Veranstaltung

IT-Security als Daueraufgabe

[24.05.2012] Im Rahmen des Forums Kommune21 auf der DiKOM Süd wurde über IT-Security diskutiert. Dabei wurden Probleme und Herausforderungen angesprochen sowie praktische Tipps für ein erfolgreiches IT-Sicherheitsmanagement gegeben.

Was Kommunen beim IT-Sicherheitsmanagement beachten müssen, war auf dem Forum Kommune21 auf der DiKOM Süd Anfang Mai 2012 in Wiesbaden zu erfahren. Rüdiger Wehrmann aus dem Bereich Informatik/Technik beim Hessischen Datenschutzbeauftragten berichtete von Erfahrungen mit IT-Prüfungen bei Kommunen. Externe Schnittstellen stellen neben der internen Datenverarbeitung ein wichtiges, aber sträflich vernachlässigtes Handlungsfeld dar, so Wehrmann. Frank Wondrak, Geschäftsführer des IT-Dienstleisters KDRS/RZRS, sieht die Einbindung mobiler Endgeräte sogar als aktuell größte Gefahr für die IT-Sicherheit. Hier gelte es, schnell ein Mobile Device Management zu etablieren. Dafür seien industriestandardisierte Lösungen gefragt. Wehrmann ist überzeugt, dass insbesondere kleinere Kommunen bei der Device Control externe Hilfe benötigen.

Worauf Kommunen achten sollten

Ein ganz zentraler Aspekt der IT-Sicherheit ist die Zutrittskontrolle, wie Rüdiger Wehrmann immer wieder betont. Als Negativbeispiel führt er eine hessische Kommune an, der im laufenden Betrieb Blades aus dem Server-Schrank gestohlen wurden. „Es hat Wochen gedauert, bis der Schaden behoben war und manche Daten sind für immer verloren – von den Kosten ganz zu schweigen.“ Zu beanstanden sei bei kommunalen IT-Prüfungen, dass zu vielen Personen Zutritt gewährt und Externe nicht begleitet werden. Auch reiche es nicht aus, ein Back-up zu erstellen, man müsse damit auch umgehen können, so Wehrmann. Darüber hinaus dürfen Passwörter auf keinen Fall hinterlegt und Zugriffsrechte nicht unnötig erweitert werden, etwa auf rechtlich eigene Gesellschaften, die als Amt behandelt werden und deshalb Zugriff aufs Netz erhalten. Das sichere Löschen von Daten stelle für viele Verwaltungen ebenfalls eine Herausforderung dar. Zudem fehle in den Kommunen häufig ein IT-Sicherheitskonzept, Dienstanweisungen seien veraltet und Zuständigkeiten nicht geregelt.
Wehrmann räumt allerdings ein: „Wollen Kommunen bei der IT-Sicherheit alles richtig machen, dann wird es kompliziert und teuer. Und die Sparzwänge machen sich eben auch in diesem Bereich bemerkbar.“ Schließlich sei die Investition in einen Kindergartenplatz öffentlichkeitswirksamer als die in die Device Control. Rüdiger Wehrmann warnt jedoch: „Kommunen sollten nicht am falschen Ende sparen.“

Unterstützung von IT-Dienstleistern

Diese Meinung vertritt auch Bertram Huke, Geschäftsführer des größten kommunalen IT-Dienstleisters in Hessen, ekom21. Sein Rat an die Verwaltungschefs lautet: „Lassen Sie zunächst einmal Ihre Sicherheitsmaßnahmen überprüfen.“ Die Devise vieler Bürgermeister „Warum Geld für IT-Sicherheit ausgeben, es ist ja noch nie etwas passiert“ sei fatal. Wenn nämlich etwas schief laufe, dann werden die Rathauschefs zur Verantwortung gezogen, denn laut Hessischer Gemeindeordnung müssen die Bürgermeister als Behördenleiter jedes Verfahren, das eingesetzt wird, freigeben.
ekom21 hat nach Aussage von Huke im Zuge der BSI-Zertifizierung seines Rechenzentrums eine große Fachkompetenz in den Bereichen Datenschutz und Datensicherheit aufgebaut und gibt diese nun in Form

von Beratungs- und Dienstleistungen weiter. Der IT-Dienstleister KDRS/RZRS, der an seiner ISO-Zertifizierung arbeitet, bietet laut Geschäftsführer Frank Wondrak ebenfalls einen Datenschutzdienst an, der insbesondere von kleinen Kommunen genutzt wird.

Mitarbeiter sensibilisieren

Organisatorisch lässt sich IT-Sicherheit am besten durch Schulungsmaßnahmen gewährleisten. Nach Aussage von Frank Wondrak gilt es, die Mitarbeiter zu sensibilisieren. Bei KDRS/RZRS werde dies nicht nur über Schulungen, sondern auch per Dienstanweisung geregelt. ekom21-Geschäftsführer Bertram Huke meint, dass sich zudem über die Technik bestimmte Verhaltensweisen erzwingen lassen. Vielfach helfe auch der gesunde Menschenverstand oder, wie Rüdiger Wehrmann ergänzt, ein gesundes Misstrauen. Am nachhaltigsten sei der Effekt jedoch, wenn Kommunen bereits schlechte Erfahrungen gemacht hätten, meint der Mitarbeiter des hessischen Datenschutzbeauftragten mit einem Augenzwinkern. Huke bezeichnet dies als klassische Lernkurve: „Wenn mir einmal etwas gestohlen wird, vergesse ich beim nächsten Mal nicht, die Alarmanlage anzuschalten." Erstrebenswert sind solche Erfahrungen dennoch nicht. Deshalb ist es ratsam, dafür zu sorgen, sie gar nicht erst machen zu müssen. Dabei sollten weder Kommunen noch Dienstleister vergessen, dass es sich bei IT-Sicherheit um eine Daueraufgabe und nicht um ein einmaliges Projekt handelt, für das Geld und Personalressourcen aufgewendet werden müssen, wie Huke ausführt.
Diese Investitionen lohnen sich aber durchaus, da damit nicht zuletzt die Nutzung von E-Government-Angeboten angekurbelt werden kann. Frank Wondrak erläutert: „Die in Studien immer wieder bescheinigte, bescheidene Akzeptanz von E-Government liegt nicht in der Technik oder Usability begründet, sondern im fehlenden Vertrauen in den Datenschutz."

(rt)

Stichwörter: IT-Sicherheit, IT-Security, Rüdiger Wehrmann, Bertram Huke, Frank Wondrak, Forum Kommune21, DiKOM Süd 2012