



syngenio
Aktiengesellschaft

P R E S S E M I T T E I L U N G

„Plusminus“-Bericht zu Sicherheit des neuen Personalausweises – echt bedenklich oder Sturm im Wasserglas?

Elmar Borgmeier, Chief Innovation Officer der syngenio AG: „Der CCC rückt ein bekanntes Thema jetzt publikumswirksam in die Öffentlichkeit.“

„Keine Panik im Hinblick auf den nPA, sondern einfach eine gute Firewall einsetzen, die jeder Internetnutzer auch heute schon verwenden sollte.“

München, 24. August 2010 ---- Was ist passiert? Das ARD-Magazin „Plusminus“ hat zusammen mit dem Chaos Computerclub (CCC) Basis-Lesegeräte für den neuen Personalausweis geprüft und gibt vor Ausstrahlung der Sendung bekannt, dass es für Betrüger problemlos möglich sei, die sechsstellige PIN-Nummer abzufangen. Die Medien überschlagen sich, zumal der Bundesinnenminister Thomas de Maizière (CDU) keinen Handlungsbedarf sieht.

Einerseits: Sicherheitsproblematik ist bekannt

Elmar Borgmeier ist Chief Innovation Officer für die Partnerunternehmen syngenio AG und achelos GmbH, die unabhängige Beratungsleistungen zu sicheren Geschäftsprozessen anbieten und gemeinsam Lösungen im Umfeld des neuen Personalausweises entwickeln. Als Insider wundert er sich über diesen Sturm im Wasserglas:

„Es ist doch seit langem bekannt, dass der Einsatz einfacher Lesegeräte einen Kompromiss in Sachen Sicherheit darstellt. Das wird auch von den Beteiligten an der Konzeption so gesehen, weswegen es auch verständlich ist, dass die Bundesregierung nicht überrascht reagiert. Kurzum: Der CCC rückt ein bekanntes Thema jetzt publikumswirksam in die Öffentlichkeit, mehr nicht.“

Andererseits: Anwender dürfen sich nicht in Sicherheit wiegen

Richtig ist laut Einschätzung von Borgmeier allerdings, dass es problematisch wäre, wenn sich Anwender in falscher Sicherheit wiegen würden. Dazu folgende Erläuterung des Experten: „Bei Verwendung eines einfachen Lesegerätes wird die PIN auf der Tastatur eines normalen Computers eingegeben und über die Schnittstelle an das Lesegerät weitergeleitet. Hierzu werden natürlich Funktionen des Betriebssystems verwendet. Wenn sich auf dem Computer Schadprogramme wie Viren oder Trojaner befinden, die Tastatureingaben abfangen oder die Weiterleitung von Daten an das Lesegerät abhören, dann kann hier die PIN ermittelt werden. Darauf

aufbauend können dann mit den gleichen Mechanismen erweiterte Angriffe gefahren werden, bei denen die Schadprogramme Daten des Ausweises auslesen, also sogenannte Man-in-the-middle-Attacken.“

A und O für die Sicherheit: Firewall

Zwischenfazit: Um den nPA mit einem einfachen Lesegerät sicher zu verwenden ist es also weiterhin entscheidend, den Computer frei von Schadprogrammen zu halten. Hierfür sind Firewall, Virens Scanner und Sorgfalt der Nutzer entscheidend.

Alternativ kann man ein sogenanntes Class-3-Lesegerät verwenden, das über eine eigene Tastatur für die PIN und ein eigenes Display für die Anzeige der freizugebenden Daten verfügt. Der Computer, an den dieses Lesegerät angeschlossen ist, fungiert dann nur noch als Durchreiche für verlässlich verschlüsselte Daten – Viren können dort nichts mehr anrichten. Allerdings kostet ein solches Class-3-Lesegerät im Moment noch über 300 Euro, während einfache Geräte um die 10 Euro kosten.

Zur Sicherheit des nPA meint Borgmeier: „Die gleichen Angriffe, die bei einem einfachen Lesegerät möglich sind, lassen sich bei einer Identifikation mit Passwörtern oder beim Einsatz von Kreditkarten im Internet einsetzen, sogar viel einfacher. Deshalb heißt das Gebot der Stunde: Keine Panik im Hinblick auf den nPA, sondern einfach eine gute Firewall einsetzen, die jeder Internetnutzer auch heute schon verwenden sollte.“

nPA erhöht Sicherheit

Er ergänzt: „Der nPA selbst ist sicher und er erhöht verschiedene Aspekte der Sicherheit im Internet. Zum Beispiel identifiziert sich der Anbieter endlich einmal durch ein Zertifikat, das der Anwender lesen und verstehen kann. Damit werden nPA-Daten nicht mehr leichtfertig an gefälschte Server gesendet. Dies ist eines der derzeitigen Hauptprobleme in Online-Banking, weil die üblichen SSL-Zertifikate zu technisch und für den Anwender unverständlich sind, so dass er seine Bank nicht von einem Betrüger unterscheiden kann.

Auch wird eine Datenschutzrichtlinie und ein Datenschutzbeauftragter verständlich angegeben – und damit dem Nutzer ein Weg aufgezeigt, den Datenschutz auch einzufordern. Gerade Datenschutz ist in Zeiten von Web 2.0 ein immer wichtigeres Thema. Und – vielleicht weniger publikumswirksam publizierte – Stichproben der Stiftung Warentest haben gezeigt, dass es für Anwender heute oft sehr schwer ist, ihre Datenschutzansprüche tatsächlich durchzusetzen.“

ca. 4.200 Zeichen mit Leerzeichen

Diesen Text können Sie auch von <http://www.haffapartner.de> herunterladen.

Die syngenio AG ist ein unabhängiges, inhabergeführtes IT-Beratungs- und -Servicehaus für Finanzdienstleister und Telekommunikationsanbieter sowie der Methoden- und Prozessberater für IT-Organisationen. Auf die hohe IT- und Branchenkompetenz der syngenio AG mit Hauptsitz in München und Niederlassungen in Bonn, Hamburg, Stuttgart und Wiesbaden vertrauen viele namhafte Unternehmen, unter anderem Deutsche Post, EnBW, FIDUCIA IT, GAD, HypoVereinsbank, KORDOBA, Santander Consumer Bank, Swiss Post Solutions, TeamBank, T-Mobile und Yes Telecom.

Weitere Informationen:

syngenio AG
Ivonne Machnacz
Andreas-Hermes-Straße 3
53175 Bonn
Fon +49 (0)228 62095-121
Fax +49 (0)228 62095-150
ivonne.machnacz@syngenio.de
<http://www.syngenio.de>

Dr. Haffa & Partner Public Relations GmbH
Sebastian Pauls
Burgauerstraße 117
D-81929 München
Fon +49 (0)89 993191-0
Fax +49 (0)89 993191-99
syngenio@haffapartner.de
<http://www.haffapartner.de>