Die ePass Richtlinien: Teure Pseudosicherheit?

Bei der Einführung des elektronischen Passes, des „ePasses“, hat man ein Papierverfahren auf ein EDV-Verfahren umgestellt. Man hat versucht – und warum es lediglich einen Versuch darstellt wird im Folgenden dargelegt werden – einen Papierprozess mit seinen Sicherheitsanforderungen und Sicherheiten auf einen elektronischen Prozess umzusetzen. Hier wurden jedoch elementare Sicherheitsregeln und Grundsätze in der Sicherheit fast schon sträflich vernachlässigt.

Was zeichnet ein Papiersystem aus?

Ein Papiersystem hat einige grundsätzlich unterschiedliche Systemeigenschaften gegenüber einem IT-basierten System. Bei einem auf Papier basierenden System – also einem System, bei dem Anträge in Formularen gestellt werden – ist die Zahl der möglichen Manipulatoren überschaubar, denn diese benötigen den direkten physischen Zugriff auf das Papier und zwar auch noch dann, wenn der Antrag bereits die Daten enthält.
Die Druckerei, die die Vordrucke erstellt, kann diese Drucke nicht missbrauchen, da die Daten, die Unterschrift, die Stempel und der Versandweg fehlen. Der Stempelmacher hat weder das Formular, noch die Unterschrift, noch die Möglichkeit, den passenden Versandweg zu nutzen. Niemand anders als die damit betrauten Mitarbeiter der Antragsbehörde, der Versandbote und die damit betrauten Mitarbeiter der Bundesdruckerei haben diese Antragsformulare in einer geeigneten Form in Händen, um Nutzen daraus zu ziehen.

Was unterscheidet IT-basierte Systeme von Papiersystemen?

Bei IT-basierten Systemen gibt es sehr viel mehr potenzielle Zugreifer. Niemand muss physikalisch innerhalb eines engen Zeitraumes, wie es bei Papiersystemen notwendig ist, an die jeweiligen Daten kommen. Man kann Dinge lange im Voraus planen, die Liste der möglichen Zugreifer vervielfacht sich. So sind es innerhalb der Behörde plötzlich nicht mehr nur die direkt damit betrauten, sondern auf jeden Fall auch die Systemadministratoren. Es gibt auch Szenarien, in denen jeder Behördenmitarbeiter bis zur Putzfrau Daten unerkannt manipulieren kann. Dann

Team 4 Innovation GBR
Herbststr. 27
85737 Ismaning

Phone: +49 89 962 073 - 54
Fax: +49 89 962 073 - 55
Web: www.Team4Innovation.com
e-mail: info@team4innovation.com

erweitert sich der Kreis der potenziellen Zugreifer weit über die Behörde hinaus. So kann sich der Softwarehersteller durch den Einbau von Hintertüren – sei es zur Wartung, zur Qualitätskontrolle oder auch aus Eigeninteressen – den Zugriff auf solche Systeme sichern. Auch die Softwarewartung ist nicht unproblematisch, denn sobald ein Helpdesk besteht, der im Problemfall dem Benutzer Online helfen kann, besteht dort natürlich ebenfalls die Möglichkeit, Dinge zu manipulieren. Man muss also den Kreis, der als zuverlässig zu definierenden Personen extrem erweitern.

Das alles sind alleine jedoch erst die internen Sicherheitsaspekte. Nachdem Systeme heute vernetzt sind – und es ja auch sein müssen –, besteht auch die Gefahr durch Angriffe von außen mittels direkter Versuche, Trojaner, Würmer, etc.

Den Versuch, einen Tresor unberechtigt zu öffnen, erkennt jeder Laie, einen Angriff auf IT-Ebene oftmals selbst ein Experte nicht.

Wenn man den Bundestrojaner als Methode zum Auslesen von Daten auf Privatrechnern in Betracht zieht und selbst gut geschützte Systeme, wie die des Bundeskanzleramtes, des Wirtschafts- und Forschungsministeriums und des Auswärtigen Amts vor Angriffen mit Trojanern nicht sicher sind, dann kann man Systeme in Städten und Gemeinden nicht als sicher betrachten. Man man muss sie realistischerweise als sicherheitstechnisch potenziell unsichere Systeme betrachten. Es müssen also Wege gefunden werden, dass diese Systeme – selbst bei einer Manipulation – nicht missbraucht werden können.
Die Notwendigkeit, die Daten verschlüsselt zu versenden, versteht sich eigentlich von selbst. Jedoch ist eine Verschlüsselung, so gut sie auch sein mag, vollkommen sinnlos, wenn sie einfach durch das Hacking eines Quellsystems umgangen werden kann oder durch das Kopieren eines Zertifikates mittels eines Trojaners.

Was ist ein sicheres System?

Ein sicheres System per se gibt es nicht und wird es niemals geben. Es gibt aber die Möglichkeit, möglichst viele Risiken aus einem System auszuschließen und somit zu einem sehr sicheren System zu kommen. Der erste Schritt, um ein System zu bewerten, ist die Klassifikation der einzelnen Teilnehmer in Sicherheitsklassen. Entscheidende Kriterien sind:

- Wo steht der Teilnehmer?
- Sind die Teilnehmerparameter durch den eigentlichen Systembetreiber steuer- und kontrollierbar?
- Hat das Teilnehmersystem Verbindungen zur Außenwelt und welcher Art sind diese?
- Ist das Teilnehmersystem manipulationssicher?
- Wie viele Personen haben direkt oder indirekt (auch über das Netzwerk) Zugriff auf das Teilnehmersystem?

Team 4 Innovation GBR
Herbststr. 27
85737 Ismaning

Phone: +49 89 962 073 - 54
Fax: +49 89 962 073 - 55
Web: www.Team4Innovation.com
e-mail: info@team4innovation.com

- Ist das Teilnehmersystem eine Embedded-Lösung für nur eine einzige Aufgabe oder ist das Gerät dazu in der Lage, unterschiedlichste Software auszuführen?
- Wird Standard-Hardware eingesetzt oder handelt es sich um proprietäre Hardware?
- Gibt es nach außen hin nutzbare bzw. manipulierbare Schnittstellen?

Diese Kriterien sind wie folgt zu bewerten:

- Je weiter ein Gerät öffentlich zugänglich ist, desto höher sein Unsicherheitspotenzial.
- Je weniger Einfluss auf das Gerät genommen werden kann, desto unwägbarer sind die von ihm ausgehenden Gefahrenpotenziale.
- Manipulationssicherheit ist vor allem bei nicht direkt kontrollierbaren Geräten ein entscheidendes Sicherheitskriterium.
- Je mehr Personen auf ein solches Gerät Zugriff haben, desto gefährdeter ist es.
- Embedded-Lösungen, die möglichst manipulationssicher aufgebaut sind, sind in weit verstreuten Anwendungen das Mittel der Wahl. Bei Geräten, die grundsätzlich dazu in der Lage sind, unterschiedlichste Software auszuführen, ist Manipulationsversuchen von Anfang an Tür und Tor geöffnet.
- So vorteilhaft Standard-Hardware und standardisierte Schnittstellen im Kosten / Nutzenverhältnis auch sein mögen und so gut dies auch für „normale“ Anwendungen funktioniert, so falsch ist es, im Sicherheitsbereich Standardgeräte einzusetzen. Diese sind bekannt, genauso wie deren Schwächen und deren Programmierbarkeit. Somit lässt sich Standard-Hardware einfach angreifen. Jeder Hacker weiß, was er dazu tun muß.
- Schnittstellen sind Fluch und Segen zugleich. Sie vereinfachen die Datenkommunikation, machen aber auf demselben Wege Manipulation möglich. Wenn man heute an einen PC einen USB-Stick anschließen kann, so kann man darauf dringend benötigte Daten von einem Rechner zum anderen transportieren, man kann aber genauso spezialisierte Schadsoftware unauffällig in ein Gerät einschleusen. Schnittstellen sollten im Sicherheitsbereich also lediglich für den benötigten Datenaustausch zur Verfügung stehen und weitere Fähigkeiten erst gar nicht mitbringen.

Betrachtung des Gesamtsystems nötig

Ein System ist immer so sicher wie sein schwächstes Glied.

Das heißt nichts anderes, als dass alle Anstrengungen für eine hohe Sicherheit vergebens sind, wenn nicht von **allen** Systemteilen die notwendigen

Team 4 Innovation GBR
Herbststr. 27
85737 Ismaning

Phone: +49 89 962 073 - 54
Fax: +49 89 962 073 - 55
Web: www.Team4Innovation.com
e-mail: info@team4innovation.com

Sicherheitsstandards erfüllt werden.
Als einfaches Beispiel lässt sich das Verschlüsselungskonzept für E-Mails „Pretty Good Privacy“ (PGP) nennen. PGP ist an und für sich ein sicheres System. Wenn man jedoch den Rechner, auf dem der „Private Key“, also der Entschlüsselungscode, hinterlegt ist, angreift und diesen ausliest, dann hilft die ganze Verschlüsselung nichts mehr. Eine andere Möglichkeit zur Manipulation funktioniert folgendermaßen:,
Man hackt das E-Mail-Postfach eines Empfängers, dann schickt man den Sendern an dieses Postfach nicht – wie vorgesehen – den originalen „Public Key“ (mit dem originalen Verschlüsselungs-Code) , sondern man schickt ihnen einen neu generierten Public-Key. Dadurch kann man die gesendeten Dokumente abfangen, mit dem eigenen Private-Key entschlüsseln und danach mit dem Public-Key des eigentlichen Empfängers wieder verschlüsseln. Man kann sich das ganze auch noch vereinfachen, in dem man eine neue E-Mail Adresse erstellt und diese als neue Empfängeradresse bekannt gibt. Somit kann man sich selbst das hacken der E-Mail Adresse sparen.

Man sieht daran, dass die beste Verschlüsselung durch das genutzte Protokoll bzw. die genutzten Strukturen schlicht und ergreifend nichtig werden kann.

Es ist also nicht die Verschlüsselung entscheidend, sondern in demselben Maß das Protokoll und mögliche andere Schwachstellen.

Die schwächste Stelle definiert die Sicherheit des Systems.

Lücken im ePass System:

Der ePass, definiert durch die technische Richtlinie BSI TR-03104 Annex 3 (XPass-Datenmodell), ist ein System, das leider derart viele Sicherheitslücken aufweist, wie man es beim heutigen Stand der Sicherheitstechnik kaum für möglich halten würde. Das Ganze erinnert an einen Raum, den man aus Leichtbauwänden baut und mit einer Tresortüre abschließt, um sich dann darüber zu wundern, warum ein Dieb mit einer Kettensäge die Wand aufschneidet, wo doch der Zugang über die Tresortüre so gut gesichert ist. Essenzielle Sicherheitsregeln werden missachtet.

Das beginnt bereits damit, dass man die Netze der Städte und Gemeinden – also der Beantragungsbehörden – als sicher definiert. Ansonsten würde man keinesfalls tolerieren, dass die ePass Clientapplication auf einem ganz normalen PC in einer Gemeinde oder Stadt läuft, der sich ganz normal in deren Netz befindet. Wie will man denn die Sicherheit dieser vielen Rechner und Netze gewährleisten? Bei vielen Gemeinden wird das Netzwerk durch externe Firmen betreut und das in teilweise sehr großen Zeitabständen. Sicherheitssysteme wie Intrusion Detection Systeme, Firewalls, Virenscanner bieten nur eine relative Sicherheit und gerade Firewalls und Intrusion Detection Systeme müssen regelmäßig gewartet und überprüft werden.

Team 4 Innovation GBR
Herbststr. 27
85737 Ismaning

Phone: +49 89 962 073 - 54
Fax: +49 89 962 073 - 55
Web: www.Team4Innovation.com
e-mail: info@team4innovation.com

Selbst in größeren Strukturen wie Landkreisen ist das Auftreten von Virenbefall keine Seltenheit und spätestens seit der Diskussion um den sogenannten Bundestrojaner sollte selbst dem letzten Laien klar sein, dass die Sicherheit von mit dem Internet verbundenen Systemen kaum - oder in normalen Betriebs- und Behördenstrukturen gar nicht – gewährleistet werden kann. Standard-PCs sind darüber hinaus äußerst angreifbar – selbst wenn sie unter Linux liefen, was aber in Bayern definitiv nicht der Fall ist. Selbst die Linux-Lösung der Stadt München bietet kaum mehr Sicherheit, da für viele Fachverfahren auf ein virtuelles oder emuliertes Windows zurückgegriffen werden muss und somit die Probleme wieder vorhanden sind.
Auch Linux ist nicht unangreifbar. Nicht umsonst gibt es – ähnlich wie unter Windows – für die Distributionen regelmäßige Updates und Virenscanner. Mit zunehmender Verbreitung wird sich auch dort das Problem verschärfen. Auch Apples MacOS ist keineswegs gegen Angriffe gefeit.
Ein solcher ePass-Clientrechner ist für jeden Mitarbeiter, der an diesem Rechner eine Anmeldeberechtigung hat, zugreifbar und erfahrungsgemäß werden die Anmelderechte in der Praxis nicht auf bestimmte Rechner eingeschränkt. Des weiteren hat die Softwareherstellerfirma oftmals einen Helpdesk–Zugang auf diese Rechner. Schon jetzt ist die Anzahl der möglichen Zugreifer und Nutzer pro betroffenem Rechner fast unüberschaubar. Ganz davon zu schweigen, wie sich das Ganze multipliziert, wenn es einem Hacker gelingt, auch nur auf einem Rechner innerhalb der Gemeinde einen Trojaner zu platzieren, der sich selbst weiterverbreitet.

Die Platzierung eines solchen Trojaners ist denkbar einfach:
Viele Nutzer öffnen immer noch E-Mails, deren Inhalt Ihnen nicht ganz klar ist, selbst wenn aktuelle Virenwarnungen innerhalb eines Unternehmens bzw. einer Behörde ausgegeben wurden. Die Wahrscheinlichkeit für dieses Szenario ist also recht hoch. Wären die Daten auf diesem Rechner nicht im Klartext verfügbar – und das ist der nächste schwere Systemfehler – dann wäre das Ganze gar nicht sonderlich problematisch. Man hat jedoch auch dort einige Kardinalsfehler gemacht:

1. Sämtliche Personendaten werden direkt und unverschlüsselt über die normale PC-Tastatur eingegeben.
2. Die Passbilder werden über einen handelsüblichen Standardscanner unverschlüsselt eingescannt.
3. Die Fingerprintscanner wurden vom BSI nur wegen der Scanqualität zertifiziert, jedoch ging es dabei in keinster Weise um Sicherheit. Diese Geräte liefern ein schlichtes Bild an den unsicheren PC.
4. Peripheriegeräte werden und können über USB an den aufnehmenden PC angeschlossen werden. Im schlimmsten Fall auch über das Netzwerk.
5. Die Signaturen sind auf dem Rechner hinterlegt bzw. dort aus- oder mitlesbar.
6. Die Verschlüsselung erfolgt – sofern hier nicht das erteilte Patent DE 10 2005 014 194 der Gesellschafter der Team4Innovation GBR verletzt wird – mittels fester Schlüssel. Diese müssen hinterlegt sein und sind somit für dritte auch auslesbar. Selbst das dem Patent DE 10 2005 014 194 entsprechende Protokoll wäre im Einsatz auf einem Standard-PC nicht sicher.

Team 4 Innovation GBR
Herbststr. 27
85737 Ismaning

Phone: +49 89 962 073 - 54
Fax: +49 89 962 073 - 55
Web: www.Team4Innovation.com
e-mail: info@team4innovation.com

Es ist also festzustellen, dass sämtliche aufgenommen Daten jederzeit problemlos auf den ePass Client PCs verfügbar sind. Eine Manipulation ist mit diversen Trojanern oder Würmern möglich.
Es geht aber auch noch weiter: So wäre es auch möglich, sich den Schlüssel und die Signatur zu kopieren und ein der Technischen Richtlinie BSI_TR_03104_A3_V21 entsprechendes Dokument zu erstellen.
Es ist also für Kriminelle nun möglich, was früher beinahe unmöglich erschien: Den Wunsch-Reisepass mit dem eigenen Bild zu versehen und sogar mit dem eigenen Fingerabdruck, einem Wunschnamen und einer Wunschadresse auszustatten – kurz: Mit einer falschen Identität. Das ganze kann man sich dann von der Bundesdruckerei erstellen lassen und verfügt somit über einen echten gefälschten Reisepass mit sämtlichen Sicherheitsmerkmalen.

Nur Horrorphantasie oder schöne neue Welt?

Die beschriebenen Verfahren sind leider keine Phantasie. Es handelt sich hier um ein einfach durchzuführendes Szenario. Für Kriminelle ist die Übernahme von Rechnern heute Routine, es gibt etliche Anbieter, die Werbemailversand oder sogar Sicherheitsangriffe über sogenannte Zombie-Rechner anbieten. Die für die Übernahme eines Behördenrechners benötigten Werkzeuge sind dieselben. Zudem ist es noch viel einträglicher, als Spam-Versand anzubieten.
Es ginge jedoch noch viel leichter. So ist ein Szenario denkbar, in dem man ein altbekanntes Remote-Desktop-Tool wie VNC oder eher Ultra-VNC in einer modifizierten, vorkonfigurierten Form mit einer automatisierten Installationsroutine zusammen auf einen USB-Stick nimmt und beim Passamt der Gemeinde seines Vertrauens in einem unbeobachteten Moment durch kurzes Aufstecken und wieder Abziehen des USB-Sticks platziert.
Hierfür muss man kein Genie sein, ein wenig Konfigurationsarbeit reicht vollkommen aus.
Früher hätte man einen Verbündeten an passender Stelle innerhalb des Passamtes einer Behörde benötigt. Diese bürokratischen Hürden muss man heute nicht mehr nehmen.
In der Geschichte hat sich gezeigt, dass Kriminelle das, was technisch möglich ist, auch umsetzen, sofern es einen hohen Gewinn verspricht.

Warum wir den Beweis nicht antreten?

Wir sind keine Kriminellen und die hier beschriebenen Schritte sind äußerst kriminell. Aber sollte nicht die nachvollziehbare Beschreibung des Vorgehens alleine schon ausreichend sein, um einen solchen – die innere und äußere Sicherheit dieses

Team 4 Innovation GBR
Herbststr. 27
85737 Ismaning

Phone: +49 89 962 073 - 54
Fax: +49 89 962 073 - 55
Web: www.Team4Innovation.com
e-mail: info@team4innovation.com

Landes bedrohenden – Irrsinn zu stoppen und sichere Methoden einzusetzen?

Wie geht es denn sicher?

1. Ein sicheres Zentralsystem:

   Die Basis für ein sicheres System mit einer Zentrale ist natürlich eine sichere Zentrale. Sicherheit wird hier durch einige, meist unbeachtete Faktoren gewährleistet.
   So sollte das ePass-Zentralsystem komplett abgeschottet vom restlichen Netzwerk der Bundesdruckerei laufen. Zugriff auf dieses System hat nur eine kleine, überschaubare Anzahl von Personen. Von keinem der sich in diesem Zentralsystem-Netzwerk befindlichen Rechner wird eine nicht unbedingt notwendige Verbindung von innen nach außen aufgebaut. E-Mails und Internet-Browser-Nutzung sind für ein solches System ein absolutes Tabu.
   Die Daten werden aus diesem Zentralsystem über Schnittstellen direkt an das Produktionssystem weitergegeben. Dazwischen befindet sich eine interne Firewall.
   Die Voraussetzungen, die für das Zentralsystem gelten, gelten ebenfalls für das Produktionssystem.
   Nach außen wird jeglicher Verkehr – bis auf den tatsächlich benötigten – durch Firewalls (mindestens 2 unterschiedliche hintereinander) gesperrt.

2. Sichere Client-Prozesse:

   Kein Windows- oder Linux-PC ist sicher oder kann als dauerhaft sicher gelten, denn auf ihnen können beliebige Programme ausgeführt werden. Daher sollten wichtige Daten unabhängig vom Rechner erhoben und verschlüsselt werden. Auch die Verschlüsselung sollte für jeden neuen Vorgang wieder einen neuen Schlüssel generieren. Das Protokoll sollte Manipulationsversuche erkennen.
   Zur Authentifizierung werden keine Signaturen verwendet, sondern biometrische Daten, die bei jedem Vorgang erneut bestätigt werden müssen.

Ist das denn Stand der Technik?

Diese Frage kann mit einem klaren Ja beantwortet werden. Das 4Security System unserer Firma Team4Innovation GBR beschreibt ein solches Vorgehen schon seit langem. Das Bundesinnenministerium hatte über Unterlagen, die Herrn Bundesinnenminister Schily a. D. direkt überreicht wurden, mehrmals Kenntnis von diesem System bekommen.
Es gab kein Interesse an dieser Lösung. Vielleicht will man ja gar nicht so sicher sein.

Team 4 Innovation GBR
Herbststr. 27
85737 Ismaning

Phone: +49 89 962 073 - 54
Fax: +49 89 962 073 - 55
Web: www.Team4Innovation.com
e-mail: info@team4innovation.com

Jedoch sehen wir in dem nun eingeführten System die unsicherste aller möglichen Lösungen und ob ein derartiger Umgang mit sensiblen Daten im Sinne des Datenschutzgesetzes ist, möchte man auch bezweifeln.

Weswegen wir uns die Mühe hierfür machen

Es geht hier nicht nur um das Thema, die eigene Lösung verkaufen zu wollen. Als Bürger sind wir ebenso betroffen und deshalb wäre uns eine andere – sicherere – Lösung, die nicht aus unserem Systemhaus stammt, deutlich lieber als das jetzige System.
Es zeigt sich einmal wieder, dass das Bundesinnenministerium und das diesem unterstellte BSI augenscheinlich wenig Kompetenz im Bereich Sicherheit aufweisen.

Autor:
Axel Ahnert – Technischer Leiter Team4Innovation

Dieser Text ist ausdrücklich zur Veröffentlichung freigegeben.
Wir freuen uns über Ihre Rücksprache bezüglich weiterer Informationen und Bildmaterial

Team 4 Innovation GBR
Herbststr. 27
85737 Ismaning
Phone: +49 89 962 073 - 54
Fax: +49 89 962 073 - 55
Web: www.Team4Innovation.com
E-Mail: info@team4innovation.com