e-Government versus Sicherheit?

Sonja Hof

Universität Linz, Österreich
Institut für Angewandte Informatik
Abteilung für Informatik in Wirtschaft, Verwaltung und Gesellschaft
Altenbergerstrasse 69, 4040 Linz
hof@ifs.uni-linz.ac.at

Schlagworte: e-Government, Sicherheitsaspekte, e-Voting

Abstract: Dieser Beitrag gibt einen Überblick über Sicherheitsaspekte wie sie in e-Government-Projekten angetroffen werden. Dabei werden deren Gefahren und Eigenheiten in Bezug auf Sicherheit betont und mögliche Konsequenzen aufgezeigt. Beispielsweise wird versucht, die Sensibilität gegenüber Sicherheitsaspekten zu erhöhen und eine entsprechende Diskussion anzuregen.

1. Einleitung

Dieser Beitrag stellt die verschiedenen Motivationen für e-Government-Lösungen den entsprechenden Sicherheitsbedenken gegenüber. Dazu werden im ersten Abschnitt das Verständnis von e-Government mit den verschiedenen Komponenten sowie die zugrunde liegenden Motivationen, e-Government-Lösungen zu entwerfen und zu implementieren, dargestellt. Im zweiten Abschnitt werden einige mögliche Bedrohungsszenarien, welche erst durch die Einführung von e-Government ermöglicht wurden, aus Sicht der Sicherheit aufgezeigt. Diese Aufstellung ist nicht als vollständige Liste gedacht, sondern dient lediglich dazu, die Sensibilität des Lesers gegenüber Sicherheitsfragen zu schärfen sowie dessen Bereitschaft, entsprechende Aufgaben mit der entsprechenden Ernsthaftigkeit zu betreiben, zu fördern. Der letzte Abschnitt fasst die Resultate der vorigen Abschnitte nochmals zusammen.

2. e-Government

Dieser Abschnitt gibt keine formale Einführung in den Bereich e-Government, sondern zeigt eine Unterteilung in verschiedene Aspekte, wie sie im restlichen Beitrag verwendet werden (siehe Abbildung 1). Diese Unterteilung sieht sich dabei nicht als generelle Klassifizierungsmethodik, sondern als Unterteilung, welche für sicherheitsbezogene Aspekte verwendet wer-

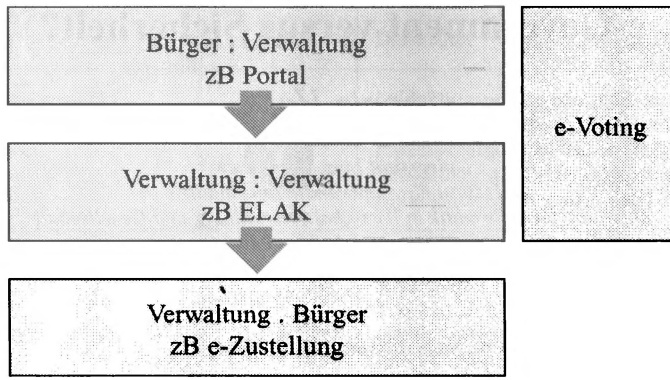

Abbildung 1: Sicherheitsbezogene Unterteilung von e-Government

den kann. Sie soll widerspiegeln, welche Beziehungen in den verschieden Bereichen des E-Government auftreten und welche Projekte in diesen Bereichen bereits umgesetzt wurden.

e-Government Anwendungen lassen sich in vier Bereiche unterteilen:

- die Beziehung Bürger-Verwaltung: Dieser Bereich deckt Prozesse ab, welche die Interaktionen zwischen Bürger und Verwaltung betreffen. Dabei wird davon ausgegangen, dass der Prozess vom Bürger initiiert wird und ein Portal genutzt wird, um mit Verwaltungsorganisationen in Kontakt zu treten [html1].
- die Beziehung Verwaltung-Verwaltung: Dieser Bereich deckt die verwaltungsinternen Prozesse ab, also solche Prozesse, welche von einer oder mehreren Verwaltungseinheit(en) bearbeitet werden.
- die Beziehung Verwaltung-Bürger: Ähnlich wie bei den Portalen geht es hierbei wiederum um Prozesse, welche eine Interaktion zwischen Bürger und Verwaltung beinhalten. Im Unterschied dazu ist bei der elektronischen Zustellung jedoch die Verwaltung die aktive Komponente, welche den Austausch anstösst [PR,03] [HL,04].
- e-Voting: Dieser Bereich wird getrennt von den anderen E-Government-Bereichen betrachtet, da er im Sicherheitsbereich einmalige Eigenschaften ausweist [NB,03].

Diese vier Bereiche decken zusammen das Spektrum von e-Government-Prozessen ab und geben somit eine geeignete Unterteilung für die Betrachtung der verschiedenen Sicherheitsbedürfnisse.

3. Sicherheitsaspekte von e-Government Projekten

Im vorherigen Abschnitt wurden die Gründe besprochen, E-Government in die Realität umzusetzen, dh die potentiellen Vorteile, die erreicht werden sollen. Die Einführung der elektronischen Verarbeitung hat jedoch auch mehrere inhärente Nachteile, welche in diesem Abschnitt teilweise aufgezeigt werden.

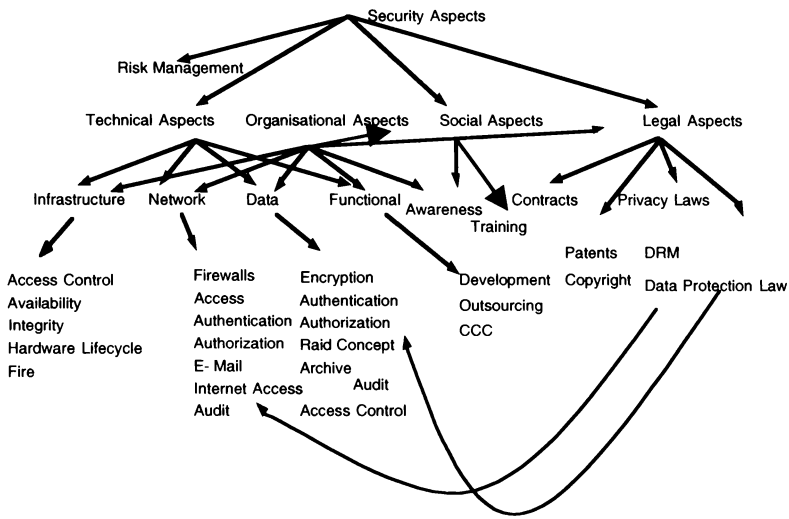

Abbildung 2: Sicherheitsbereiche in sicherheitsrelevanten Prozessen

Die Einführung der elektronischen Verarbeitung erlaubt es, viele Arbeitsprozesse zu automatisieren. Diese Automatisierung wirkt sich selbstverständlich auch auf die Sicherheit aus [FA,01]. Zunehmend werden auch Attacken auf Computersysteme automatisiert ausgeführt werden. Zusätzlich bietet die elektronische Verarbeitung auch einen Ansatz diverse schon früher existente Angriffszenarien mit einer stark reduzierten Anzahl an Mitwissern durchzuführen.

Abbildung 2 zeigt einen Überblick über die verschiedenen Sicherheitsbereiche [SH,03], welche für sensitive elektronische Prozesse relevant sind. Man kann daraus zwei Folgerungen extrahieren: Erstens gibt es nicht nur einen einzigen sicherheitsrelevanten Bereich, sondern nur eine Kombination verschiedener Bereiche, welche sich durch Berücksichtigung aller Aspekte ergibt, bietet eine stabile und sichere Umsetzung. Zweitens lassen sich die verschiedenen Sicherheitsbereiche nicht klar unterteilen, dh es

gibt keine klare baumartige Struktur. Querverbindungen auf verschiedenen Ebenen wie zB im Bereich Recht und Infrastruktur erhöhen den Grad der Sicherheit und ermöglichen gleichfalls eine Integration verschiedener Disziplinen.

Für den Bereich e-Government kann man die folgenden wichtigsten Sicherheitsbereiche festlegen:

- Die drei „A's", Grundlage jeglicher Sicherheitsarchitektur: Authentisierung (Kennwort, Smartcard, ...), Autorisierung (Zugriffsberechtigungen, Rollenkonzepte, ...) und Administration (Benutzerverwaltung, Systemunterhalt, Planungsprozesse, ...).
- Privatsphäre (Privacy): Auf Grund ihrer inhärenten Aufgaben arbeitet jede Verwaltung mit Daten, welche der Privatsphäre ihrer Klienten angehören. Diese Daten müssen entsprechend bearbeitet und gespeichert werden.
- Vertrauen (Trust): Technisch noch so durchdachte und ausgefeilte Sicherheitssysteme, welche auch bei internationalen Firmen im Einsatz sind, müssen nicht automatisch für e-Government Lösungen akzeptabel sein, da im Gegensatz zu obigen Systemen im e-Government eine zusätzliche Anforderung hinzukommt: Das Vertrauen des Endbenutzers (Bürgers).
- Integrität: Das System muss sicherstellen, dass niemand Daten verändern kann.
- Nachvollziehbarkeit: Im Rahmen der elektronischen Prozesse muss feststellbar sein, wann, wer, welche Änderungen durchgeführt hat. Erst damit wird die Absicherung gegenüber Datenmanipulationen durch interne Personen erreicht.
- Anonymität: In einzelnen Bereichen von E-Government – insbesondere im e-Voting – ergibt sich zusätzlich die Anforderung der Anonymität, dh dass ein Nutzer Aktionen ausführen kann (zB wählen), welche nicht auf Ihn zurückgeführt werden können dürfen.

Einige der obigen Bereiche sind allgemeingültig, dh sie sind auch ausserhalb von E-Government-Anwendungen relevant [DG,99]. Andere Bereiche jedoch sind entweder spezifisch für E-Government (zB Anonymität und Vertrauen) oder treten in E-Government-Umgebungen in einer ausgeprägteren Form auf (zB Privatsphäre).

Zur Erfüllung einiger der obigen Anforderungen bietet die Industrie bereits Technologien an, die sich in verschiedenen Umfeldern schon bewährt haben, zB:

- Verschlüsselung: Daten werden dahingehend manipuliert, dass nur Benutzer mit dem entsprechenden Schlüssel die Daten in verständlicher Form einsehen können [RG,02].

- Digitale Signatur: Vereinfach ausgedrückt versteht man darunter den elektronischen Ersatz der Unterschrift von Hand. Damit ist es möglich, zu überprüfen, ob ein Dokument tatsächlich von der erwarteten Person ausgeführt wurde.
- Smartcard: Physikalische Karte, welche sich in unserem täglichen Leben schon vollständig etabliert hat. Damit können Daten nicht nur auf Wissensbasis (wie bei Kennwörtern) geschützt werden [WRFE,99]. Der Einsatz von Smartcards ist in vielen Bereichen bereits gängig und wird in den nächsten Jahren wohl noch weiter ausgebaut werden. Erstrebenswert in diesem Zusammenhang sind multifunktionale Karten, die nicht nur für eine Anwendung einsetzbar sind [GOAR,96].
- Biometrie: Diese ermöglicht eine Authentisierung nicht durch die Kriterien von Wissen oder Besitz, sondern mit dem „Sein" an sich. Hierbei werden Körpermerkmale, zB das Muster der Iris, der Fingerabdruck oder persönliche Eigenschaften wie die Aussprache oder der Gang analysiert und mit einem entsprechenden Muster verglichen.
- Audit: Ein Audit ist ein fälschungssicheres Protokoll, welches die abgelaufenen Prozesse mitprotokolliert und damit sicherstellt, dass jedwede Änderung am System oder an den Daten im Nachhinein einer bestimmten Person zugeordnet werden kann.

Abbildung 3 zeigt die verschiedenen Sicherheitsbedürfnisse der e-Government-Komponenten, welche in Kapitel zwei vorgestellt wurden (aus Gründen der Übersichtlichkeit wurden nur die Hauptsicherheitsaspekte der einzelnen Bereiche markiert). Sie zeigt dabei deutlich, dass alle Komponenten sowohl mehrere als auch unterschiedliche Sicherheitsbedürfnisse haben.

	Portal	ELAK	Zustellung	e-Voting
Authentisierung	•	•	•	•
Autorisierung	•	•		
Privatsphäre	•		•	•
Nachvollziehbarkeit		•	•	
Verfügbarkeit				•
Anonymität				•
Integrität		•	•	•

Abbildung 3: Sicherheitsbedürfnisse der E-Government Komponenten

Für die Relevanz einer bestimmten Bedrohung sind zwei Faktoren entscheidend.

- Wahrscheinlichkeit: Damit ist die Wahrscheinlichkeit gemeint, mit der ein bestimmter Angriff durchgeführt wird.
- Schadenssumme: Diese bestimmt den maximalen Schaden, welcher durch einen bestimmten Angriff entstehen kann. Dies beinhaltet explizit nicht nur monetäre Schäden, sondern auch indirekte Schäden in anderen Bereichen, zB Stabilität des politischen Systems.

4. Zusammenfassung

Das Ziel dieses Beitrages war es, die Sensibilität des Lesers für Sicherheitsaspekte zu erhöhen. Bei allen e-Government-Projekten sollte Sicherheit höchste Priorität besitzen. Dies einerseits, weil der potentielle Schaden eines erfolgreichen Angriffes sehr groß sein kann und andererseits wegen der Natur des Systembenutzers spezielle Randbedingungen existieren. Der typische Anwender einer e-Government-Lösung ist nämlich kein Experte und besitzt in der Regel auch kein vertieftes Computer-Anwenderwissen.

Einen speziellen Status hat diesbezüglich der Bereich des e-Voting. Einerseits handelt es sich hierbei um eine Aktion, welche von den Bürgern sehr bewusst als wichtiges Werkzeug wahrgenommen wird. Andererseits stellt es bezüglich Anonymität und Verfügbarkeit spezielle Anforderungen, die an andere e-Government-Prozessen nicht oder nur in abgeschwächter Form gestellt werden.

In diesem Zusammenhang möchte der Beitrag als Anregung dienen, mit detaillierten Studien e-Government Projekte zu hinterfragen und dabei die beiden Dimensionen „Aufwand" versus „Ertrag", oder anders formuliert „Risiko" versus „Vereinfachung", einander gegenüberzustellen.

Referenzen

[SH,03] *Hof, S.* (2003), Security Aspects within e-Government. In Proceedings of the DEXA, 2003.

[html1] *Portalverbund Whitepaper,* www.cio.gv.at.

[PR,03] *Reichstädter, P.* (2003), Spezifikation Elektronische Zustellung, www.cio.gv.at

[FA,01] *Grundlagen Bedrohungen und Schutzmassnahmen, Arrigoini F.,* IT-Security Special, 1/2001, 2001.

[RG,02] *Gramer R.,* Signature Schemes Based on the Strong RSA Assumption, ACM Transactions on Information and System Security, Vol. 3, No. 3, August 2000, 161–185.

[NB,03] *Braun, N., P. Heindl,* et al. (2003), e-Voting in der Schweiz, Deutschland und Österreich ein Überblick. Arbeitspapiere zum Tätigkeitsfeld Informationsverarbeitung und Informationswirtschaft. Wien, Wirtschaftsuniv. 2003, 2.

[WRFE,99] *W. Rankel, W. Effing;* Handbuch der Chipkarten, Aufbau-Funktionsweise-Einsatz von Smart Cards, 1999, Carl Hanser Verlag, ISBN 3-446-21115-2.

[GOAR,96] *J. Gosling, K. Arnold;* The Java Programming Language. Addison Wesley, 1996 (ISBN 0-201-63455-4).

[DG,99] *Gollmann Dieter,* 1999. Computer Security (ISBN 0-471 97844 2).

[HL,04] *Lakatha H.,* Erfahrungen aus dem Betrieb eines Zustellservers, e|Gov Days 2004, Budapest und Wien, 2004-04-15.