Wettbewerbsbeitrag zum
Deutschen IT-Sicherheitspreis 2016

Verfahren für eine neue Dimension von Internetsicherheit

Rudolf Philipeit
buergerservice.org e.V., Berliner Str. 5, 91522 Ansbach
E-Mail: rudolf.philipeit@buergerservice.org

14. Januar 2016

Zusammenfassung

Technologien für IT-Sicherheit stehen heute in sehr großem Umfang zur Verfügung und werden situativ in unterschiedlichsten Qualitätsstufen zum Einsatz gebracht. Für eine neue Dimension von Internetsicherheit mit neuen Diensteangeboten müssen bestimmte dieser Technologien in der breiten Masse auf Akzeptanz und Nutzung stoßen. Das hier beschriebene Verfahren greift diese Herausforderung auf.

1 Stand der Forschung/Technik

Forschung und Technik im Bereich der IT-Sicherheit haben mit der Entwicklung des Internet vielfältige Sicherheitslösungen für die Komponenten und Dienste in diesem Netz hervorgebracht. Abgrenzbare Netzwerke wie Intranets oder Extranets lassen sich damit relativ sicher betreiben. In Abhängigkeit des jeweiligen Schutzbedarfs kommen die passenden Sicherheitslösungen nach dem Stand der Technik zum Einsatz und werden in vielen Fällen vom Gesetzgeber sogar gefordert.

Im öffentlichen Internet hingegen konnten sich in der breiten Masse wichtige IT-Sicherheitslösungen nach dem Stand der Technik bisher nicht durchsetzen. Das betrifft im Besonderen Lösungen zur Identifikation, zur Authentifikation und zur Verschlüsselung.

Als Stand der Technik ist für Identifikation, Authentifikation und Verschlüsselung u. a. die Online-Ausweisfunktion des neuen Personalausweises der Bundesrepublik Deutschland anzusehen. Das Gesamtsystem ist zertifiziert und leistet für Anwender und Anbieter höchste technologische und rechtliche Sicherheit:

- Die verwendeten Protokolle und Mechanismen haben sich gegen alle Angriffsversuche bewährt. Sie sind international anerkannt und etabliert.
- Alle Daten werden vom Ausweis bis zum Diensteanbieter verschlüsselt übertragen (sog. Ende-zu-Ende-Verschlüsselung).
- Die eingesetzten Komponenten werden nach den Vorgaben und Technischen Richtlinien des BSI entwickelt und geprüft.
- Studien bestätigen die hohe Sicherheit der Sicherheitstechnologien.
- Zum Schutz der Daten ist eine Übertragung vom Chip nur unter bestimmten Voraussetzungen möglich:
    - Im Gegensatz zu einfachen Funkchips, wie sie z. B. in Schlüsselkarten oder Skipässen verwendet werden, ist der Personalausweis nur mit einem gültigen Berechtigungszertifikat auslesbar. Ein unbemerktes Auslesen ist nicht möglich.
    - Vor jeder Datenübermittlung prüft der Ausweis, ob ein gültiges Berechtigungs-zertifikat vorliegt, also dem Anfragenden die Daten übermittelt werden dürfen.
    - Die persönlichen Daten werden nur übermittelt, wenn die 6-stellige PIN eingegeben wurde (2-Faktor-Authentifizierung).
    - Alle Informationen und Übertragungen sind mit international etablierten technischen Verfahren (Verschlüsselung und Signatur) sicher geschützt.

Demgegenüber steht im täglichen Gebrauch des Internet durch die Nutzer ein über zwanzig Jahre alter Stand der Technik: Benutzername und Passwort. Dieses rein softwarebasierte Sicherheitssystem wurde durch zunehmenden Datenklau immer unsicherer und kann heute nur noch für unkritische Dienste verwendet werden.

2 Idee

Unsere Beobachtungen zum Thema IT-Sicherheit in den letzten Jahren, besonders im Zusammenhang mit der Einführung des neuen Personalausweises (nPA) und seiner Online-Ausweisfunktion (eID), haben als Ausgangspunkt für die nachfolgend beschriebene Idee folgendes Bild ergeben:

> Das öffentliche Internet hat sich im freien Spiel eines weitgehend unregulierten Marktgeschehens international als Spaß-Internet entwickelt. Dienste wie eBay, Facebook, WhatsApp usw. wurden dabei alltäglich. Das easy to use-Konzept dieser Dienste hat keinen Raum für anspruchsvolle IT-Sicherheit gelassen. Im bildhaften Vergleich kann man das heutige öffentliche Internet mit einer überdimensionalen Autoscooter-Anlage vergleichen. Leichtigkeit beim Fahren (nur Gasgeben und Lenken - keine Bremse, keine Gangschaltung, keine Verkehrsregeln, kein Führerschein), unerkanntes Anrempeln, risikoarmer Diebstahl von Gegenständen aus den offenen Fahrzeugen und die Abhängigkeit vom stromgebenden Anlagenbetreiber sind als Analogien leicht wiederzuerkennen.
>
> Niemand kommt bei einem Autoscooter auf die Idee, ein KFZ-Nummernschild (entspricht der Online-Ausweisfunktion des nPA) anzubringen oder eine Bremse (entspricht Metadaten zur Umsetzung des Rechts auf Vergessens) einzubauen usw.
>
> Gleichwohl wissen wir aus der realen Welt, dass es neben dem Spaß-Autoscooter auch einen Straßenverkehr mit einem enormen Nutzenpotential gibt. In diesem Straßenverkehr hat auch jedermann freie Fahrt, solange kein anderer Verkehrsteilnehmer beeinträchtigt wird und auch die eigene Sicherheit größtmöglichen Schutz erfährt (Sicherheitsgurt, Airbag). Um dies zu gewährleisten, sind eine eineindeutige hoheitliche Identifikation (KFZ-Nummernschild), eine Authentifikation (Autoschlüssel) und eine Verschlüsselung (geschlossene Fahrzeuge) das Fundament für die Infrastruktur des Straßenverkehrs.

Die hier beschriebene Idee - Verfahren für eine neue Dimension von Internetsicherheit - geht bewusst nicht darauf ein, wie die „Autoscooter-Anlage“ sicherer gemacht werden könnte. Dieses Vorhaben wird bereits von vielen Marktteilnehmern seit langer Zeit betrieben. Stattdessen ist die Frage, wie es in unserer Gesellschaft gelingen kann, neben der unsicheren „Autoscooter-Anlage“ einen sicheren „Straßenverkehr“ nach obigem Bild zusätzlich im Internet entstehen zu lassen.

Grundlage der Idee ist ein kostenfreies Linux-Live-System mit der derzeitigen Bezeichnung „BuergerDVD“ zusammen mit einem kostengünstigen Kartenlesegerät für den nPA. Der Begriff Live-System oder Direktstartsystem bezeichnet in der Informatik ein Betriebssystem, das ohne Installation und Beeinflussung des Inhaltes einer im System vorhandenen Festplatte gestartet werden kann. Ein eigens für die nPA-Anwendung gebootetes Betriebssystem ist somit total unabhängig vom PC und dem darauf verwendeten Betriebssystem. Dem Benutzer wird für ein Höchstmaß an Sicherheit jegliche Änderungsmöglichkeit entzogen. Das gesamte Betriebssystem befindet sich auf einem bootfähigen Medium wie CD-ROM, DVD oder einen Flash-Speicher, beispielsweise einem USB-Stick mit Schreibschutz. Ein Rechnerstart kann so auch ohne Festspeicher oder ohne vorinstalliertes Betriebssystem ermöglicht werden.

Das System ist so konzipiert, dass sich kein Eindringling dauerhaft in das System einnisten kann. Nach jedem neuen Startvorgang mit der Software der BuergerDVD steht ein sauberes, neutrales Betriebssystem nach dem plug&play-Gedanken für die Nutzung aller Dienste mit Online-

Ausweisfunktion zur Verfügung. Selbst kostengünstige Kartenlesegeräte für den nPA zum Preis von ca. 20 Euro können hier sicher verwendet werden.

Der aktuelle Entwicklungsschritt bei den Ideengebern ist die Integration des Linux-Live-Systems auf einem schreibgeschützten USB-Stick zusammen mit einem nPA-Kartenlesegerät, einem UMTS-Datenstick (für eine gesicherte Internetverbindung) und einem gegen BadUSB gesicherten USB-Hub in einem Gehäuse. Der Schutz gegen BadUSB wird bei diesem Gerät in der Form umgesetzt, dass keine Eingabegeräte an diesen USB-Anschlüssen zugelassen werden, sondern nur USB-Sticks vom Benutzer zum Einbringen und Ausgeben von Dokumenten. Diese Komponente wird derzeit als SID-Box (sichere ID-Box) bezeichnet. Zusammen mit einem Standard-PC stellt die SID-Box ein nPA-Terminal dar.

Abbildung 1 Die SID-Box beinhaltet Betriebssystem, nPA-Kartenlesegerät und gegen BadUSB geschützte USB-Anschlüsse. Die SID-Box wird per USB an einen bootfähigen USB-Anschluss eines Standard-PCs angeschlossen. Der nPA wird zum Auslesen auf die SID-Box aufgelegt.

Verbindungen mit der SID-Box werden z. Zt. nur zugelassen, wenn es sich um Diensteangebote für die Online-Ausweisfunktion des Personalausweises handelt. Da sich hier beide Seiten mit einem hochsicheren Zertifikatssystem gegenseitig ausweisen, kann auch kein Man in the Middle-Angriff das Gesamtsystem kompromittieren.

Zusammenfassung der Idee

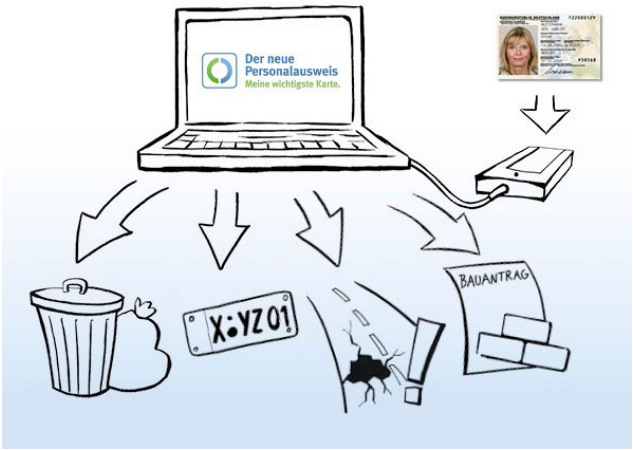
Das Zusammenspiel eines geschlossenen Betriebssystems (Linux-Live-System) auf einer kontrollierten Hardware (SID-Box) mit abgeschotteten Verbindungswegen zum Internet (UMTS-Verbindungen) und einem abgegrenzten und überwachten Diensteangebot (Dienste für die Online-Ausweisfunktion) ermöglicht ein bisher unerreichtes Sicherheitsniveau für ein ganz neues Angebot an digitalen Diensten für alle in Deutschland. Die sehr kostengünstige Herstellung der Endgeräte (vorhandener Standard-PC + SID-Box = nPA-Terminal) erlaubt eine massenhafte Verbreitung von nPA-Terminals an allen denkbaren Konzentrationspunkten (Behörden, Institutionen, Unternehmen, Banken, Versicherungen, Vereine, Schulen usw.). Damit entstehen vertrauenswürdige Knotenpunkte (Digital Service Points) zur sicheren Abwicklung von elektronischen Geschäftsvorfällen für jedermann.

3 Nutzen

Der Nutzen der beschriebenen neuen Dimension von Internetsicherheit ist für jeden erlebbar. Ähnlich wie mit Einführung der EC-Karte und den Geldausgabeautomaten der Zugang zum Bargeld erleichtert wurde, so werden mit dem nPA und den nPA-Terminals die Zugänge zu heute noch analogen Diensten (z.B. Post-Ident, Behördengänge, Kauf hochwertiger Güter usw.) erleichtert.

Allein die heute bereits vorhandenen Diensteangebote für die Online-Ausweisfunktion schaffen an vielen Stellen sofort einen Mehrwert:

- Studierende benötigen in bestimmten Studiengängen zur Abschlussprüfung ein Führungszeugnis. Dieses kann mit dem nPA elektronisch, also ohne den Weg zum evtl. hunderte von Kilometern entfernten Wohnortmeldeamt, an einem nPA-Terminal in der Hochschule beantragt werden.
- Eine aktuelle Rentenauskunft ist in unterschiedlichen Situationen notwendig, beispielsweise während der Beratung zur finanziellen Vorsorge fürs Alter in der Bankfiliale, oder bei der Diskussion zu Altersteilzeitmodellen im Betrieb. In all diesen Fällen kann ein vorhandenes nPA-Terminal den Weg zum Amt und das zeitverzögerte Wiederaufnehmen des Gesprächs vermeiden.
- Das Abmelden oder Ummelden von Kraftfahrzeugen kann z. B. ohne Wartezeit in der KFZ-Zulassungsstelle an einem nPA-Terminal im Autohaus erfolgen.
- Ein De-Mail-Account kann ohne aufwändigen analogen Identifizierungsprozess online beauftragt werden.



Neben dieser kleinen Beispielauswahl stehen bereits über 100 weitere Dienste für den nPA bereit. Besonders bedeutsam ist hierbei, dass immer beide Seiten von der Nutzung der Online-Ausweisfunktion profitieren: der Diensteanbieter und der Dienstenutzer. Damit ist gewährleistet, dass durch die Anschubsituation mit Hilfe der nPA-Terminals eine Eigendynamik möglich ist. Der Nutzen steigt mit neuen Diensten exponentiell an und ermöglicht ab einem gewissen Zeitpunkt sogar eine Diffusion in das bereits etablierte und noch unsichere Spaß-Internet.

4 Marktchancen

Bereits heute haben ca. 35 Mio. Bürgerinnen und Bürger in Deutschland den neuen Personalausweis mit Online-Ausweisfunktion erhalten. Bis zum 31.10.2020 ist der nPA bei nahezu jedem Einwohner ab 16 Jahren vorhanden. Wurde die Online-Ausweisfunktion nicht bereits bei der Abholung eingeschaltet, so kann diese gegen eine Gebühr von 6 Euro aktiviert werden. Die Infrastruktur Online-Ausweis beinhaltet dabei neben der Online-Ausweisfunktion auch die komplette Administration (PIN-Puk-Brief, Sperrhotline, Fahndungslisten bei Diebstahl/Verlust, Überwachung der Diensteanbieter usw.). Für diese Infrastruktur hat unsere Gesellschaft bis zum Jahr 2020 ca. 2 Mrd. Euro alleine bei den Gebühren für den nPA bezahlt. Diese Investition von uns allen soll mit der oben beschriebenen Idee für unsere Gesellschaft aktiviert werden.

Die bereits heute vorhandene kritische Masse von 35 Mio. Online-Ausweisen erlaubt die sofortige Umsetzung der Idee. Um wettbewerbsneutral jeden Konzentrationspunkt für ein nPA-Dienste-angebot erreichen und im Sinne der Idee aktivieren zu können, wurde der gemeinnützige Verein buergerservice.org e.V. ausgesucht. Der Vereinszweck ist hier das Vermitteln von Medienkompetenz zur Online-Ausweisfunktion des Personalausweises. Es ist somit eine Symbiose zwischen der Herausgabe der SID-Box als Endgerät zum Vermitteln von Medienkompetenz durch buergerservice.org und der Nutzung der SID-Box für Erleichterungen bei der Vorgangsbearbeitung in Unternehmen und Institutionen gegeben. Diese Symbiose wird durch ein leichtgängiges Mitgliedschaftsmodell von buergerservice.org e.V. unterstützt, welches kleinsten Einheiten ein Mitmachen für ca. 15 Euro pro Monat ermöglicht. Daneben sind vielfältige weitere Geschäfts-modelle möglich.

Ziel ist es, bis zum Jahr 2020 über 100.000 nPA-Terminals, hauptsächlich in Deutschland, zum Einsatz zu bringen (Vergleichszahl: ca. 56.000 Geldautomaten existieren in Deutschland). Im Fokus liegen hierbei Behörden, Gerichte, Notare, Bankfilialen, Versicherungen, Bibliotheken, Schulen, Vereine, Postfilialen, Autohäuser usw.

Für das Mitgliedschaftsmodell bedeutet dies ein jährliches Aufkommen bei den Mitgliedsbeiträgen von 12 Monate * 15 Euro * 100.000 = 18 Mio Euro.

Noch bedeutsamer ist jedoch der gesamtgesellschaftliche Nutzen. Bei einer Nutzung von fünf Vorgängen pro Werktag und nPA-Terminal bedeutet dies im Jahr 2020 ein Jahresvolumen von 260 Tage * 100.000 Terminals * 5 Vorgänge = 130 Mio Vorgänge (entspricht ca. zwei Vorgänge pro Bürger/Jahr). Bei jedem dieser Vorgänge werden Zeit und Kosten in erheblichem Umfang gespart. Ein durchschnittlicher Gang zum Amt kann mit zwei Stunden angesetzt werden. Eine durchschnittliche Fahrstrecke von 5 Kilometer scheint dabei plausibel. Alleine mit diesen beiden Werten ergibt sich bei geringsten Kostenfaktoren (8,50 Euro Mindeststundenlohn und 30 Cent Kilometerpauschale) ein gesamtgesellschaftlicher Nutzen von:

(2 * 8,50 Euro + 5 * 0,30 Euro) * 130 Mio = 2,405 Mrd. Euro pro Jahr.