IT-Sicherheit

Risiken minimieren

[21.01.2016] Vom Deutschen Bundestag bis hin zum multinationalen Konzern: Kaum eine Institution ist heute vor den Angriffen von Cyber-Kriminellen gefeit. Das gilt auch für Kommunen und kommunale Unternehmen. Sie sind aber nicht schutzlos.

Es wird viel von IT-Sicherheit gesprochen in diesen Tagen. Die Sicherheit von E-Mail-Accounts, Internet- und E-Commerce-Auftritten, aber auch von kritischen Infrastrukturen gewinnt an Bedeutung. Spätestens seit den Hackerangriffen auf den Deutschen Bundestag im Sommer 2015 ist uns allen bewusst, dass Cyber-Kriminelle auch vor gut geschützten Institutionen nicht haltmachen. Doch Kommunen und kommunale Unternehmen sind dieser Bedrohung nicht schutzlos ausgeliefert. Vor Hackerangriffen von außen schützt eine Firewall, die von einem IT-Administrator stets auf dem aktuellsten Stand gehalten wird. Das größere Problem ist häufig in der eigenen Organisation zu finden. Ein mögliches Szenario ist die Unachtsamkeit: Der Sachbearbeiter nimmt von einem Bekannten einen USB-Stick mit den neuesten Hits mit ins Büro. Als Gratiszugabe beinhaltet der Datenträger aber auch eine Schad-Software, die sich unbemerkt im Netzwerk ausbreitet. Die Folgen: Vom Server-Ausfall bis zum anonymen, unberechtigten Zugriff auf Finanz- und Personendaten ist alles möglich. Aber auch der Vorsatz ist ein denkbares Szenario: Die öffentliche Verwaltung bietet viele Möglichkeiten, um auf dem elektronischen Weg, etwa per De-Mail, zu kommunizieren, Daten via ELSTER auszutauschen oder sich beispielsweise über Bürgerportale zu informieren. Schad-Software, die vorsätzlich in diese Systeme eingeschleust wird – beispielsweise durch einen entsprechend fingierten E-Mail-Anhang –, kann enorme Schäden anrichten. Beide Fälle zeigen, dass die IT-Sicherheit auch durch die Mitarbeiter bedroht ist. Für solche Szenarien müssen die Kommunen Vorkehrungen treffen und sie vor allem auch umsetzen. Hierbei helfen technische und organisatorische Maßnahmen, um die erkannten und gegebenenfalls bewerteten Risiken zu minimieren. Den Grundstein dafür legt ein so genanntes Informationssicherheitsmanagement-System (ISMS).

Technische und organisatorische Maßnahmen

Zu den technischen Maßnahmen zählen der Einsatz aktuellster Virenschutzprogramme, die Verwendung neuester Patches der Firewall, die regelmäßige Überprüfung durch so genannte Penetrationstests, die Umsetzung sicherer Programmieranforderungen und elektronische Zugangskontrollen zu sicherheitsrelevanten Bereichen. Organisatorische Maßnahmen sind wesentlich komplexer und betreffen letztendlich jeden Verwaltungsmitarbeiter, vom Auszubildenden bis zum Bürgermeister. Essenziell wichtig ist dabei die Kommunikation der Regeln und Maßnahmen. Denn was nützt die neueste Virenschutz-Software, wenn diese manuell am Arbeitsplatzrechner deaktiviert wurde? Wozu die Inbetriebnahme einer elektronisch personalisierten Zugangskontrolle, wenn dem freundlich grüßenden Handwerker die Tür zum Rechenzentrumsbereich aufgehalten wird, ohne Rückversicherung, dass er berechtigten Zutritt erhalten darf? Ein drittes Beispiel: PIN-Nummern auf Smartphones sind hilfreich und notwendig. Wenn aber der Abteilungsleiter, der die Regelung mit unterschrieben hat, diese bei seinem Gerät aus Bequemlichkeit heraus nicht nutzt, ist diese Maßnahme schlichtweg unwirksam. In der Regel ist der Datenschutzbeauftragte den meisten Mitarbeitern bekannt. Aber wer ist für die IT-Sicherheit der erste Ansprechpartner? Die Nennung eines Verantwortlichen sollte in der heutigen Zeit kein Problem mehr sein. Er benötigt aber auch die Chance, dass er Aufgaben mit der gebotenen Ernsthaftigkeit umsetzen kann. Dazu gehören Einsicht in die Abläufe, Weisungsbefugnis und ein direkter Draht zur Leitungsebene. Auch

die Bildung einer eigenen internen IT-Sicherheitsmarke kann dabei helfen, das Bewusstsein innerhalb der Verwaltung für das Thema zu steigern.

Sicherheit muss sich im Grundverständnis verankern

Diese Fakten machen deutlich, dass Deutschland einen enormen Aufholbedarf hat. In Bezug auf die Informations- und IT-Sicherheit ist die Bundesrepublik auf dem Stand eines Entwicklungslandes. Längst sind in anderen europäischen und asiatischen Ländern höhere Standards etabliert. Hier gilt es, alle Beteiligten für die Thematik zu sensibilisieren. Sicherheit, gerade im IT-Bereich, muss sich im Grundverständnis verankern. Die Verantwortung der kommunalen Verwaltung wird sich in diesem Zusammenhang signifikant erhöhen. Dies erfordern einerseits die Beteiligungsstrukturen an medizinischen Einrichtungen wie Krankenhäusern und Universitätskliniken, an Strom- und Wasserversorgungsunternehmen sowie an kommunalen Rechenzentren und Forschungsinstituten. Andererseits erfordert der eigene Verwaltungsapparat einen sicheren Umgang mit Daten. Es soll nicht unerwähnt bleiben, dass es bereits positive Ansätze aus kommunalen Beteiligungsunternehmen und öffentlichen Verwaltungen gibt. IT-Sicherheit führt dann zum Erfolg, wenn sich mehrere Partner zusammenschließen, gemeinschaftlich Lösungen erarbeiten und diese effizient umsetzen: Der Deutsche Städte- und Gemeindebund, der Deutsche Städtetag sowie der Deutsche Landkreistag haben gemeinsam mit der Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister, Vitako, bereits im Dezember 2014 in einer Arbeitsgruppe eine so genannte Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen erarbeitet. Dieses Papier stellt übersichtlich eine Vielzahl wichtiger Informationen zur Verfügung, um einen erfolgreichen Einstieg in die Thematik zu gewährleisten.

()

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

Stichwörter: IT-Sicherheit, Hackerangriffe, ISMS, Schad-Software, Virenschutz