Westoverledingen

Zu klein für echten Schutz?

[17.11.2015] In kleinen Kommunen kümmern sich Generalisten um die IT-Systeme. Um sie zielgerichtet gegen Gefahren abzusichern, fehlen häufig die Ressourcen. Wie kann die Sicherheit der IT-Infrastruktur trotzdem erhöht werden?

Eine gute IT arbeitet wie eine funktionierende Verdauung – man bemerkt sie erst, wenn etwas Wesentliches kaputt ist. Ernsthafter gesprochen: Die Informationstechnik einer Verwaltung gehört inzwischen zu einer Kritischen Infrastruktur, ähnlich wie die Strom- oder Telefonnetze. Welche Gefahren drohen dieser Infrastruktur? Einige Beispiele aus den schlechten Träumen eines IT-Leiters und den sich daraus ableitenden Fragen: Herausforderungen aus der alten Welt: Einbruch, Zerstörung – ist der Server-Raum sicher? Was ist nachts oder am Wochenende? Habe ich Zugangskontrollen? Weiß ich, wer wann im Server-Raum war? Läuft die Klimaanlage? Läuft sie zu gut und die Server frieren ein? Läuft sie zu schlecht und die Server sterben den Hitzetod? Herausforderungen aus der neuen Welt: Social Hacking – wurden Passwörter von Mitarbeitern ausgespäht oder geschickt erfragt? Echtes Hacking – ist jemand intern oder extern in mein System eingedrungen? Kompromittierung – hat jemand bewusst oder unbewusst Daten verändert? An den wenigen Beispielen ist erkennbar, dass es nicht die eine Bedrohung gibt, sondern eine Vielzahl sich verändernder Gefahren. Wer hätte vor zehn Jahren an Trojaner auf Tablets von Ratsmitgliedern gedacht? In vielen kleineren Organisationen besteht die IT-Abteilung – sofern vorhanden – aus Generalisten, die neben dem Aufrechterhalten des Dienstbetriebes auch für die Bereiche Anwendungsbetreuung, Support oder Schulung zuständig sind. Um die IT-Systeme zielgerichtet gegen Gefahren wappnen zu können, fehlt es häufig an Ressourcen.

Datensicherheit hat oberste Priorität

Im Folgenden geht es weniger um technische Lösungsansätze, sondern um die Möglichkeiten, Bedrohungen zu verhindern. Die ganze IT taugt nicht, wenn zentrale Probleme die Benutzung verhindern. Der IT-Leiter muss sich keine Gedanken um einen nicht funktionierenden Drucker im Bürgeramt machen, solange sein System von außen infiltriert wird und das Netz abzustürzen droht. Datensicherheit muss oberste Priorität in der IT haben und das muss Außenstehenden – etwa dem Ratsmitglied, das gern private Apps auf seinem Tablet installiert hätte – auch klar gemacht werden. Hilfestellung sowohl bei der Argumentation als auch der technischen Umsetzung bietet beispielsweise der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI).
In vielen Kommunen ist die Bestellung eines IT-Sicherheitsbeauftragten längst überfällig, analog zum Datenschutz- oder Sicherheitsbeauftragten. Dieser kann, muss aber nicht zwingend aus der eigenen Verwaltung kommen. Viele Rechenzentren bieten eine solche Position zur Miete an. Die wesentlichen Aufgaben des IT-Sicherheitsbeauftragten sind:
• die Analyse der vorhandenen IT-Architektur nebst Dokumentation,
• der Aufbau einer IT-Sicherheitsorganisation,
• die Entwicklung von IT-Sicherheitskonzepten,
die Kontrolle der Umsetzung.

Besseres Gespür für Datensicherheit

Eine Gemeinde mit überschaubarem Personal kann sich fragen, ob alle Verfahren selber gehostet werden müssen, denn jeder gestattete Zugriff von außen stellt ein potenzielles Sicherheitsrisiko dar. Die Gemeinde Westoverledingen bedient sich beispielsweise in Bereichen der Schüler- und Kindergärtenverpflegung, des Fundwesens und natürlich des Standesamtswesens externer Anbieter aus dem SaaS-Umfeld (Software as a Service). Und falls ein entsprechendes Unglück eintritt, gibt es inzwischen in Niedersachsen für Sicherheitsbelange das Landes-Computer-Emergency-Response-Team (CERT), welches eine strategische Rolle in der IT-Security des Landes Niedersachsen einnehmen soll. Solche CERTs werden zurzeit in vielen Bundesländern etabliert. Durch den medialen Ruck, der durch das Land aufgrund von Whistleblowern wie Edward Snowden gegangen ist, hat sich in den vergangenen Monaten das Gespür für IT- und Datensicherheit spürbar verbessert. Musste man früher den Kollegen oder Gremien-Mitarbeitern die Gefahren des Passwort-Hinausposaunens durch eigene Beispiele verdeutlichen, so reicht heute meist ein Hinweis auf den Hacker-Angriff auf den Bundestag. Der beste Weg ist natürlich, zu überzeugen statt zu überreden oder gar zu zwingen. Ein vorbildliches Beispiel, wie eine Sensibilisierungskampagne zum Thema IT-Sicherheit aufgebaut und durchgeführt werden kann, zeigt die Stadt Oldenburg in ihrem IT-Security-Awareness-Projekt „Wolfi“. Mit mehr Sensibilität weiß das oben genannte Ratsmitglied, warum es nicht erlaubt ist, private Apps auf seinem Tablet zu installieren.

Chefetage muss dahinter stehen

Um die direkten und indirekten Gefahren zu bannen, ist ein hoher Personal- und Sachaufwand notwendig. Um genügend Mittel für entsprechende Ressourcen im Etat zu haben, gilt es, diese rechtzeitig einzuwerben. Oft ist IT-Personal, das nicht selten aus der Wirtschaft rekrutiert wird, nicht mit dem Finanzgebaren der öffentlichen Verwaltung vertraut. Zudem lassen sich viele organisatorische Maßnahmen, die die Verwaltung als Ganzes betreffen, kaum ohne ein Commitment der Führung durchsetzen. Die Chefetage sollte in die Lage versetzt werden, zu erkennen, dass das Hauptmaterial, mit der Verwaltungen arbeiten, Informationen sind – und sie sollte wissen, welche Folgen der Verlust oder die Verfälschung dieser Ressource hat. Zudem schadet es nicht, die Ratsmitglieder für dieses Thema anzuwärmen. Als Argumentationshilfe kann die Darstellung der entstehenden Kosten dienen. Hier fallen zunächst die reinen Wiederherstellungskosten an. Nicht vergessen werden darf zudem die Ausfallzeit der Mitarbeiter. In einer Verwaltung mit einem hohen Automationsgrad sind die Kollegen bei Ausfall der IT quasi arbeitslos. Des Weiteren lässt sich mit drohendem Vertrauensverlust der Bürger in die Infrastruktur der Behörde argumentieren, denn ein einmal verlorenes Vertrauen ist schwer wiederzugewinnen. IT-Sicherheit ist schon lange kein rein technisches Thema mehr. Dazu ist die Bedrohungslage zu vielfältig und die Beziehungen in einer Behörde zu komplex. Es gilt daher, der IT ein festes Fundament für die Bekämpfung von Sicherheitsproblemen zu geben. Dieses kann nur in vertrauensvoller Zusammenarbeit mit Personal und Führungskräften gelegt werden.

()

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

Stichwörter: IT-Sicherheit, Westoverledingen, BSI, CERT