Bürgerkarte gegen Phishing

Die Funktion Bürgerkarte dient nicht nur zur rechtsverbindlichen Unterfertigung von Schriftstücken, sondern hilft auch gegen Phishing-Attacken.

Organisiert von Univ.-Prof. Dr. Patrick Horster der Universität Klagenfurt, veranstaltete die Forschungsgruppe Systemsicherheit der Universität am 8. November 2006 den 3. Österreichischen IT-Sicherheitstag – nach Klagenfurt und Graz diesmal in Wien.

Kommerzialrat Hans-Jürgen Pollirer von der Bundessparte Information und Consulting der Wirtschaftskammer Österreich berichtete über den Fortgang der im Oktober 2005 gestarteten Aktion „it-safe.at" der Wirtschaftskammer, in deren Rahmen Berater in Unternehmen kommen und Sicherheits-Checks durchführen. Bis zur Tagung wurden etwa 300 solcher Checks durchgeführt, sie werden vom BMWA zu 75 Prozent gefördert. Bei diesen Checks hat sich etwa ergeben, dass in 83 Prozent der Fälle die Sicherung der Daten im Büro selbst durchgeführt worden ist, also ohne räumliche Trennung, wodurch etwa bei einem Brand im Büro auch die gesicherten Daten vernichtet worden wären.

Ob die Datensicherung erfolgreich war, wurde in 34 Prozent der Fälle nicht überprüft, in 20 Prozent wurde die Datensicherung seltener als einmal pro Monat durchgeführt. Das gibt zu denken, da bei einer 2006 durchgeführten Studie der FHS für Informationsberufe 75 Prozent der befragten österreichischen kleinen und mittleren Unternehmen (KMU) die Abhängigkeit der täglichen Abläufe von einer funktionierenden Informationstechnologie als

Mit der Bürgerkarte sollen Phishing-Angriffe vermieden werden.

FOTO: SYMANTEC

hoch oder sehr hoch bezeichnet haben. „Es fehlt das Bewusstsein für Sicherheitsmaßnahmen" stellte Pollirer fest, wobei in dieses Bild passt, dass in 66 Prozent der besuchten Unternehmen keine schriftlichen Anweisungen zum Umgang mit Computern bestanden haben, bei 49 Prozent keine Verhaltensregeln bei Auftreten eines Virus und in etwas mehr als der Hälfte keine Dokumentation der Konfiguration der Computer-Systeme vorhanden war. 64 Prozent hatten keine Vorkehrungen für den Fall des Austritts von Mitarbeitern getroffen, wie etwa automatisches Löschen des Passwortes oder Rückgabe von Firmendokumenten. Laptops waren nur zu 30 Prozent durch Verschlüsselung geschützt, mehr als die Hälfte (55 %) der WLANs wurde unverschlüsselt und ohne Zugriffsschutz betrieben.

„Ein Mindestmaß an Sicherheitsrichtlinien muss auch im Kleinbetrieb vorhanden sein", betonte Pollirer. Das IT-Sicherheitshandbuch wird im Frühjahr 2007 in der dritten Auflage erscheinen. Es ist an eine Kooperation mit dem Wissenschaftsministerium gedacht, um Lehrern und Administratoren Inhalte der Aktion nahe zu bringen und um IT-Sicherheit zu einem Bestandteil der Ausbildung zu machen. Der Schulung kommt besondere Bedeutung zu – 32 Prozent der Ursachen für Ausfallzeiten und Datenverluste sind auf menschliche Fehler zurückzuführen. Ferner soll ein Modul zur Erstellung von Betriebsvereinbarungen geschaffen werden, das rechtliche und organisatorische Aspekte der Nutzung der Informationstechnologie im Betrieb erfassen und regeln soll.

Durch Betriebsvereinbarungen soll geregelt werden, in welchem Umfang in einem Betrieb die private Nutzung der Informationstechnologie gestattet ist, insbesondere des Internets und das E-Mailing. Laut Dr. Barbara Oberhofer (Wirtschaftskammer Österreich) muss ein Arbeitgeber seinen Mitarbeitern keine Informationstechnologien zur Verfügung stellen, und er kann deren private Nutzung verbieten.

In der Praxis hat sich allerdings herausgebildet, dass es Arbeitnehmern erlaubt wird, das Internet insoweit als Informationsmedium zu nutzen, als dies zumindest entfernt mit der beruflichen Tätigkeit zu tun hat.

Um Schwierigkeiten zu vermeiden, sollten Regeln aufgestellt werden über Ausmaß und Umfang einer privaten Nutzung und darüber, was jedenfalls verboten ist, wie etwa das Downloaden urheberrechtlich geschützter Werke (Bilder, Filme, Musikstücke, Programme), strafgesetzwidriger oder anstößiger Inhalte, das Aufsuchen kostenpflichtiger Sites, das Mitbieten bei

Heikle Firmendaten sollten räumlich getrennt gesichert werden.

Versteigerungen von Firmencomputern aus oder das Versenden von Massen-Mails. Wird derartigen Verboten zuwider gehandelt, kann dies zur Kündigung führen und zur Entlassung, wenn ein weiteres Zusammenarbeiten bis zum Ablauf der Kündigungsfrist nicht mehr zumutbar ist.

Die Einführung von Kontrollen und technischen Systemen zur Kontrolle der Arbeitnehmer bedarf, sofern diese Maßnahmen (Systeme) die Menschenwürde berühren, nach § 96 Abs 1 Z 3 Arbeitsverfassungsgesetz (ArbVG, BGBl 1974/22, zuletzt BGBl I 2006/147) einer Betriebsvereinbarung, für die die Zustimmung des Betriebsrats zwingend notwendig ist und nicht durch die Entscheidung einer Schlichtungsstelle ersetzt werden kann. Ist kein Betriebsrat errichtet, muss jeder einzelne Arbeitnehmer der Maßnahme zustimmen (§ 10 Arbeitsvertragsrechts-Anpassungsgesetz – AVRAG, BGBl 1993/459).

Kontrollmaßnahmen werfen auch datenschutzrechtliche Probleme auf, da beispielsweise Log-Files personenbezogene Daten sind, auf deren Geheimhaltung jedermann ein verfassungsgesetzlich gewährleistetes Recht hat (§ 1 Abs 1 DSG 2000).

Eingriffe sind, wenn der Betroffene nicht zustimmt, nur im Rahmen einer Interessenabwägung zulässig (§ 8 Abs 1 Z 4 DSG) oder, bei sensiblen Daten, wenn die Verwendung erforderlich ist, um den Rechten und Pflichten des Auftraggebers auf dem Gebiet des Arbeits- oder Dienstrechts Rechnung zu tragen, und sie nach besonderen Rechtsvorschriften zulässig ist (§ 9 Z 11 DSG).

In der Praxis wird laut Oberhofer nach dem Modell einer „stufenweisen Kontrollverdichtung“ vorgegangen: Wenn bei überblicksweisen Kontrollen in einzelnen Bereichen eine zu hohe Nutzung festgestellt wird, erfolgt eine Abmahnung, verbunden mit nachfolgender genauerer Kontrolle dieses Bereichs. Wird weiteres Zuwiderhandeln festgestellt, drohen Sanktionen.

Phishing-Attacken. Diplom-Ingenieur Thomas Rössler vom E-Government Innovationszentrum (EGIZ; www.egiz.gv.at) wies darauf hin, dass Phishing-Angriffe misslingen, wenn das potenzielle Opfer die „Bürgerkarte“ für Transaktionen verwendet. Das EGIZ untersteht direkt dem Chief Information Officer (CIO) des Bundes, Prof. Reinhard Posch. Die Bürgerkarte ist keine Karte an sich, sondern eine Funktionalität, die auf verschiedenen Medien und durch verschiedene Technologien realisiert werden kann, etwa durch Aktivierung auf der Bankomat- oder Kreditkarte, der E-Card, einem Studentenausweis, oder durch das Handy.

Wird beispielsweise beim Online-Banking die Funktion „Bürgerkarte“ verwendet, sind der Besitz des diese Funktionalität beinhaltenden Mediums erforderlich sowie die PIN als Zugangscode zu diesem Medium – also Besitz und Wissen. Wenn sich schon jemand dazu verleiten lassen sollte, auf angebliche Anfrage seines Bankinstituts, seine PIN bekannt zu geben (Phishing = Password Fishing), nützt das dem Angreifer nichts. Er ist nicht im Besitz des für die Transaktion erforderlichen Mediums. Dazu kommt, dass die Geschäftsvorgänge mit der Funktion „Bürgerkarte“ elektronisch unterschrieben werden, wobei das sich spezifisch ergebende Signaturergebnis nicht wiederverwendbar und auch nicht reproduzierbar ist und somit von Angreifern nicht missbraucht werden kann. Letztlich wird durch die mit der Bürgerkarte verbundene Software die zu signierende Transaktion dem Anwender angezeigt, sodass spätestens hier ein Missbrauch erkennbar werden sollte.

Die Signaturfunktion der Bürgerkarte wurde mittlerweile auf PDF-Dokumente ausgedehnt. Bei reinen Textdokumenten kann die Signatur sogar vom Papierausdruck rekonstruiert und geprüft werden. Damit ist das Erfordernis einer sicheren Signatur nach dem Signaturgesetz bzw. der Amtssignatur bei amtlichen Schriftstücken nach dem E-GovG erfüllt. Für Dokumente, die nicht nur Text enthalten, wurde eine binäre Signatur entwickelt, bei der keine Rekonstruktion über den Ausdruck möglich ist.

„Im Hinblick darauf, dass es nicht einmal etwas kostet, auf die E-Card, die fast jeder hat, die Funktion Bürgerkarte zu übertragen, fragt man sich, warum die Bürgerkarte auf diesem Medium und auch insgesamt noch keine weitere Verbreitung gefunden hat“, erläuterte Rössler. „Auch abseits vom E-Government ist die Bürgerkarte auf vielfältigste Weise einsetzbar.“

Zahlungen im Internet. Aus Sicht des Unternehmers referierte Univ.-Prof. Dr.

FOTO: CHRISTIAN SONNENSCHEIN

Sonja Janisch: „Streitwerte bei Konflikten um Domainnamen liegen bei 50.000 Euro.“

Hans-Jürgen Pollirer: „Bewusstsein für Sicherheitsmaßnahmen fehlt.“

Peter Mader von der Universität Salzburg über Zahlungssysteme im Internet: Wie sicher kann ein Unternehmer sein, sein Geld tatsächlich zu bekommen, welche Missbrauchsmöglichkeiten bestehen durch Dritte, wie kundenfreundlich sind die einzelnen Systeme und inwieweit eignen sie sich für die Zahlung kleiner Geldbeträge (Micropayments). Wenn eine Zahlung bloß über die Angabe der Kreditkartennummer (und des Ablaufdatums der Karte) erfolgen soll, ist die Gefahr des Missbrauchs groß.

Der Karteninhaber gibt dem Kartenaussteller eine Anweisung, an den Vertragshändler zu bezahlen. Diese wird über den Vertragshändler dem Kartenaussteller weitergeleitet, der mit dem Kaufbetrag wieder den Karteninhaber belastet.

Die Schwierigkeit liegt in der Nachweisbarkeit, dass die Zahlungsanweisung tatsächlich vom (rechtmäßigen) Karteninhaber gekommen ist, wobei die Beweislast den Kartenaussteller trifft. Daher ist Vorauszahlung weitgehend üblich, aber auch Nachnahme oder Lieferung auf Rechnung.

Die Situation für den Verkäufer bessert sich, wenn zusätzlich zur Angabe der Kreditkartennummer die Eingabe eines Passworts („Secure Code“) verlangt wird. Es kann davon ausgegangen werden, dass nur der rechtmäßige Karteninhaber das Passwort kennt. Würde behauptet, dass es von einem anderen verwendet wurde, besteht der Verdacht, dass das Passwort dem anderen durch eine Obliegenheitsverletzung bekannt wurde, was eine Haftung des Karteninhabers bewirkt. Beide Systeme sind bedienungsfreundlich; für Micropayments eignen sie sich nur bedingt.

Hohe Zahlungs- und Missbrauchssicherheit wird mit Prepaid-Karten ähnlich den Telefon-Wertkarten erreicht. Die Karte wird gekauft und der 16-stellige Code aufgerubbelt. Über dessen Eingabe wird vom Bankinstitut, von dem die Karte stammt, der jeweilige Betrag dem Händler überwiesen. Der Kunde hat die Möglichkeit, die Karte zu sperren. Das System eignet sich auch für Micropayments. Bei einem Kaufvorgang können auch mehrere Karten verwendet werden, deren höchster Nennwert 100 Euro beträgt.

Ähnlich funktioniert die mit limitierten Geldbeträgen „aufgeladene“ Smartcard. Sie kann über einen Chipkartenleser wie Bargeld verwendet werden und bietet hohe Zahlungssicherheit für den Verkäufer, ist einfach

Fotos: Kurt Hickisch

zu bedienen und eignet sich für Micropayments. Wie Bargeld, das gestohlen werden kann, bietet sie allerdings keine Sicherheit vor Missbrauch durch Dritte.

Bei Zahlungssystemen über Handy wird die Handy-Nummer eingegeben; es erfolgt vom Systembetreiber ein automatisierter Rückruf mit Zahlungsempfänger und Zahlungsbetrag. Die Bestätigung erfolgt durch Eingabe der PIN oder über SMS. Die Abrechnung erfolgt über das Bankkonto oder die Mobilfunkrechnung. Sollte das Konto nicht gedeckt sein, erhält der Verkäufer die Kundendaten. Zahlungssicherheit sowie Sicherheit vor Missbrauch durch Dritte sind hoch; für Micropayments eignet sich das System nicht. Über das jeweilige Geldinstitut des Kunden laufen die verschiedenen Netbanking-Systeme, die die Eingabe von PIN und TAN erfordern.

„Bei überschaubarem Käuferrisiko ist das Risiko des Verkäufers meist ungleich höher", zieht Prof. Mader Bilanz. „Bei Bezahlvorgängen im Internet besteht das Problem der Identifizierung des Schuldners; über die elektronische Signatur ließe sich ein höherer Standard erreichen." Dazu komme das Problem der vielen PINs; jede Sorgfaltsverletzung führe zu einer Haftung des Kunden.

Über weitverbreitete Irrtümer im E-Business-Recht referierte Univ.-Ass. Dr. Sonja Janisch (Universität Salzburg). So etwa erwirbt man durch die Registrierung eines Domainnamens kein geschütztes Recht, das jenes übersteigt, das, etwa als Namensrecht (§ 43 ABGB), als Unternehmenskennzeichen (§ 9 UWG) oder als geschützte Marke (§ 10 MSchG) vorher schon bestanden hat. Viel eher wird

Peter Mader: „Zusätzlich zur Kreditkartennummer ein Passwort eingeben."

durch die Registrierung eines Domainnamens in Rechte Dritter eingegriffen, nämlich in Namens-, Kennzeichen- oder Markenrechte, in den Firmenschutz nach § 37 Unternehmensgesetzbuch (UGB, bis 31. Dezember 2006 Handelsgesetzbuch – HGB) oder in den Titelschutz nach § 80 UrhG. In der Form des „Domain-Grabbings" liegt eine sittenwidrige Behinderung nach § 1 UWG vor.

„Streitwerte bei juristischen Konflikten im Zusammenhang mit Domainnamen liegen um 50.000 Euro und die Verfahren sind dementsprechend teuer", erläuterte Janisch. „Eine Abmahnung kostet einige hundert Euro."

Haftungsausschlussklauseln (Disclaimer) befreien den Betreiber einer Website nicht von der Haftung, somit auch nicht von der Haftung für den Inhalt der Seiten, zu denen er Links setzt. Eine gesetzliche Haftung kann nicht durch Willen der Parteien ausgeschlossen werden. Allerdings kommt das Gesetz (§ 17 Abs 1 Z 1 und 2 E-Commerce-Gesetz – ECG, BGBl I 2001/152) dem Linksetzer entgegen: Er haftet grundsätzlich dann nicht, wenn er von einer rechtswidrigen Tätigkeit oder Information tatsächlich keine Kenntnis hat oder nach Erlangen dieser Kenntnis unverzüglich tätig wird, um den Link zu entfernen.

Thomas Rössler: „Bürgerkarte macht Online-Banking sicherer."

Er haftet aber, wenn er die fremden Informationen als eigene darstellt (§ 17 Abs 2 ECG). Auch wenn man über eine Website nichts bestellen kann, müssen Informationspflichten beachtet werden. Zumindest ist das Impressum nach § 25 MedienG erforderlich. Wird ein Dienst der Informationsgesellschaft angeboten (das ist so gut wie jeder kommerzielle Auftritt im Internet), sind die Informationspflichten nach § 5 Abs 1 ECG zu beachten. Werden Preise angeführt, sind diese so auszuzeichnen, dass sie ein durchschnittlich aufmerksamer Betrachter leicht lesen und zuordnen kann. Es muss eindeutig erkennbar sein, ob es sich um Bruttopreise handelt oder nicht, und ob Versandkosten enthalten sind. Wird eine Bestellmöglichkeit angeboten, sind die weiteren Informationspflichten nach § 9 ECG, § 5c Konsumentenschutzgesetz und § 2 Preisauszeichnungsgesetz zu beachten.

Dass dann, wenn ein Österreicher im Internet Verträge abschließt, immer österreichisches Recht anzuwenden ist, kann in dieser Allgemeinheit nicht gesagt werden. Im Bereich der EU gilt nach dem Europäischen Vertragsstatutübereinkommen (EVÜ, BGBl III 1998/208) bei Verbraucherverträgen in der Regel das Recht des Staates, in dem der Verbraucher seinen gewöhnlichen Aufenthalt hat (Art 5 Abs 3 EVÜ). Bei Unternehmerverträgen gilt freie Rechtswahl (Art 3). Ist eine solche nicht erfolgt, unterliegt der Vertrag dem Recht des Staates, mit dem er die engsten Verbindungen aufweist; das ist dort, wo die charakteristische Leistung zu erbringen ist (Art 4). Für Vertragsverhältnisse außerhalb der EU knüpft das Gesetz über das internationale Privatrecht (IPR-Gesetz, BGBl I 1998/119, zuletzt idF BGBl I 2004/58) an die Rechtsordnung an, zu der die stärkste Beziehung besteht (§ 1 IPRG).

Ob Texten oder Bildern der Copyright-Vermerk angefügt ist, ist für das Urheberrecht nicht von Bedeutung. Entscheidend ist das Vorliegen eines „Werkes" als eigentümliche geistige Schöpfung auf den Gebieten der Literatur, der Tonkunst, der bildenden Künste oder der Filmkunst (§ 1 UrhG). Ob wirklich eine geistige Schöpfung vorliegt, kann mitunter zweifelhaft sein; im Zweifel sollte eine Übernahme von Werken aus dem Internet unterlassen werden. Fotos sind sogar dann, wenn sie nicht die Qualität eines Werkes erreichen, als einfache Lichtbilder nach § 73 UrhG geschützt.

Bildnisse von Personen unterliegen dem Schutz vor Veröffentlichung nach § 78 UrhG. „Bei einem Streitwert von üblicherweise cirka 30.000 Euro sind auch Anwalts- und Gerichtskosten entsprechend hoch", warnt Janisch. „Ein Prozess wegen eines einzigen entgegen dem Urheberrecht verwendeten Fotos kann 10.000 Euro kosten."

Der nächste IT-Sicherheitstag wird Ende Oktober/Anfang November, 2007 in Salzburg stattfinden. *Kurt Hickisch*

FOTOS: KURT HICKISCH