Trusted Computing im Dienste von E-Government

von Marcel Winandy

Für eine sichere Kommunikation im E-Government ist der Einsatz vertrauenswürdiger Computersysteme und -programme ein wichtiger wie notwendiger Bestandteil. Trusted Computing Technologie könnte eine kostengünstige und effiziente Möglichkeit zur Bildung vertrauenswürdiger Kommunikationsinfrastrukturen sein.

E-Government verspricht eine effiziente Verwaltung durch die kostengünstige Nutzung des Internets. Die Vorteile sind viel versprechend: schnellere und genauere Datenerfassung, neue Möglichkeiten der Datenauswertung und kostengünstigere Abwicklung. So sollen Bürger und Bürgerinnen zukünftig nicht mehr lange im Amt warten müssen, sondern können ihre Anträge online am Computer ausfüllen und über spezielle E-Government-Portale eingeben. Ebenso soll die Kommunikation zwischen Wirtschaft und Verwaltung online abgewickelt werden, z.B. bei der Vergabe von öffentlichen Ausschreibungen.

Da die Übermittlung von Daten zu E-Government-Diensten über das Internet erfolgen soll, muss die Sicherheit der Daten und die Authentizität des Urhebers gewährleistet sein. Bewährte Verschlüsselungstechniken und Verfahren der Digitalen Signatur kommen dafür zum Einsatz – wie bereits im E-Commerce. Allerdings hat die Erfahrung im E-Commerce-Bereich gezeigt, dass diese Schutzmaßnahmen nicht ausreichend sind. Prominente Angriffe sind Phishing sowie Schadprogramme. Bei Phishing-Angriffen werden Anwender auf gefälschte Webseiten gelockt, um dort ihre Zugangsdaten für z.B. ihr Online-Banking einem Betrüger preiszugeben. Schadprogramme können sich auf dem Rechner des Anwenders einnisten, um dann PIN oder Passwort-Eingaben abzufangen oder Daten zu verändern. Letzteres ist besonders kritisch, wenn beispielsweise vor Abgabe der Steuererklärung ein Schadprogramm ohne Wissen des Benutzers die Zahlen fälscht, oder wenn ein Unternehmen ein Angebot für eine öffentliche Ausschreibung abgeben will und ein Schadprogramm heimlich den Preis anhebt, so dass auf jeden Fall die Konkurrenz den Zuschlag bekommen würde. Der Einsatz von Chipkarten kann dagegen leider nicht helfen, denn welche Daten letztendlich zu einer Signatur-Chipkarte für die Digitale Unterschrift geschickt werden, bewirken die Programme, die auf dem Rechnersystem des Anwenders laufen.

Die genannten Szenarien zeigen, dass der Einsatz vertrauenswürdiger Computersysteme und -programme im E-Government besonders wichtig ist. Aber wie kann man garantieren, dass der verwendete Computer des Anwenders vertrauenswürdig ist und dass keine manipulierten Programme oder Trojanische Pferde[1] darauf laufen? Diese Frage ist nicht trivial, da ein Computer zu Hause oder im Unternehmen auch für eine Vielzahl anderer Aufgaben neben dem E-Government verwendet wird. Die Gefahr, dass sich ein Schadprogramm einschleicht (z.B. aufgrund eines Downloads aus dem Internet aus nicht vertrauenswürdiger Quelle) oder die Rechnersoftware anderweitig manipuliert wird, ist groß. Dies resultiert nicht zuletzt aufgrund konzeptioneller Sicherheitsschwächen derzeit allgemein eingesetzter PC-Betriebssysteme.

Es gibt jedoch bereits heute kommerziell verfügbare Technologien, die dieser Gefahr entgegenwirken können. Trusted Computing, von der Trusted Computing Group[2] spezifiziert, ist eine kostengünstige Technologie, die Verfahren und Mechanismen bereitstellt für die Bildung vertrauenswürdiger IT-Infrastrukturen. Das Herzstück dieser Technologie ist das TPM (*Trusted Platform Module*), ein kleiner Computerchip, der auf die Hauptplatine des PCs angebracht wird. Das TPM bietet, ähnlich wie eine Smartcard, kryptographische Funktionen sowie geschützten Speicher für kleine Datenmengen. Dies kann genutzt werden, um kryptographische Schlüssel vor Manipulation oder Ausspähen zu schützen. Ferner können beim Hochfahren des Rechners Prüfwerte der geladenen Software (die sogenannte Plattformkonfiguration) in den geschützten Bereich des TPM geschrieben werden. Das TPM bietet die Möglichkeit, diese Prüfwerte mit bestimmten (vom TPM geschützten) Schlüsseln zu verknüpfen. Daraus

1 Ein Trojanisches Pferd ist ein Schadprogramm, welches vorgibt eine nützliche Funktion zu erfüllen (z.B. ein Texteditor), aber heimlich schädliche Aktionen ausführt (z.B. den Text vor dem Speichern böswillig abändert).

2 https://www.trustedcomputinggroup.org

resultieren zwei wichtige Verfahren: *Attestation* erlaubt die kryptographisch abgesicherte Überprüfung der Plattformkonfiguration von einem entfernten Rechner aus; *Sealing* kann den Zugriff von (verschlüsselten) Daten an die Plattformkonfiguration des Rechners binden.

Die Anwendung dieser Verfahren würde es ermöglichen, dass ein E-Government-Server vor dem Anmelden oder Hochladen von Dokumenten vorher prüft, ob der PC des Anwenders in einem „vertrauenswürdigen Zustand" ist, d.h. eine Plattformkonfiguration aufweist, die zuvor als gültig definiert wurde. Wenn jedoch ein Schadprogramm ausgeführt wird, würde dies die Prüfwerte verändern und der E-Government-Server kann den Vorgang ablehnen und eine Warnung ausgeben. Das zweite Verfahren, Sealing, würde es einem Anwender erlauben, bestimmte Dokumente lokal auf seinem Rechner so zu verschlüsseln, dass nur dann auf diese Dokumente zugegriffen werden kann (d.h. dass sie entschlüsselt werden könnnen), wenn sich Plattformkonfiguration nicht geändert hat. Auf diese Weise kann man verhindern, dass ein später eingenistetes Schadprogramm auf die Daten zugreift oder sie verändert.

Auch wenn es bereits eine Vielzahl von Herstellern gibt, die ihre PCs, Server, und Notebooks mit einem TPM-Chip ausliefern, genügt der Einsatz eines TPMs alleine nicht. Man braucht noch eine entsprechende Softwarebasis, die das TPM geeignet und effizient nutzt; mit anderen Worten: ein Trusted-Computing-fähiges Betriebssystem. Das aktuelle Microsoft Windows Vista nutzt zwar das TPM während des Hochfahrens für seine Festplattenverschlüsselung „Bitlocker", allerdings sind dies nur rudimentäre Funktionaliäten des TPM und schützt beispielsweise nicht die Ausführung kritischer Anwendung zu einem späteren Zeitpunkt.

Für einen umfassenderen Schutz wird eine sichere Ausführungsumgebung für E-Government Anwendungen benötigt, die heutige Betriebssystem (noch) nicht bieten. Es gibt allerdings viele Forschungs- und Entwicklungsprojekte, die an entsprechende Verbesserungen arbeiten. Ziel ist die Entwicklung eines Sicherheitskerns, der verschiedene Anwendungsbereiche auf einem Rechner isoliert voneinander ausführen kann und die Funktionen des TPMs nutzt, um die Bereiche zu schützen und gegenüber entfernten Rechnern zu attestieren. *Turaya*[3] ist ein Beispiel für einen derartigen Sicherheitskern, der aus einem vom Bundesministerium für Wirtschaft und Arbeit geförderten Forschungs- und Entwicklungsprojekt hervorgegangen ist und als Open Source verfügbar ist. *OpenTC*[4] ist ein von der EU gefördertes Projekt, welches die Entwicklung eines Trusted Computing Rahmenwerk für sichere Betriebssysteme als Ziel hat. Dies sind nur Beispiele, weitere Forschungs- und Entwicklungsarbeiten sind noch nötig. Aber erste Prototypen zeigen brauchbare Ergebnisse, die nicht zuletzt auch für ein sicheres E-Government eingesetzt werden können – und sollten.

Marcel Winandy ist wissenschaftlicher Mitarbeiter am Horst Görtz Institut für IT-Sicherheit der Ruhr-Universität Bochum. Er forscht im Bereich Trusted Computing und Sichere Betriebssysteme.

3 http://www.emscb.de/content/pages/About-Turaya-de.htm
4 http://www.opentc.net/