Kommunale Wege zur IT-Sicherheit

IT-Sicherheit ist ein Prozess, kein Projekt

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) – das ist kommunale IT-Sicherheit.

Von Jens Lange, Kassel

Trügerische Gefährdungen

An Warnungen vor Cyber-Kriminalität mangelt es nicht und Initiativen zur Cyber-Sicherheit sind derzeit beliebte politische Projekte. Das Präfix *Cyber* ist zum Schlagwort für IT-Sicherheit geworden, obwohl es sich in erster Linie auf Internet-Technologien bezieht. Die Gefährdungen und Wahrnehmungen im kommunalen Alltag stellen sich aber oft ganz anders dar. Der Cyber-Raum ist eine abstrakte Bedrohung und gleicht eher einer Galaxie, die nie ein Mensch zuvor gesehen hat. Irrtum und Nachlässigkeit der eigenen Mitarbeiter haben hingegen eine viel höhere Bedeutung. Dies zeigen Analysen und Studien der letzten Jahre immer wieder. Daneben sind Software-Mängel, unbefugte Kenntnisnahme und eine schlechte Dokumentation wenig beachtete, aber reale Gefährdungen. Wenn sich Beschäftigte verdächtige E-Mails von zu Hause an die Arbeit schicken, da man diese dort „sicher“ öffnen kann, dann ist bei der Aufklärung zu E-Mail-Gefahren wohl etwas schief gelaufen. Auch die fatale Grundhaltung, für die IT-Sicherheit sei doch die IT-Abteilung zuständig, ist weit verbreitet. Technik allein schafft aber noch keine Sicherheit von Informationen. Dies in den Köpfen der Beschäftigten zu verankern, ist eine elementare Aufgabe. Datenbankname = Nutzername = Passwort? Was für jeden Computernutzer mit ein wenig Grundverständnis als Schwachstelle sofort erkennbar ist, findet sich selbst in etablierten Fachanwendungen als Kardinalfehler im Softwaredesign. Bei über 200 Fachanwendungen, die in einer Kommunalverwaltung laufen können, besteht ein weites Feld für versteckte Untiefen. Software-Mängel stehen beständig unter den Top 5 der Gefährdungen.

Bausteine zum Grundschutz

Haben Sie auch schon einmal überlegt, ob sich eine Kaskoversicherung für Ihr Auto wirklich lohnt – und haben Sie darauf eine klare Antwort gefunden? Nein? Alle, die einen Unfall hatten, wissen, dass es sich lohnt. Alle anderen wägen ab, zweifeln und rechnen, kommen aber zu keinem Ergebnis.

Risiken und die Eintrittswahrscheinlichkeit eines Schadens lassen sich in der Einzelbetrachtung einfach nicht voraussagen. Da ist es gut, wenn die Vorgehensweise des Bundesamts für Sicherheit in der Informationstechnik (BSI) nach IT-Grundschutz Risikoanalysen abnehmen kann. Aus den IT-Grundschutz-Katalogen lassen sich im Baukastenprinzip mit den zutreffenden Bausteinen die geeigneten Maßnahmen ermitteln, um einen normalen und hohen Schutzbedarf von Informationen abzusichern. IT-Grundschutz ist seit Jahren der Standard in der öffentlichen Verwaltung auf Bundes- und Landesebene. Er bietet auch für Kommunen eine gute Ausgangsbasis. Aber Achtung: Man sollte IT-Grundschutz als eine Methode verstehen, bei der man die lokalen Besonderheiten einer Kommune beachten sollte. Die Bausteine und die geforderten Maßnahmen sind kein Gesetz. Manche Maßnahmen lassen sich nur teilweise oder überhaupt nicht umsetzen. Andere wiederum sind entbehrlich, weil man nicht beschriebene Alternativen gefunden hat oder die Empfehlungen nicht relevant sind. In Einzelfällen – und das muss man ganz klar sagen – kann es für Kommunen auch notwendig sein, das Restrisiko zu tragen, wenn bestimmte Anforderungen nicht übertragbar sind.

Bislang gab es für Kommunen keine Verpflichtung, IT-Grundschutz oder vergleichbare Standards anzuwenden. Dies ändert sich zunehmend, wenn auch nicht immer gradlinig und zielführend. Auf Bund/Länderebene ist seit April 2010 der „IT-Planungsrat“ als zentrales Gremium für die föderale Zusammenarbeit in der Informationstechnik etabliert worden. Er wurde für eine verbindliche IT-Koordinierung von Bund, Ländern und Kommunen geschaffen. Im April 2013 hat der IT-Planungsrat eine Leitlinie für Informationssicherheit beschlossen, die die Einführung und Aufrechterhaltung von IT-Grundschutzstandards nach 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 (Bund/Länder/Kommunen) können die IT-Grundschutz-Standards auch für Kommunen festlegt werden. Beim Nationalen Waffenregister war dies als Vorgriff über ein eigenes Gesetz bereits der Fall. Bei anderen Verfahren dieser Art kann dies zukünftig durch die Leitlinie auch erfolgen. Die Orientierung an den IT-Grundschutz ist daher für Kommunen nicht nur sinnvoll, sondern auch geboten.

Im Angesicht der IT-Sicherheit

Die IT-Grundschutz-Vorgehensweise ist im BSI-Standard 100-2 beschrieben und als eine der ersten Maßnahmen für die Initiierung eines Sicherheitsprozesses ist es wichtig, die Rolle des IT-Sicherheitsbeauftragten zu vergeben. IT-Sicherheitsbeauftragte haben einen vielfältigen Aufgabenbereich. Sie beraten die Leitungsebene bei der Gestaltung der IT-Sicherheit und unterstützen sie bei der Umsetzung und Fortschreibung von Sicherheitsmaßnahmen. Sobald das Thema ein Gesicht bekommt, erhält es eine höhere Verbindlichkeit in der Wahrnehmung der Beteiligten. Für IT-Sicherheitsbeauftragte gibt es keine zwingenden Anforderungen zur Ernennung und keine geregelte Ausbildung. Sie sollten in erster Linie Diplomaten sein, denn gefragt sind Kommunikationsfähigkeit, Menschenkenntnis und Sozialkompetenz. IT-Sicher-

heit im Mikrokosmos einer Kommunalverwaltung ist viel mehr ein psychologisches Thema, als es zunächst den Anschein hat. Für eine Qualifizierung bietet sich der Fortbildungsgang „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung“ der Bundesakademie für öffentliche Verwaltung (BAköV) an. Im Rahmen einer „Sommerakademie“ kann dieser auch von Bediensteten der Kommunen in Anspruch genommen werden.

Nach den Vorgaben des BSI und dem Rollenbild, sollte der IT-Sicherheitsbeauftragte eine Stabsstelle innehaben. Die Einrichtung einer solchen Stabsstelle gestaltet sich im kommunalen Umfeld aber 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 z.B. 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. Umso wichtiger wird es, Wissen, Erfahrungen und Informationen auf dieser Ebene zu bündeln und zielgerichtet zu vermitteln. Engagierte IT-Sicherheitsbeauftragte haben hierfür zusammen mit dem Deutschen Landkreistag ein geschlossenes Internetforum zum Informations- und Erfahrungsaustausch aufgebaut (IT-SiBe-Forum.de). Hier werden Themen von aktuellen Ereignissen bis zu grundlegenden Konzepten diskutiert und Informationen darüber ausgetauscht. Eine Plattform für Neueinsteiger und Profis die kostenlos zur Verfügung steht.

Breitenwirkung im Team

Um sämtliche übergreifende Belange der Informationssicherheit innerhalb einer Behörde einzubeziehen und um IT-Sicherheitsbeauftragte zu unterstützen, ist die Einrichtung einer ständigen Arbeitsgruppe empfehlenswert. In der IT-Grundschutz-Vorgehensweise wird diese als das „IS-Management-Team“ bezeichnet. Neben IT-Sicherheits- und Datenschutzbeauftragten, IT-Verantwortlichen und Vertretern der Nutzer, sollten auch Beschäftigte hinzugezogen werden, die keine IT-Affinität besitzen, aber Erfahrung aus dem „Lebensraum“ der Verwaltung mitbringen. Um in die ganze Breite einer Verwaltung zu wirken, ist es außerdem hilfreich, interdisziplinäre Sichtweisen bei den Themen zu bekommen. Eine der ersten Aufgaben der Arbeitsgruppe kann das Erstellen einer „Leitlinie für Informationssicherheit“ sein.

Leitlinie als Richtlinie

Eine eigene „Leitlinie für Informationssicherheit“, in der Grundsätze, Ziele, Maßnahmen und Verantwortlichkeiten festgelegt werden, ist unentbehrlich. Der im IT-Grundschutz verwendete Begriff der „Leitlinie“ ist nicht ganz zutreffend, denn eine empfehlende Handlungsanweisung ohne bindenden Charakter reicht hierfür nicht aus. Besser ist da die Einordnung als eine Richtlinie, die im Sinne einer Verwaltungsvorschrift verwendet wird. Eine Richtlinie für Informationssicherheit beschreibt, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit hergestellt werden soll. Sie beinhaltet die angestrebten Informationssicherheitsziele sowie die verfolgte Sicherheitsstrategie. Über die Sicherheitsziele beschreibt sie damit auch das angestrebte Sicherheitsniveau in der Verwaltung. Sie ist somit Anspruch und Aussage zugleich, dass dieses Sicherheitsniveau auf allen Ebenen erreicht werden soll. Zugleich kann eine solche Richtlinie aber auch klarstellen, dass die erforderlichen Ressourcen und Investitionsmittel nur im Rahmen der zur Verfügung stehenden Haushaltsmittel möglich sind.

Es ist sinnvoll, mit der Richtlinie auch die Definitionen von Schutzbedarfskategorien anzugeben. Schutzbedarfskategorien helfen bei der Auswahl angemessener Sicherheitsmaßnahmen und sie orientieren sich an dem Ausmaß möglicher Schäden. Im IT-Grundschutz unterscheidet man die Schutzbedarfskategorien „normal, „hoch“ und „sehr hoch“. In der Regel hat ein höherer Schutzbedarf einen höheren Aufwand an Sicherheitsmaßnahmen und höheren Kosten zur Folge. Die Prozessverantwortlichen neigen bei einer Schutzbedarfsfeststellung jedoch oft zu einer höheren Bewertung, da die Höhe eines Schadens häufig nicht genau bestimmt werden kann. Überzogene Sicherheitsmaßnahmen können hier sogar zu weniger Sicherheit führen, wenn sie von den Beteiligten nicht mehr akzeptiert und umgesetzt werden. Um dem zu begegnen, sollten nachvollziehbare Kriterien für die Schutzbedarfskategorien bereits in der Richtlinie für Informationssicherheit festgelegt werden.

Wesentlichkeit geht vor Vollständigkeit

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 es müssen nicht alle Geschäftsprozesse betrachtet werden. Es kann viel zielführender sein, die Ämter selbst entscheiden zu lassen, für welche Bereiche sie IT-Sicherheitskonzepte für notwendig erachten. Ein Punkt, der durchaus in der Leitlinie festgeschrieben werden kann. Das überrollt die Ämter 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. Für alle Beteiligten ist es außerdem förderlich, zunächst einen übersichtlichen und handhabbaren Umfang anzugehen.

Die IT-Grundschutz-Methodik bietet zudem über die sog. „Qualifizierungsstufen“ A bis C einen weiteren Ansatz, schrittweise die IT-Sicherheit aufzubauen. Maßnahmen der Einstiegsstufe A sind essenziell für die Sicherheit innerhalb des betrachteten Bausteins und vorrangig umzusetzen, während Maßnahmen der Stufe C zeitlich nachrangig umsetzbar sind.

So kann das Sicherheitsniveau nach und nach erhöht und aufrechterhalten werden. IT-Sicherheit ist ein Prozess, kein Projekt.

IT-Sicherheit auf der Basis von IT-Grundschutz ist eine Chance und gleichzeitig eine Herausforderung für eine Kommunalverwaltung. Die Kosten des Nichtstuns sind jedoch weitaus höher als die Kosten des Handelns und man sollte sich um die eigene IT-Sicherheit kümmern, bevor es andere tun. □

Jens Lange, IT-Sicherheitsbeauftragter der Stadt Kassel