Vertrauen ist die Basis

von Michaela Harlander

Eine wesentliche Voraussetzung dafür, dass der Bürger die Online-Kommunikation mit seiner Verwaltung akzeptiert und vor allem praktiziert, ist Vertrauen in die Datensicherheit. Doch bislang wird auf Behördenseite häufig zu sorglos mit dem Thema umgegangen.

Elektronischer Service wird immer wichtiger, dies gilt auch in der öffentlichen Verwaltung. Die Zahl der Bürger, die ihre Behördengänge zukünftig online erledigen möchten, steigt kontinuierlich an. Schon heute klopfen viele Internet-User lieber an die virtuelle Pforte eines Rathauses, als sich persönlich in das entsprechende Amt zu begeben. Immer mehr Gemeinden und Behörden bieten deshalb einige ihrer Dienstleistungen online an. Wenn seitens der Verwaltung die grundsätzliche Entscheidung zur Umsetzung eines Online-Bürgerservice gefallen ist, sind diverse Kriterien für die Auswahl der richtigen Online-Anwendung entscheidend: Benutzerfreundlichkeit, eine einfache Implementierung des Systems und natürlich die Kosten spielen eine wesentliche Rolle. Ein zentraler Punkt bei der Planung einer e-Government-Lösung ist die Datensicherheit; denn durch das Anbieten von Online-Dienstleistungen lassen Angriffe auf das Computersystem und damit auf das Behördennetzwerk nicht lange auf sich warten. Dabei sind Bürgerdaten hochsensibel, da sie vertrauliche Informationen enthalten und deshalb vor unbefugten Eingriffen bestmöglich geschützt werden müssen.

Vor unangenehmen Diskussionen über das Thema Datensicherheit …

Die größte Bedrohung für vertrauliche Daten stellt zunächst ein nicht ausreichend sorgfältiger Umgang mit den gewonnenen Daten dar. Zugang zu den vertraulichen Daten dürfen nur die zuständigen Sachbearbeiter haben. Entsprechende Sicherheitsmaßnahmen, wie etwa Zugriffsbeschränkungen oder Klassifizierung der Daten sowie klare Richtlinien für den Umgang mit den Daten sind innerhalb der Behörden unabdingbar. Eine weitere Gefahr für die Daten lauert auch auf dem Weg vom Bürger zur Behörde. Die Datenübertragung muss mit einer ausreichend guten Verschlüsselung und unter Einhaltung geeigneter Sicherheitsmaßnahmen erfolgen.

Auf Sicherheitsprobleme, denen sich die Bürger durch einen unachtsamen Umgang mit dem Medium Internet aussetzen, hat die Behörde wenig Einfluss. Umso eindringlicher sollte jedoch davor gewarnt werden, dass sich Bürger mit dem Herunterladen von Software aus unsicheren Internet-Quellen sehr einfach Programme einfangen können, die die Sicherheit der persönlichen Daten gefährden. Bedrohungen gehen allerdings auch von den Mitarbeitern selbst aus: Nicht selten sind sie es, die bewusst oder unbewusst Sicherheitslücken im System verursachen. Werden Richtlinien nicht beachtet oder bestimmte Tricks angewandt, können die internen Sicherheitssysteme außer Kraft gesetzt und Schaden verursacht werden, zum Beispiel durch das Öffnen virusinfizierter

Dokumente, die an e-Mails angehängt wurden. Die Folge: Sie öffnen Hackern dadurch virtuelle Türen und Tore. Die öffentliche Verwaltung sollte hier durch entsprechende Richtlinien und Schulungen sicher stellen, dass die eigenen Mitarbeiter kein zusätzliches Gefahrenpotenzial importieren.

Neben den bereits erwähnten Bedrohungen sind Behördennetze immer stärker Hacker-Attacken, also dem unerlaubten Eindringen über das Internet ins Behördennetzwerk, ausgesetzt. Die Schäden, die ein solcher Angriff verursachen kann, reichen von der Einsicht vertraulicher Daten über Manipulation bis hin zum kompletten Lahmlegen des Online-Angebots. Letzteres tritt auf, wenn Dateien gezielt geändert oder gelöscht werden, so dass der Nutzer nicht mehr darauf zugreifen kann. Was kann nun die öffentliche Verwaltung gegen all diese potenziellen Gefahren unternehmen?

Um derartigen Bedrohungen effizient entgegen zu wirken, ist Expertenwissen unabdingbar. Durch ein umfassendes und in sich stimmiges Sicherheitssystem werden die sensiblen Daten optimal geschützt. Wer das Netzwerk effektiv durch ein Sicherheitssystem schützen möchte, sollte möglichst konsequent und systematisch vorgehen:

Einer Analyse der Anforderungen und des bestehenden Netzwerks sowie Erstellung einer Sicherheitskonzeption folgt die Ausarbeitung der passenden Schutzmaßnahmen sowie die Festlegung von Zugriffsrechten und Benutzerrichtlinien im Netzwerk entsprechend den sicherheitspolitischen Überlegungen. Der nächste Schritt beinhaltet Auswahl, Konfiguration und Installation von Sicherheitslösungen wie Firewalls, Angriffserkennungssystemen (IDS) und Virenscannern. Letzter Punkt: Security Audits, sprich regelmäßige Überprüfung der bestehenden Sicherheitskonzepte und deren Umsetzung nach definierten Standards, gegebenenfalls Anpassung. Durch die vielen Gefahren aus den eigenen Reihen und dem Internet ist ein Sicherheitssystem speziell für e-Government eine hochkomplexe Aufgabenstellung: Nur eine auf das jeweilige Internet-Angebot zugeschnittene, professionelle Beratung gewährleistet die Sicherheit der Bürgerdaten dauerhaft und zuverlässig. Erste Orientierungshilfe leisten das IT-Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik (BSI) oder die ISO-Norm 17799. Diese Standards unterstützen bei der Erstellung von Policys und der Durchführung von Audits. Zudem zertifiziert das BSI nach den internationalen Prüfkriterien ITSEC Sicherheitssysteme wie etwa Firewalls. Eine solche Zertifizierung bietet Transparenz im IT-Sicherheitsmarkt: Geprüft von einer unabhängigen Einrichtung garantiert sie, dass das System den Sicherheitsanforderungen entspricht und die Aussagen des Herstellers zutreffen.

Zusammenfassend lässt sich somit festhalten: Online-Behördengänge und entsprechende Internetangebote des Bundes, der Länder und Kommunen werden auch in Zukunft weiter zunehmen. Wichtig ist, dass bereits bei der Planung solcher Lösungen sorgfältig vorgegangen wird. Neben zusätzlichem Service und Vereinfachung der Behördengänge ist vor allem die Datensicherheit ein wesentliches Kriterium für den Einsatz neuer e-Lösungen. Nur wenn die Sicherheit des virtuellen Rathauses garantiert ist, festigt sich das Vertrauen der Bürger dauerhaft in die Online-Verwaltungsabwicklung. Dann ersetzt e-Government schon bald eine Vielzahl von Behördengängen – zum Vorteil aller.

… schützt nur Expertenwissen.

Dr. Michaela Harlander ist Geschäftsführerin von GeNUA, Gesellschaft für Netzwerk- und UNIX-Administration mbH, München.

Web-Service

Informationen zum IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik sind im Internet verfügbar:

- www.bsi.de/gshb/