen sicherheitsrelevanten Vorgaben und reibungslosen Verwaltungsprozessen im täglichen IT-Betrieb gewahrt bleibt. Der Anwender gestaltet diesen Prozess also mit.

()

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

Stichwörter: IT-Sicherheit, ISMS, Datenschutz