Sicherheit mit Augenmaß

von Rüdiger Grimm

Kommunikation im offenen Netz: e-Government ist einem besonderen Sicherheitsproblem ausgesetzt. Was unter dem Begriff Security genau zu verstehen ist und welche Schutzmaßnahmen für die öffentliche Verwaltung sinnvoll sind, zeigt der folgende Beitrag.

Sicherheit im e-Government und e-Commerce: Neben gemeinsamen Problemen und Antworten gibt es hier wichtige Unterschiede. Der öffentliche Diensteanbieter ist neutraler, erfüllt Gemeinwohlaufgaben und hat dadurch eine geringere Konkurrenzlage als die private Wirtschaft. Ihm wird ein höheres Vertrauen und ein höherer Anspruch entgegengebracht, sich fair zu verhalten. Weiterhin vollziehen einige öffentliche Institutionen Hoheitsaufgaben und haben daher höhere Ansprüche an die Rechtssicherheit ihrer Aktivitäten.

Unter Sicherheit in der Informations- und Kommunikationstechnik versteht man die Gewissheit ihres ordnungsgemäßen Ablaufs. Neben dem Schutz gegenüber Fehlern und unbeabsichtigten Unfällen (Safety) interessiert hier vor allem der Schutz vor gezielten Angriffen und Manipulationen (Security). Zum Verständnis der Security-Problematik muss man erstens die Interessen und Konflikte der beteiligten Personen und Institutionen analysieren und zweitens die technischen Angriffsmöglichkeiten aufdecken. Daraus ergeben sich die Sicherheitsanforderungen sowie die technischen und organisatorischen Sicherungsmaßnahmen.

Technisch besteht deshalb ein besonderes Sicherheitsproblem für e-Government (und ebenso für e-Commerce, e-Demokratie und all die anderen elektronischen Kooperationsbereiche), weil ein offenes Kommunikationsnetz die Kooperationspartner sowohl miteinander verbindet, und zwar weltweit, als auch physisch voneinander trennt. Zwar kann nun jeder mit jedem zu jeder Zeit in Kontakt treten und Geschäfte abwickeln, aber man sieht und hört sich nicht mehr, die Partner und ihre Handlungen sind nicht mehr synchron beobachtbar. Dadurch sind viele traditionelle Sicherungsmechanismen wie das Erkennen von Gesichtern und Stimmen oder die Beobachtung einer handschriftlichen Tintensignatur bei der Überprüfung eines Reisepasses außer Kraft gesetzt. Gleichzeitig entsteht eine Fülle neuer Kommunikations- und Bewegungsdaten, die für unautorisierte Beobachter bequem auszuforschen und auszuwerten sind.

Aus Schwächen der Technik ergeben sich folgende abstrakte Sicherheitsanforderungen: Datenschutz, Vertraulichkeit, Verfügbarkeit, Authentizität, Transaktionssicherheit. Nicht alle Sicherheitsanforderungen gelten unter allen Umständen in gleichem Ausmaß. Einige Sicher-

Internet: Viren haben oft leichtes Spiel.

heitsanforderungen können sich sogar gegenseitig ausschließen, zum Beispiel das Recht auf unbefangenes und daher nicht verfolgbares Informationssuchen gegenüber der Unabstreitbarkeit verbindlicher Willenserklärungen. Sicherheit ist niemals allein technisch begründet, sondern hängt vom jeweiligen Anwendungskontext ab, und hierbei von den beteiligten Menschen und ihren Interessenlagen, die zueinander in Konflikt stehen können.

Betrachten wir zunächst den Datenschutz. Es besteht eine Interessenskollision zwischen der Verwaltung und den Bürgern. Die Verwaltung will für einen reibungslosen Ablauf und zur Wahrnehmung ihrer

Schutzaufgaben möglichst viel von ihren Bürgern wissen und sammelt daher gerne Daten über Bürger. Die Bürger dagegen wollen zwar den reibungslosen Schutz der Behörden gerne in Anspruch nehmen, gleichzeitig aber frei und unbefangen von staatlicher Kontrolle bleiben. Den Interessenausgleich formuliert die Datenschutzgesetzgebung. In Deutschland und Europa setzt sie auf eine Handvoll Prinzipien wie Datensparsamkeit, Transparenz und Nutzerkontrolle. Die moderne Kommunikationstechnik liefert selbst Unterstützungsfunktionen für den Datenschutz.

Hier hat e-Government eine positive Sonderstellung: Wegen der besonders hohen Erwartung seitens der Bürger an die Fairness der öffentlichen Dienste, und wegen der hohen Zustimmung seitens der Beamten und Angestellten des öffentlichen Dienstes zum Datenschutz der Bürger, sind die Konflikte ausgleichbar. Und da der öffentliche Dienst hierarchisch gegliedert ist, ist Datenschutz leichter durchzusetzen, als bei dezentralen autonomen Organisationsformen.

Die Vertraulichkeit im Web kann durch das etablierte SSL-Protokoll gut gewährleistet werden. Aber Achtung: e-Mail und häufig auch noch Passwörter werden im Netz in der Regel unverschlüsselt übertragen. Hier helfen Verschlüsselungsverfahren in den Anwendungskomponenten wie PGP oder S/MIME, die zwar zur Verfügung stehen, aber kaum verbreitet sind. In Bezug auf Verfügbarkeit der Dienste greifen vorhandene Verfahren der Anomalieerkennung, Virenschutz und ein ausreichendes Ressourcenangebot mit redundanten Komponenten und einer regelmäßigen Sicherungsarchivierung der Daten.

Ein schwieriges und bis heute nicht gelöstes Problem bildet die Anforderung nach Authentizität. Dabei sind drei Bereiche angesprochen: die Authentizität der Daten (Ist der Reisepass echt?), die Authentizität der beteiligten Kommunikationspartner (Ist der Antragsteller wirklich die Person, die sie zu sein behauptet?) und die Authentizität des Anwendungskontextes (Bezieht sich die Genehmigung wirklich auf meinen Antrag im Rahmen der Ausschreibung?). Die Authentizität von Daten vereinigt die gesicherte Identität (Herkunft) und die Unverletztheit des Wortlauts (Integrität). Die elektronische Signatur gilt gemeinhin als Allheilmittel zur Sicherung der Authentizität. Den zu Grunde liegenden technischen Mechanismus liefert die asymmetrische Verschlüsselung, die für offene Kommunikationsumgebungen konzipiert ist, in denen sich die beteiligten Personen vorab nicht kennen und vielleicht auch nur einmal oder ganz wenige Male treffen. Um dieses für den Alltagsgebrauch im globalen Maßstab zuverlässig abzusichern, sind zusätzliche hohe Sicherungsverfahren zu betreiben. Dazu gehört die gesetzlich abgesicherte Dienstleistungsinfrastruktur von Überprüfungs-, Zertifizierungs-, und Informationsdiensten. Deshalb hat sich die qualifizierte elektronische Signatur auf diesem hohen Niveau bis heute nicht durchgesetzt. Es darf bezweifelt werden, dass sie jemals von den Bürgern akzeptiert wird.

Glücklicherweise ist das aber auch gar nicht in dem Maße nötig, wie häufig behauptet wird. In der ▶

April-Ausgabe von Kommune 21 wird zum Beispiel beschrieben, wie Mülheim an der Ruhr mit alternativen Plausibilitätsprüfungen und vereinfachten Erkennungsverfahren geschlossener Gruppen „signaturlos glücklich“ wichtige e-Government-Dienste, auch solche rechtsverbindlicher Natur, durchführt. Denn die Kommunikation im vertrauten Kontext von Bürgerdiensten liefert zahlreiche Möglichkeiten, die Identität von Personen und die Integrität von Daten abzusichern. Dazu gehören Rückrufe, Angabe von vertraulichem Wissen wie Geburtsdaten und Steuernummern, sowie die Rücknahme von fälschlich erbrachten Diensten,

e-Versand: Sicherheit ist gefragt.

wie das im täglichen Leben bereits heute allgemein gehandhabt wird. Es ist beispielsweise kein Problem, ein fehlerhaftes elektronisches Antragsformular durch ein richtiges zu ersetzen, sowohl elektronisch, schlimmstenfalls durch postalische Zusendung als Reparaturmechanismus. Und da das so simpel ist, sind der Anreiz und damit die Gefahr der Fälschung gering.

Anders ist das bei wertvollen Dokumenten wie Personalausweis, Besitzurkunden oder akademische Titel. Bei einem rein elektronischen Einsatz solcher Dokumente ist eine erhöhte Signaturabsicherung gerechtfertigt. Keinesfalls aber gerechtfertigt ist die flächendeckende Hochsicherheitsanforderung an alle Signaturanwendungen. Mit den einfacheren „fortgeschrittenen Signaturen“ im Zusammenspiel mit kommunikativen Sicherungselementen sind die meisten Anwendungsfälle gut abzudecken.

Die Transaktionssicherheit bildet ein Kernstück des e-Government. Hier geht es um den ordnungsgemäßen Gesamtablauf: e-Government-Prozesse sind in Kommunikation eingebettet und bestehen eben nicht aus isolierten Daten. Diese Anforderung lässt sich zu einem großen Teil mit Mitteln der Kommunikation und mit einfachen Integritätsmerkmalen erfüllen. Dazu gehören Informationsdienste zur Aufklärung und Transparenz, Rückruf- und Rückfragemöglichkeiten, zeitlich befristete Kontext-Quittungen, und schließlich die Reparatur von Fehlern durch Storno, Verbesserung und Wiederholung.

Dies alles hat Konsequenzen für die Praxis: In erster Linie müssen die Betreiber der öffentlichen Dienste und ihre Mitarbeiter über die Sicherheitsproblematik aufgeklärt werden. In demselben Maß muss auch die Bevölkerung über Chancen, Risiken und risikominderndes Verhalten bei e-Government informiert werden. Teilweise wird das eine Aufgabe der Schulen und der Berufsausbildung sein. Das kann sofort umgesetzt werden.

Zweitens sollten die Behörden e-Government als eine zusätzliche Kommunikationsschiene neben der physischen Präsenz, dem Telefon und der Papierpost realisieren. Die zugehörigen Sicherungsmechanismen sollen diesen Medienmix und die Kommunikationsmöglichkeiten ausnutzen. Auch das kann heute umgesetzt werden und ist bereits vielerorts auf dem Wege.

Eine dritte Aufgabe betrifft die elektronische Signatur. Diese ist weiter zu entwickeln und auf die zugehörigen Anwendungsbereiche angemessen zuzuschneiden. Auf dem hohen Sicherheitsniveau der qualifizierten Signatur sind alle wertvollen Dokumente mit Langzeitwirkung in verschiedenen Anwendungsbezügen in ihrem Beweiswert zu schützen. Auf geringerem Niveau kann die fortgeschrittene Signatur einen sinnvollen Beitrag zur Transaktionssicherheit im Zusammenspiel mit kommunikativen Absicherungen liefern. Damit sind fast alle Anwendungen in geschlossenen Nutzergruppen gut abzusichern, welche ohnehin den größten Anteil von e-Government darstellen.

Viertens bildet die einfache Handhabbarkeit der Dienste eine wesentliche Voraussetzung zu ihrer Sicherheit. Dazu ist es erforderlich, dass die Sicherungsverfahren standardisiert werden. Die neue Spezifikationssprache XML für Daten und ihre Sicherheitsmerkmale spielt dabei eine bedeutende Rolle. Kommunikationsregeln wie die Protokollfamilie OSCI für e-Government-Dienste sind hier hilfreich. Das kürzlich geschlossene Signaturbündnis zwischen öffentlichen und privatwirtschaftlichen Anwendungsbereichen kann ebenfalls die Realisierbarkeit und Akzeptanz von Sicherungsmechanismen verbessern.

Prof. Dr. Rüdiger Grimm ist Leiter des Fachgebiets Multimediale Anwendungen mit einem Schwerpunkt auf e-Commerce und e-Government an der Technischen Universität Ilmenau.