Schritt für Schritt voran

Die Bürger erwarten von der Verwaltung, dass ihre Daten geschützt werden. Mit der ganzheitlichen Analyse der kommunalen IT-Prozesse wird hierfür die Grundlage geschaffen. Das Ziel ist, ein angemessenes Schutzniveau zu erreichen und zu halten.

In einer Zeit, in der keine Woche vergeht, in der nicht neue Spionageaktivitäten der NSA und Datenschutzskandale auch im Bereich der Internetwirtschaft bekannt werden, stellen die Bürger sich schnell die Frage: Wie gehen private oder öffentliche Organisationen mit meinen Daten um? Dabei rücken neben sozialen Netzwerken, denen man freiwillig seine Daten anvertraut, insbesondere das Gesundheitswesen und öffentliche Stellen ins Blickfeld, denen auf Grundlage von Gesetzen Bürgerdaten mitgeteilt werden (müssen).

Die kommunalen Verwaltungen sehen sich in der Datenverarbeitung mit der Herausforderung konfrontiert, von der eingefahrenen, umständlichen papierbasierten Vorgangsbearbeitung auf verlässliche IT-gestützte Prozesse zu wechseln. Diese dürfen die Mitarbeiter nicht verunsichern, sie dürfen keinen Mehraufwand produzieren und müssen vor allem Vertrauen beim Bürger wecken.

Um dieses Ziel zu erreichen, hat sich in der Praxis eine ganzheitliche, dreistufige Vorgehensweise bewährt:

1. Erfassung der Datenflüsse, der Datenkritikalität, der IT-Systeme und der an der Datenverarbeitung beteiligten Mitarbeiter

Bei der Erfassung der involvierten IT-Systeme ist die Unterscheidung zwischen Individual- und Standardsystemen sinnvoll. Standardsoftware induziert im Allgemeinen Best-Practise-Verfahren zu Datenschutz und Datensicherheit. Individualsysteme erlauben eine passgenaue Anpassung auf einen Prozess.

In der Mitarbeitererfassung ist zu berücksichtigen, dass kommunale Verwaltungen sich zunehmend externer IT-Dienstleister bedienen. Die Information, wer auf Basis welcher Vorgaben was im Kontext der Verarbeitung der Bürgerdaten tut, erleichtert die Identifikation von Sicherheitsmaßnahmen.

Foto: Olson/Shutterstock

Senior mit Notebook: Der Bürger hat ein Recht darauf, dass die Daten, die er der Kommunalverwaltung anvertraut, vor Diebstahl und Manipulation geschützt werden.

Wichtige Analysepunkte lassen sich identifizieren, indem neben dem Ist-Stand der Planungsstand beziehungsweise Ideen zum Thema ermittelt werden. So zum Beispiel zum Konzept „Behörden-Cloud“, also der Zusammenschluss von IT-Systemen zur Effizienzsteigerung im Rahmen einer Cloud-Lösung. Aufgrund der Gesetzeslage können solche Lösungen nicht für die gesamte kommunale IT genutzt werden. Mit einigem Fingerspitzgefühlen lassen sich aber durchaus Einsatzszenarien identifizieren, die allen Anforderungen gerecht werden.

2. Ableitung geeigneter Maßnahmen zur Erreichung des notwendigen Sicherheitsniveaus

Die Identifizierung der richtigen organisatorischen, technischen, personellen und infrastrukturellen Maßnahmen ist der Schlüssel zu Kosteneffizienz, Effektivität und „Lebbarkeit“. Die Expertise erfahrener Berater und Informationen aus anderen Bereichen und Pilotprojekten können hier helfen, schnell eine geeignete Lösung zu finden. Erfolgskritische Fragestellungen lassen sich durch Betrachtung der „Schnittstellen“ finden:

- Bürger – kommunales IT-System: Wird der Bürger identifiziert, und wie erfolgt die die Authentisierung? Ist der Kommunikationskanal geschützt?
- Bürger – kommunaler Mitarbeiter: Sind die Mitarbeiter der Verwaltung im Hinblick auf Datenschutz ausreichend geschult? Wurde eine Anlaufstelle für Bürger mit Datenschutzfragen etabliert? Sind die rechtlichen Grundlagen zur Datenverarbeitung klar?
- Kommunale Mitarbeiter – kommunales IT-System: Sind die Mitarbeiter im Hinblick auf „Awareness“ geschult? Fühlt sich der Mitarbeiter sicher im Umgang mit Bürgerdaten?
- Kommunale Verwaltung – IT-Dienstleister: Berücksichtigen die IT-Verträge alle relevanten Sicherheitsaspekte?

- Schnittstelle zwischen kommunalen Verwaltungen: Wie ist der Datentransfer geschützt? Wie sind die Datenübertragungen legitimiert?

Die Beantwortung dieser Fragen führt zu relevanten Aspekten der Sicherheitskonzeption. Aus der Menge möglicher Maßnahmen haben sich in der Praxis die Folgenden als besonders wirksam erwiesen:

- „Security Behavior“: Untersuchungen haben gezeigt, dass Veranstaltungen zum Thema „Risikobewusstsein“ gegenüber Awareness-Schulungen besser geeignet sind, um Mitarbeitern die Sicherheit im Umgang mit sensiblen Bürgerdaten zu vermitteln.

- Externe Audits: Auditierungen durch einen neutralen Dritten sind sinnvoll, um den Nachweis angemessener Sicherheit zu führen und um Betriebsblindheit auszuschließen. Dies gilt vor allem beim Einsatz von IT-Dienstleistern.

- Kontinuierliche Prozesse: Im Sicherheits- und Datenschutzmanagement sind sie zentral zur Aufrechterhaltung eines guten Sicherheitsniveaus.

- Zentrale Anlaufstelle: Eine zentrale Anlaufstelle für Bürger zu Datenschutzfragen entlastet die Organisation und kanalisiert Informationsflüsse.

3. Umsetzung der Maßnahmen und Einbettung in einen Verbesserungsprozess

Klar bewährt hat sich die Maßnahmenumsetzung in Häppchen gefolgt von einer Kontrolle. So lassen sich Maßnahmen besser an die Anforderungen anpassen und führen zu besseren Ergebnissen.

Die konsequent ganzheitliche Betrachtungsweise der Themen Datenschutz und IT-Sicherheit ermöglicht es der Verwaltung, schnell und kosteneffizient ein angemessenes Schutzniveau für die Verarbeitung von Bürgerdaten in der kommunalen IT zu erreichen. Die Beschäftigung mit diesen Themen ist ein fortwährender Prozess und eine Aufgabe, der wir uns alle im Zuge einer sich stetig weiterentwickelnden Gesellschaft und IT-Landschaft stellen müssen. *Patrick Theobald*

Der Autor

Dr.-Ing. Patrick Theobald ist Geschäftsführer des IT-Dienstleisters IT-Security@Work in Dreieich (www.isw-online.de)

Foto: Jackson/Shutterstock

Sicherheitsproblem: Die üblichen Ansätze zur Abwehr von Bedrohungen der kommunalen IT genügen nicht mehr, um die heutigen ausgekügelten Angriffe abzuwehren.

IT-Bedrohungen

Klassische Schutzsysteme schwächeln

Das Jahr 2013 war geprägt von zahlreichen IT-Angriffen durch Insider und Externe. Sie haben gezeigt, dass bei der IT-Sicherheit noch vieles im Argen liegt. Folglich wird dieses Thema auch 2014 eine zentrale Bedeutung einnehmen. Dabei werden sich vier Trends herauskristallisieren: Die IT-Verantwortlichen müssen Angriffe an den Zugängen zu ihren Systemen besser abwehren (Perimeterschutz), es ist den Bedrohungen durch Insider stärker Augenmerk zu schenken, und es müssen die privilegierten Accounts und die sogenannten Application Accounts besser geschützt werden.

Bei allen vergangenen zielgerichteten Web-Attacken wurde die Abschottung der eigenen Netze durch Perimeter-Schutz erfolgreich überwunden. Klassische Sicherheitskonzepte, die auf dem Einsatz von Firewalls, Anti-Viren-Scannern, Webfilter-Techniken oder VPN-Systemen basieren, haben sich als unzureichend erwiesen. Deshalb sind zusätzliche Lösungen als Ergänzung dieser Systeme unverzichtbar.

In vielen Unternehmen ist es üblich, dass Systemadministratoren einen uneingeschränkten Zugriff auf Daten, Applikationen und Server haben, ohne dass es eine Funktionstrennung gibt. Das war auch der Fall bei Edward Snowden, der als Systemingenieur und -administrator auf hochvertrauliche Informationen zugreifen konnte. Es ist von grundlegender Bedeutung, dass Mitarbeiter – und damit auch Systemadministratoren – nur Zugang zu Daten haben, die sie für ihre tägliche Arbeit benötigen. Zudem muss die Option vorhanden sein, dass auch diese Zugriffsmöglichkeit in Echtzeit entzogen werden kann.

Privilegierte Benutzerkonten mit weitreichenden Rechten stellen für jedes Unternehmen ein hohes Sicherheitsrisiko dar. Da nahezu bei allen gravierenden externen und internen IT-Attacken der letzten Zeit Passwörter von privilegierten Nutzern als „Einfallstor“ verwendet wurden, muss dieser Aspekt in den Fokus der Sicherheitsstrategie rücken.

Eine weitere Sicherheitslücke sind die in Anwendungen, Skripten oder Konfigurationsdateien gespeicherten Passwörter (Application Accounts). Diese Anwendungen greifen automatisch auf Backend-Systeme zu, die eine Authentifizierung erfordern. Da die Passwörter meistens im Klartext vorliegen und nie geändert werden, können sie auch problemlos von Angreifern genutzt werden.

„Marktforscher sehen heute bei Themen wie Big Data, Internet der Dinge oder Cloud die zentralen IT-Trends“, sagt Jochen Koehler, Regionaldirektor bei dem auf den Schutz kritischer IT-Infrastrukturen spezialisierten Unternehmen Cyberark in Heilbronn (www.cyberark.com). „Das ist richtig, aber einen Punkt darf man nicht vergessen: Bei allen neuen Lösungen, Services und Technologien wird die Sicherheit von elementarer Bedeutung sein.“