Sicherheit mit **Niveau**

von Ulrich Kemp

Alle Vorgänge im e-Government müssen am Thema Sicherheit orientiert sein. Die Bürger erwarten höchste Vertraulichkeit im Umgang mit ihren Daten. Security Policies sind die Grundlage für Verfügbarkeit und Datenschutz.

Das Marktforschungsinstitut Forsa hat im August 2002 ermittelt, dass bereits rund 50 Prozent aller Deutschen über das Internet erreichbar sind. Mit der Zahl der Online-Bürger wächst auch der Ruf nach Behördenleistungen, die über das Netz funktionieren. Gleichzeitig erwarten die Bürger vom Staat die höchste Vertraulichkeitsstufe beim Umgang mit ihren Daten. Hoheitliche Aufgaben dürfen keinen Risiken ausgesetzt sein. Aber auch die Integrität von Verwaltungsdaten, wie Bescheiden oder Melderegistern, muss unter allen Umständen gewahrt bleiben.

Sicherheit ist folglich mehr als eine bestimmte technische Einzellösung. Vielmehr müssen alle Bestandteile und Vorgänge im e-Government einer grundsätzlichen Orientierung am Thema Sicherheit folgen. Sicherheitsrichtlinien (Security Policies) und ein fundiertes Know-how sind die Grundlage für einen dauerhaften Schutz. In einem kontinuierlichen Prozess sollte die Sicherheit daher in allen Bereichen des e-Government von Anfang an verankert sein. Der Faktor Mensch spielt natürlich bei der Absicherung von elektronischen Prozessen die Hauptrolle. Schließlich nützen die sorgfältigste Planung und die beste technische Ausrüstung nichts, wenn sie nicht verantwortungsvoll eingesetzt wird. Regelmäßige Schulungen und Sicherheitstests halten beispielsweise das Sicherheitsbewusstsein auf dem nötigen Niveau.

Bei der Einführung elektronischer Geschäftsprozesse kommen eine Reihe zusätzlicher Forderungen ins Spiel. Um den Service zu verbessern, sollen beispielsweise die meisten elektronisch angebotenen Leistungen rund um die Uhr zur Verfügung stehen. Die zugehörigen Systeme (Hintergrundsysteme, Netzwerkinfrastruktur) müssen also auf den Dauerbetrieb ausgelegt sein. Da sich zudem die Sicherheitsanforderungen ständig weiterentwickeln, sollte die IT-Infrastruktur möglichst ohne Betriebsunterbrechung ihren Sicherheitsstandard kontinuierlich an die aktuelle Lage anpassen können.

Faktor Mensch: Absicherung von elektronischen Prozessen.

Bei Flut- oder Brandkatastrophen, Terrorattacken oder Gebäudeschäden dürfen zudem die Kernprozesse und -daten nicht verloren gehen. Die erprobten Konzepte des Business Continuity Planning helfen beispielsweise beim redundanten Betrieb von Ausweichrechenzentren und Speicherspiegelungen über große Entfernungen hinweg. Zum sicheren Betrieb einer Server-Umgebung gehört daher auch eine Clusterfunktionalität, die den Totalausfall eines Servers absichert. Redundant ausgelegte Server- und Storage-Systeme beugen dem Datenverlust vor: Wird ein System von einem Teil- oder Totalausfall betroffen, übernimmt das andere System unterbrechungsfrei den Betrieb.

Da viele Vorgänge nicht mehr persönlich ausgelöst werden, müssen die Benutzer durch elektronische Maßnahmen eindeutig identifiziert werden. Ein Beispiel dafür sind Smart-Card-Lösungen mit der digitalen Signatur nach dem aktuellen Signaturgesetz, das seit der Veröffentlichung im Bundesgesetzblatt am 27. August 2002 amtlich ist. Eine Schlüsselrolle für den Erfolg des e-Government misst auch die Initiative D21 der elektronischen Signatur als wesentliche Voraussetzung für einen sicheren elektronischen Geschäftsverkehr bei. Um per Internet in allen Fällen rechtsverbindlich handeln zu können, soll eine qualifizierte Signatur künftig möglichst direkt auf dem Personalausweis vorhanden sein.

Identität: Anmeldung am System.

Doch mit der Identifizierung allein ist es nicht getan. Um Transaktionen sicher zu machen, müssen alle Schritte für beide Seiten eindeutig nachvollziehbar sein. Im Fehlerfall, beispielsweise bei einer unterbrochenen Telefonleitung, dürfen keine falschen Daten übermittelt werden. Alle Vorgänge müssen nach der Fehlerbehebung in einem klar definierten Zustand sein. Neben einer umfassenden Protokollierung werden dafür transaktionsgesicherte Systeme benötigt, wie sie beispielsweise im Online-Banking erprobt sind. Bei kostenpflichtigen Vorgängen stellt ein Zurückweisungsschutz zudem sicher, dass der Auslöser den Vorgang auch wirklich persönlich auslösen will. Andererseits erhält der Bürger damit die belegbare Bestätigung, dass sein Auftrag auch wirklich beim Empfänger angekommen ist – ein wichtiger Fortschritt beim Einhalten von Fristen.

Spätestens beim Anschluss ans Internet erwächst den behördlichen Prozessen eine neue Klasse von Sicherheitsanforderungen: Hacker, Viren, Störangriffe und zufällig oder absichtlich falsch abgeschickte Daten müssen vom eigentlich erwünschten Geschäftsverkehr mit Bürgern und Unternehmen getrennt werden. Damit die behördeninternen Systeme sicher vor Eindringlingen sind, stehen mehrstufige Firewall-Systeme bereit, die – ähnlich einem System von Burggräben und Zugbrücken – den Ansturm von außen kanalisieren und nur erwünschte (Daten-)Reisende einlassen. Dazwischen werden – ähnlich einer Quarantänestation – Dokumente, e-Mails oder auch komplexe Datenstrukturen in einer so genannten „Demilitarisierten Zone“ auf Viren und sonstige Schädlinge geprüft. Damit die Datenverbindung bis zum Schreibtisch des Bürgers auch auf den öffentlichen Netzen vor Abhören oder Datenmodifikation sicher ist, kommen automatisch arbeitende Verschlüsselungsverfahren zum Einsatz. Beispielsweise bieten https und SSL (Secure Sockets Layer) eine standardisierte Methode, die auf allen Plattformen ohne Zusatzaufwand oder besondere Installationen funktioniert. Auf diese Weise kommen die Daten immer sicher ins Amt und zurück.

Ulrich Kemp ist Geschäftsführer Vertrieb Deutschland von Fujitsu Siemens Computers.

Kurzprofil: Fujitsu Siemens Computers

Fujitsu Siemens Computers bietet eines der umfassendsten Produktportfolios im Enterprise Computing – von Intel- und Unix-Servern bis zu Großrechnern und Speicherlösungen. Das Unternehmen ist darüber hinaus einer der führenden Anbieter von mobilen Produkten, Business-PCs und Workstations. Fujitsu Siemens Computers verfügt über ein vollständiges Spektrum an Lösungen für alle Sicherheitsfragen – von der Smart Card bis zum hochsicheren Datacenter. Ein eigens eingerichtetes Security Competence Center sorgt für Beratung und Dienstleistungen rund um das Thema IT-Sicherheit.

• www.fujitsu-siemens.de