

IT-Security ist Chefsache!

Es gibt keinen Bereich im öffentlichen Leben, der nicht von der Informationstechnologie durchdrungen, beeinflusst und abhängig wäre: Die gesamte Wirtschaft, Politik, Kultur, selbst der Sport gehört dazu. Kein Bundesligatrainer verzichtet zum Beispiel darauf, seine Analysen und Beobachtungen datentechnisch zu verarbeiten und abzuspeichern. Gleiches gilt für Behörden und andere Verwaltungsstrukturen. Die Aussage ist nicht übertrieben, dass „ein Leben ohne Informationstechnologie“ weder vorstellbar noch möglich ist.

Aber: wo Abhängigkeiten entstehen, erhöhen sich auch Risiken. Ein Computervirus bringt ganze Netzwerke zum Absturz, ein Hacker kann gigantische Schäden verursachen. Das „I-love-you“-Virus kostete die Weltwirtschaft nach Ermittlungen des amerikanischen FBI unglaubliche 10 Milliarden (!) Dollar. Da nimmt es Wunder, dass die Sensibilität von Datenbeständen kaum, zumindest aber wenig thematisiert wird.

Behörden haben natürlich ihren Beauftragten für Informationstechnologie, IT-Netzwerke sind installiert und werden meist reibungslos betrieben. Dass aber der Amtsleiter von dieser Arbeit viel verstünde oder sich sogar darum kümmerte, darf, von Ausnahmen vielleicht abgesehen, bezweifelt werden. Sollte er aber! Denn dazu ist das Thema viel zu wichtig, viel zu brisant, sagen wir's doch deutlich: es ist viel zu gefährlich! Deshalb lautet die in Fachkreisen unumstrittene Maxime: IT-Sicherheit ist Chefsache!

Man braucht nicht bis zur Polizei, dem Verfassungsschutz oder gar der Bundeswehr zu gehen, um zu begründen, wie dünn das Eis ist, auf dem sich die Informationstechnologie bewegt, wie albraumhaft ein Ausspähen von Daten zum Beispiel durch terroristische Angreifer sein würde.

Ziehen wir ein einfacheres, weniger Furcht erregendes Beispiel heran, nämlich simple Personendaten einer Behörde:

Wo immer sie anfallen und gespeichert werden, sind sie selbstverständlich schutzwürdig und schutzbedürftig und nur wenigen Mitarbeitern zugänglich zu

machen; solche Daten genießen absolute Vertraulichkeit! Aber auch behördliche Datenbestände über amtliche Vorgänge, Verfahren, Verhandlungen, über Gespräche, Informationsbeschaffungen und Vernetzungen; nichts davon ist für die Öffentlichkeit bestimmt, es sei denn, es besteht eine ausdrückliche Absicht, die Allgemeinheit daran partizipieren zu lassen, beispielsweise als Antwort oder freiwillige Information gegenüber einzelnen Bürgern, der Politik oder Presse, Rundfunk und Fernsehen.

Mit Vertrauen und Vertraulichkeit darf jedoch nicht nachlässig oder gar fahrlässig umgegangen werden. Deshalb genießt IT-Security höchste Priorität. Nicht nur, wenn es darum geht, irgendwelche Erfindungen und Konstruktionspläne vor den Spionageversuchen der globalen Konkurrenz zu schützen. Behördenverwaltungen haben gleiche Pflichten.

Nehmen wir das Landesamt für Gesundheit und Soziales Berlin (LAGeSo). Es verteilt sich mit sechs Standorten auf das gesamte Stadtgebiet. Die einzelnen Ämter sind über das Berliner Landesnetz datentechnisch miteinander verbunden. In den sechs Standorten ist die Anbindung der insgesamt etwa 900 Endgeräte über lokale, voll geschwitze Netzwerke mit Nortel-Komponenten realisiert. Die Datenbestände sind gewaltig, täglich kommen zigtausende Datensätze hinzu. Vertraulich sind sie nahezu alle, nur der Grad der Vertraulichkeit ist unterschiedlich hoch.

Vor etwa einem halben Jahr entwickelte die mikado ag in Berlin, ein mittelständisches IT-Unternehmen, ein neues IT-Security-System: MACmon (von Mac-Adressen monitoring), das die Aufmerksamkeit des Servicebereichs IT des Landesamtes erregte. Es arbeitet herstellerübergreifend und schützt vor Angriffen, Sicherheitsverletzungen, Ausspähungen, Datenmanipulationen und Schädigungen in einem bisher nicht gekanntem Maße.

Das Landesamt für Gesundheit und Soziales versteht sich als moderner Dienstleister für die Bürgerinnen und Bürger Berlins und versorgt etwa jeden sechsten Berliner mit Leistungen aus dem sozialen und gesundheitlichen Bereich. Das lohnt - als Hinweis auf die Quantität und Qualität der Aufgabe und den sich daraus ergebenden immensen Datenbestand -, wiederholt zu werden: Jeder sechste!

Was sind das für Aufgaben, die so vielfältig sind und über die klassischen Arbeiten der „Versorgungsverwaltung“ weit hinausgehen? Das Landesamt übertrug der Firma mikado den Aufbau des MACmon-Servers und die Inbetriebnahme. Alle rund 50, teils kaskadierten, aktiven Netzwerk-Komponenten der Standorte sind in die Abfrage eingebunden. Die Implementierung von MACmon erfolgte reibungslos.

MACmon schützt vor Angriffen und Ausspähungsversuchen von außen und innen. Bei der Entwicklung des Produkts wurden Fehler, Mängel und Lücken bestehender IT-Sicherheitssysteme berücksichtigt und getilgt. Dabei hatte sich die mikado ag einer umfangreichen und detaillierten Liste bedient, deren Inhalt und Umfang auf Praktiker aus allen Bereichen, auch der verschiedensten Behörden und Verwaltungen, zurückgeht. Hier wurde also ein IT-Produkt an der Realität ausgerichtet und nicht etwa die Realität in Richtung Produkt verbogen. Bleibt ja gelegentlich als Eindruck im IT-Wesen, dass die Anwender bitte schön selbst sehen mögen, wie sie damit zurechtkommen.

Die Anwendung von MACmon beim LAGeSo läuft stabil. Abgefragt wird im 4-Minuten-Takt. Beim Erkennen einer nicht zugelassenen MAC-Adresse werden die entsprechenden Ports zuverlässig gesperrt und auch wieder nach eingestellter Zeit automatisch entsperrt. Zeitgleich mit der Sperrung erfolgt eine Information per Mail. Fehler sind noch nicht aufgetreten. Der Betreuungsaufwand ist zu überschauen und zu leisten.

Der Leiter des IT-Servicebereichs des Landesamtes, Stefan Trautmann, kommt zu einem beachtlichen Urteil. Er schreibt: „MACmon ist ein ohne großen Aufwand schnell einzuführendes effizientes und bedienungsarmes Tool, um das Einbringen betriebsfremder Hardware in das LAN zu erschweren. Der Einsatz ist ein bedeutender Schritt in Richtung mehr Sicherheit.“ Stefan Trautmanns Fazit: „Wir sind mit dem Produkt sehr zufrieden!“

HEINER GIERSBERG

mikado ag - Weitere Informationen unter www.mikado.de