IT-Sicherheit

Schrittweise umsetzen

[13.01.2014] IT-Sicherheit setzt Vertraulichkeit, Verfügbarkeit und Integrität voraus – auch in der kommunalen Verwaltung. Um ein entsprechendes Konzept ins Rollen zu bringen, hilft der Einsatz eines IT-Sicherheitsbeauftragten.

Kommunen sollen Daten zur Verfügung stellen und zugleich schützen, Verwaltung und Bürger verbinden und wo notwendig, auch trennen. IT-Sicherheit wird in der Kommunalverwaltung jeden Tag im wahrsten Sinne des Wortes erlebt. Dabei ist es heute wichtiger denn je, den Bürgern glaubwürdig zu vermitteln, dass ihre Daten vor Dritten geschützt sind (Vertraulichkeit), dass sie Service in Anspruch nehmen können, wenn sie ihn benötigen (Verfügbarkeit), und dass die Daten korrekt sind (Integrität).
An Warnungen vor Cyber-Kriminalität mangelt es nicht. Der Präfix Cyber ist zum Schlagwort für IT-Sicherheit geworden, obwohl er sich in erster Linie auf Internet-Technologien bezieht. Die Gefährdungen und Wahrnehmungen im kommunalen Alltag stellen sich aber ganz anders dar und der Cyberspace ist eine eher abstrakte Bedrohung. Die Faktoren Irrtum und Nachlässigkeit eigener Mitarbeiter hingegen haben in Fachkreisen eine viel höhere Bedeutung. Daneben sind Software-Mängel, unbefugte Kenntnisnahme und eine schlechte Dokumentation wenig beachtete, aber reale Gefährdungen. Die Vorgehensweise nach IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist eine gute Grundlage, um einen normalen und hohen Schutzbedarf von Informationen abzusichern. IT-Grundschutz ist in der öffentlichen Verwaltung auf Bundes- und Landesebene seit Jahren der Standard für IT-Sicherheit. Er bietet auch für Kommunen eine gute Ausgangsbasis. Man sollte IT-Grundschutz aber als eine Methode verstehen, bei der man die lokalen Besonderheiten einer Kommune beachten muss.
Im April 2013 hat der IT-Planungsrat eine Leitlinie für Informationssicherheit beschlossen, welche die Einführung und Aufrechterhaltung von IT-Grundschutzstandards nach dem BSI vorgibt. Die Leitlinie ist für Bund und Länder verbindlich, den Kommunen wird die Anwendung jedoch nur empfohlen. Eine vermeintliche Wahlfreiheit mit Nebenwirkungen, denn bei ebenenübergreifenden Verfahren können nach dieser Leitlinie auch für Kommunen wieder IT-Sicherheitsstandards auf Basis von IT-Grundschutz festgelegt werden. Beim Nationalen Waffenregister war dies bereits der Fall.

IT-Sicherheitsbeauftragten bestellen

Für die Initiierung eines Sicherheitsprozesses ist es wichtig, die Rolle des IT-Sicherheitsbeauftragten zu vergeben, damit das Thema ein Gesicht bekommt. IT-Sicherheitsbeauftragte sollten in erster Linie Diplomaten sein, Zertifikate und Abschlussurkunden sind vorab wenig hilfreich. Gefragt sind vielmehr Kommunikationsfähigkeit, Menschenkenntnis und Sozialkompetenz, denn IT-Sicherheit im Mikrokosmos einer Kommunalverwaltung ist viel mehr ein psychologisches Thema, als es zunächst den Anschein hat. Die Einrichtung einer Stabsstelle gestaltet sich im kommunalen Umfeld häufig schwierig, zumal die Tätigkeit oft nur mit einem Zeitanteil ausgeübt wird. Denkbar ist eine Kombination mit der Aufgabe des behördlichen Datenschutzbeauftragten, wenn dies das jeweilige Landesdatenschutzgesetz zulässt. Ist eine weisungsfreie Ausprägung nicht möglich, hilft es, die Funktion bei der Bestellung mit Sonderrechten, wie beispielsweise einem direkten Vortragsrecht beim Bürgermeister, auszustatten. Es muss aber klar sein: Der IT-Sicherheitsbeauftragte hat zwar die Aufgabe, das Thema voranzubringen und zu koordinieren, die Verantwortung für die IT-Sicherheit liegt aber letztlich weiterhin bei der Leitungsebene.
Kommunale IT-Sicherheitsverantwortliche stehen in einem Spannungsfeld zwischen einer Selbstverpflichtung zu IT-Grundschutz, gesetzlichen Anforderungen und den limitierten Ressourcen der

Verwaltung. Umso wichtiger wird es, Wissen, Erfahrungen und Informationen auf dieser Ebene zu bündeln und zielgerichtet zu vermitteln. Engagierte Beauftragte haben hierfür zusammen mit dem Deutschen Landkreistag ein geschlossenes Internet-Forum zum Informations- und Erfahrungsaustausch aufgebaut (IT-SiBe-Forum.de).
Um sämtliche übergreifende Belange der Informationssicherheit innerhalb einer Behörde einzubeziehen und um IT-Sicherheitsbeauftragte zu unterstützen, ist die Einrichtung einer ständigen Arbeitsgruppe empfehlenswert. Neben IT-Sicherheits- und Datenschutzbeauftragten, IT-Verantwortlichen und Vertretern der Anwender sollten auch Beschäftigte hinzugezogen werden, die nicht IT-affin sind, aber Erfahrung im „Lebensraum“ der Verwaltung mitbringen. Um in die ganze Breite einer Verwaltung zu wirken, ist es außerdem hilfreich, interdisziplinäre Sichtweisen auf die Themen zu bekommen.

Leitlinie für Informationssicherheit etablieren

Eine der ersten Aufgaben der Arbeitsgruppe kann das Erstellen einer Leitlinie für Informationssicherheit sein. Diese beschreibt, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit hergestellt werden soll. Sie beinhaltet die angestrebten Ziele sowie die verfolgte Strategie. Über die Sicherheitsziele beschreibt sie auch das angestrebte Sicherheitsniveau in der Verwaltung. Sie ist somit Anspruch und Aussage zugleich, dass dieses Niveau auf allen Ebenen erreicht werden soll. Zugleich kann eine solche Leitlinie aber auch klarstellen, dass die erforderlichen Ressourcen und Investitionsmittel für die Umsetzung von Maßnahmen nur im Rahmen der zur Verfügung stehenden Haushaltsmittel möglich sind. Es ist sinnvoll, mit der Leitlinie auch Definitionen von Schutzbedarfskategorien festzusetzen – normal, hoch und sehr hoch. In der Regel hat ein höherer Schutzbedarf einen höheren Aufwand an Sicherheitsmaßnahmen und höhere Kosten zur Folge.
Bei der Planung und Umsetzung ist ein Leitgedanke hilfreich: Wesentlichkeit geht vor Vollständigkeit. Es muss kein IT-Sicherheitskonzept für die gesamte Verwaltung auf einmal erstellt und nicht alle Geschäftsprozesse müssen betrachtet werden. Es kann viel zielführender sein, die Ämter selbst entscheiden zu lassen, für welche Bereiche sie dies für notwendig erachten. Das überrollt sie einerseits nicht, entlässt sie aber auch nicht aus der Verantwortung. Wenn nur für ein bis drei Prozesse in jedem Amt ein Sicherheitskonzept erstellt und umgesetzt wird, erzielt dies bereits einen hohen Wirkungsgrad in der Gesamtverwaltung. So kann das Sicherheitsniveau schrittweise erhöht und aufrechterhalten werden. IT-Sicherheit ist ein Prozess, kein Projekt.

()

Dieser Beitrag ist in der Januar-Ausgabe von Kommune21 im Schwerpunkt IT-Sicherheit erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Bundesamt für Sicherheit in der Informationstechnik (BSI), Kassel