Netzwerk Elektronischer Geschäftsverkehr

Fachhochschule Gelsenkirchen

Gefördert durch:
Bundesministerium für Wirtschaft und Technologie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheitstipp: Neuen Personalausweis sicher verwenden

Seit dem ersten November 2010 ist der neue elektronische Personalausweis (nPA) in Umlauf. Herz der Plastikkarte ist ein kleiner Computerchip, der einige Onlinefunktionen, wie beispielsweise die Online-Ausweisfunktion, ermöglicht. Auf Wunsch können die jeweiligen Online-Funktionen vom Nutzer freigeschaltet werden. Die Bundesregierung aber auch Privatunternehmen setzen große Hoffnungen in die digitale Komponente des Ausweises: Auf lange Sicht gesehen solle die Online-Identifikation die alltägliche Geschäftswelt im Internet revolutionieren und herkömmliche Passwörter und Zugangsschlüssel ablösen. Doch mit der Einführung des neuen Ausweises geht auch eine kritische Berichterstattung einher. Datendieben sei aufgrund der zum Teil unsicheren Kartenlesegeräte Tür und Tor geöffnet, so die Gegner des nPA. Nachfolgend erfahren Sie, wie Sie die Online-Funktionen des neuen Ausweises nutzen können und dabei Sicherheitsrisiken vermeiden.

Neue Online-Funktionen: Sie haben die Wahl

Zunächst sollten Sie überlegen, ob Sie die neuen Online-Funktionen des Personalausweises überhaupt freischalten lassen möchten. Denn: Sie haben die Wahl. Bei der Beantragung Ihres neuen Ausweises werden Sie gefragt, ob Sie eine Aktivierung der Online-Authentisierung wünschen. Entscheiden Sie sich dagegen, wird die elektronische Datenübertragung Ihres Ausweises deaktiviert. In diesem Fall sind zwar alle Ihre personenbezogenen Daten (außer Unterschrift, Augenfarbe und Körpergröße) elektronisch auf dem Computerchip gespeichert, können aber nicht durch herkömmliche Kartenlesegeräte ausgelesen werden. Lediglich bei einer hoheitlichen Identitätskontrolle, beispielsweise bei der Überschreitung von Landesgrenzen, können dann noch elektronisch Daten durch befugte (Grenz-)Beamte ausgelesen werden. Mit Ausnahme Ihres Fingerabdrucks stehen alle Daten, die für die digitale Datenübertragung infrage kommen, sichtbar auf Ihrem Personalausweis. Es ist nicht möglich, weitere Daten oder Vermerke elektronisch hinzuzufügen.

Aktuell ist das baldige Ende herkömmlicher Passwörter und Zugangsschlüssel noch nicht in Sicht. Sie können die Online-Funktionen des Ausweises auch jederzeit im Nachhinein für eine Bearbeitungsgebühr von derzeit sechs Euro (Stand: Mai 2011) in Ihrem Bürgeramt freischal-

ten lassen. Sofern Sie sich für die Nutzung der Online-Funktionen entscheiden, können Sie bei jedem Vorgang stets selbst bestimmen, ob und welche personenbezogenen Daten Sie elektronisch übermitteln wollen.

Sichern Sie Ihre IT-Umgebung

Neben den integrierten Sicherheitsvorkehrungen auf dem Computerchip des Personalausweises und in der elektronischen Übertragung Ihrer Daten hängt ein sicherer Einsatz der Online-Funktionen ganz entscheidend von Ihrer konkreten Computerumgebung ab (siehe: IT-Sicherheitstipp und Hintergrundinfos *Basisschutz für Ihren PC* [1]).

Ist Ihr System nur gering geschützt, erhöht sich die Gefahr deutlich, Opfer eines Datendiebstahls zu werden. **Verwenden Sie deshalb neben einem aktuellen Virenschutzprogramm eine Personal-Firewall, die ungewollte Verbindungen nicht zulässt. Aktualisieren Sie regelmäßig Ihre Schutzprogramme und Anwendungen (wie *Mozilla Firefox* oder *Internet Explorer*) sowie PlugIns (wie *Java*, *Adobe Flash Player*) Ihrer IT-Umgebung, die mit dem Internet kommunizieren. Achten Sie auch regelmäßig auf Updates Ihres Betriebssystems sowie für die so genannte *AusweisApp* [2], die Sie als Treibersoftware für die Nutzung der Online-Funktionen benötigen. Hinweise auf aktuelle Sicherheitsupdates erfahren Sie über den kostenfreien Service „securityNews“ [3].**

Der Bund eröffnet Interessierten die Option, ein so genanntes *Sicherheitskit* zu erwerben. In einem solchen Kit sind enthalten: Ein Basiskartenleser für die elektronische Datenübertragung, Informationen zur Nutzung von Chipkarten und zusätzliche individuell zusammengestellte Bestandteile wie zum Beispiel Antivirensoftware.

Schützen Sie PIN, PUK und Sperrkennwort

Mit dem Erhalt des neuen Ausweises im Scheckkartenformat wird Ihnen eine sechsstellige PIN, ein PUK (Entsperrschlüssel) und ein so genanntes *Sperrkennwort* mitgeteilt. Die PIN wird bei jeder elektronischen Datenübertragung abgefragt. **Geben Sie diese auf keinen Fall an Dritte weiter und bewahren Sie sie an einem anderen Ort als Ihren Ausweis auf. Sie haben die Möglichkeit, Ihre PIN jederzeit nach Ihren Wünschen zu ändern. Diese sollten sie auch regelmäßig nutzen. Vermeiden Sie leicht zu erratende Zahlenkombination wie etwa „123456“ oder Geburtsdaten bei der Vergabe der neuen PIN.** Besser ist es, eine Zahlenkombination zu wählen, die mit Ihnen und Ihrem gesamten Umfeld nicht in Zusammenhang gebracht werden kann (siehe: IT-Sicherheitstipp und Hintergrundinfos *Passwort sicher erstellen* [1]). Die PUK wird als Entsperrschlüssel erforderlich, sofern Sie Ihre PIN bei einer Abfrage drei Mal in Folge falsch eingegeben haben.

Falls Sie Ihren Ausweis verlieren sollten, lassen Sie die Online-Funktionen so schnell wie

möglich mithilfe des Sperrkennwortes über folgende telefonische Sperr-Hotline sperren: 0180-1-333 333 (3,9 ct/Minute aus dem deutschen Festnetz, maximal 42 ct/Minute aus dem deutschen Mobilfunknetz, Nummer auch aus dem Ausland erreichbar). Eine Sperrung ist auch in Ihrem Bürgeramt möglich.

Schützen Sie alle geheimen Passwörter (PIN, PUK, Sperrkennwort) und Ihre Zugangsdaten vor der Einsicht durch unbefugte Personen.

Wählen Sie einen sicheren Kartenleser aus

Das Kartenlesegerät stellt das Verbindungsglied zwischen Ihrem Ausweis und Ihrem Computer dar. Zur Auswahl stehen drei verschiedene Typen von Kartenlesegeräten: *Basis-*, *Standard-* und *Komfortlesegeräte*.

Der Basiskartenleser beinhaltet keine eigene Bedientastatur und ist somit der unsicherste Typ. **Nutzer dieses Gerätes sollten darauf achten, Ihre PIN stets per Maus auf der Bildschirmtastatur der AusweisApp einzugeben und nicht auf der vorliegenden physischen Tastatur.**

Experten empfehlen jedoch die Nutzung des Standard- oder Komfortgerätes mit separater Tastatur. Christian J. Dietrich, Sicherheitsexperte vom *Institut für Internet-Sicherheit - if(is)*, rät: **„Die PIN-Eingabe sollte stets über das Pinpad des Gerätes erfolgen.** Denn ein solches Verfahren erhöht erheblich den Schutz des Nutzers vor Schadprogrammen wie Keyloggern, die versuchen die PIN des Eingebenden mitzulesen.“

Achten Sie beim Kauf eines Kartenlesegerätes unbedingt auf ein BSI-Zertifikat (rundes Logo; siehe Rückseite des neuen Personalausweises), das die Sicherheit des Gerätes garantiert. Ganz wichtig: Lassen Sie Ihren Ausweis nur genauso lange auf dem Lesegerät, wie für den Datentransfer erforderlich. Andernfalls könnten Sie Opfer eines Phishing-Angriffes (Datenklau) werden (siehe: IT-Sicherheitstipp und Hintergrundinfos *Sicherer Umgang mit dem Internet* [1]).

Etwa fünf Zentimeter beträgt die maximale Distanz, in der der Chip des Ausweises von einem Lesegerät erfasst werden kann.

Übermitteln Sie Ihre Daten nur an berechtigte Anbieter

Jeder Dienstleister, der eine *eID-Funktion* (eID = electronic Identity) bereitstellt, muss sich mithilfe eines staatlichen Berechtigungszertifikat ausweisen. Dieses Zertifikat zeigt an, dass es sich um einen seriösen Anbieter handelt und welche personenspezifischen Daten (Name, Anschrift, Geburtsdatum, et cetera) für den jeweiligen Geschäftszweck übermittelt werden sollen. Mögliche Anbieter sind beispielsweise privatwirtschaftliche Unternehmen mit Online-Services, Online-Shops, Banken, E-Mail-Anbieter, Soziale Netzwerke, Verkaufsautomaten für Fahrkarten et cetera, aber auch einige staatliche Einrichtungen wie Behörden.

Bevor es überhaupt zu einer Datenübertragung kommt, wählen Sie stets eigenhändig aus, welche Datenfelder (wie Vorname, Nachname) an den Anbieter übertragen werden. Im Anschluss bestätigen Sie Ihre Auswahl mit der Eingabe Ihrer PIN.

Haben Sie bei der Beantragung Ihres nPA freiwillig Ihren Fingerabdruck zur Verfügung gestellt, so wird dieser neben Ihrem digitalen Foto ebenfalls elektronisch abgespeichert. Bisher gibt es jedoch keine gesetzliche Verpflichtung, seinen Fingerabdruck abspeichern zu müssen.

Gegebenenfalls wird neben Ihrem biometrischen Foto also auch Ihr Fingerabdruck digital übermittelt – und zwar ausschließlich bei Gebrauch der hoheitlichen Ausweisfunktion (beispielsweise gegenüber Polizeibeamten).

Die Funktion der Online-Authentifizierung wird in absehbarer Zeit eine eher untergeordnete Rolle spielen. Bisher hat die *Vergabestelle für Berechtigungszertifikate* (VfB) lediglich 74 staatliche Berechtigungszertifikate ausgestellt (Stand: Mai 2011) [4]. Die neue Online-Ausweisfunktion stellt neben den herkömmlichen Authentifizierungs-Verfahren also nur eine zusätzliche Möglichkeit der Identifikation dar, die bisher nur von sehr wenigen Dienstleistern angeboten wird.

Zusätzlich zur Online-Ausweisfunktion, gibt es eine weitere Funktion, nämlich die der digitalen Unterschrift. Nach dem Signaturgesetz (SigG), ist die so genannte *qualifizierte elektronische Signatur* (QES) rechtlich der eigenhändigen persönlichen Unterschrift gleichgestellt, um beispielsweise Dokumente oder Verträge rechtsgültig zu unterzeichnen. Zur Nutzung der QES benötigen Sie neben einem Komfortlesegerät und einer *Signatur-PIN*, auch ein *Signaturzertifikat*, das Sie mithilfe staatlich zugelassener Dienstleister [5] auf Ihren Personalausweis nachladen können. Im Moment bietet jedoch keiner der zugelassenen Dienstleister auch tatsächlich das Nachladen des Signaturzertifikats an, sodass Sie also bislang noch keinen Gebrauch von der QES machen können (Stand Mai 2011) [6].

Autoren:

Malte G. Schmidt, FH Gelsenkirchen, Institut für Internet-Sicherheit

B.Sc. Deborah Busch, FH Gelsenkirchen, Institut für Internet-Sicherheit

Dipl.-Inform.(FH) Sebastian Spooren, FH Gelsenkirchen, Institut für Internet-Sicherheit

Prof. Dr. (TU NN) Norbert Pohlmann, FH Gelsenkirchen, Institut für Internet-Sicherheit

Weiterführende Informationen:

[1] http://ratgeber.it-sicherheit.de

[2] https://www.ausweisapp.bund.de

[3] https://www.it-sicherheit.de/sn/

[4] http://www.bundesverwaltungsamt.de

[5] http://www.bundesnetzagentur.de

[6] http://www.personalausweisportal.de

http://www.ec-net.de

http://www.kmu-sicherheit.de

http://www.bsi.bund.de

Bildquelle: © Institut für Internet-Sicherheit - if(is) – www.internet-sicherheit.de

Das Netzwerk Elektronischer Geschäftsverkehr

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr, in 28 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business Lösungen. In dieser Zeit hat sich das Netzwerk mit über 30.000 Veranstaltungen und Einzelberatungen mit über 300.000 Teilnehmern als unabhängiger und unparteilicher Lotse für das Themengebiet „E-Business in Mittelstand und Handwerk“ etabliert. Das Netzwerk stellt auch Informationen in Form von Handlungsanleitungen, Studien und Leitfäden zur Verfügung, die auf dem zentralen Auftritt www.ec-net.de heruntergeladen werden können. Die Arbeit des Netzwerks wird durch das Bundesministerium für Wirtschaft und Technologie gefördert.

Fachhochschule Gelsenkirchen, Institut für Internet-Sicherheit - if(is)

Das Institut für Internet-Sicherheit ist eine fachbereichsübergreifende wissenschaftliche Einrichtung der Fachhochschule Gelsenkirchen. Es forscht und entwickelt auf Basis innovativer Konzepte im Bereich der Internet-Sicherheit. 2005 gegründet, hat es sich unter der Leitung von Prof. Dr. (TU NN) Norbert Pohlmann und in enger Zusammenarbeit mit der Wirtschaft innerhalb kurzer Zeit einen Ruf als eine der führenden deutschen Forschungsinstitutionen der IT-Sicherheit gemacht. Weitere Informationen finden Sie unter: http://www.internet-sicherheit.de

Sichere E-Geschäftsprozesse in KMU und Handwerk

Die Checkliste IT-Sicherheit wurde im Rahmen des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerks Elektronischer Geschäftsverkehr (NEG) erstellt. Das Verbundprojekt wird vom Bundesministerium für Wirtschaft und Technologie (BMWi) unterstützt und soll helfen, in kleinen und mittleren Unternehmen mit verträglichem Aufwand die Sicherheitskultur zu verbessern. Hier werden insbesondere kleine und mittelständische Unternehmen sowie das Handwerk zu wichtigen Aspekten der Informationssicherheit sensibilisiert und praxisnah informiert. Alle Details finden Sie unter: http://www.kmu-sicherheit.de