Vernetzte Welt

„Sichere Wege in der vernetzten Welt“ war das Motto des 11. Deutschen IT-Sicherheitskongresses, der in Bonn/Bad Godesberg stattfand.

Vor einem Jahrhundert haben die Menschen im Auto vor allem ein schnelleres Pferd gesehen“, sagte Innenminister Dr. Wolfgang Schäuble, am 12. Mai 2009 bei der Eröffnung des vom *Bundesamt für Sicherheit in der Informationstechnik (BSI)* veranstalteten Kongresses. „Aber heute wissen wir, wie sehr das Auto die Welt verändert hat. Auch die modernen Informations- und Kommunikationstechnologien verändern unser Leben und die Gesellschaft“.

Neue Freiheiten, aber auch neue Abhängigkeiten und Bedrohungen seien entstanden. „Mit der IT-Sicherheit steht und fällt die Funktionsfähigkeit unserer Gesellschaft“, betonte Schäuble und verwies auf die besonders gefährdeten Infrastrukturen von Telekommunikation, Finanzen, Energie, Gesundheit und Verkehr, die zu vier Fünftel privatwirtschaftlich geführt werden. In den USA denke man bereits daran, eine Art „Internet-Notstand“ auszurufen.

Deutschland werde die Ausgaben für die IT-Sicherheit um 175 Millionen Euro aufstocken, kündigte Schäuble an. In Vorbereitung seien eine durch Datenskandale in der jüngsten Zeit ausgelöste Novellierung des Bundesdatenschutzgesetzes sowie die Anpassung des aus dem Jahr 1990 stammenden BSI-Gesetzes an die heutige Gefahrenlage. Das BSI soll künftig verbindliche Richtlinien für die Datensicherheit bei Bundesbehörden erlassen können.

Die virtuelle Welt werde zum Tatort; die Cyberkriminalität habe sich professionalisiert. Es gebe einen blühenden Markt der Botnetz-Vermietung. Deutschland liege, bezogen auf die Anzahl der mit „Bots“ infizierten Computer, im Ländervergleich nach China und den USA auf Platz 3. Es müsse die Möglichkeit geschaffen werden, dass Internet-Provider infizierte PCs zur Not auch vom Netz nehmen könnten, wenn von ihnen Gefahr ausgehe.

Die für Phishing ausgebrachte Malware löst nicht nur Finanz-Transaktionen aus, sie kann auch Menschen ihre digitale Identität stehlen.

Foto: Symantec

Zumindest in der Europäischen Union müsse ein einheitliches IT-Sicherheitsniveau geschaffen werden. Einen wichtigen Beitrag hiefür könne die 2004 gegründete *Europäische Agentur für Netz- und Informationssicherheit ENISA* leisten. Direktor dieser Agentur wird ab 16. Oktober 2009 der derzeitige Präsident des BSI, Dr. Udo Helmbrecht.

Der Schutz kritischer Informations-Infrastrukturen (KII) stellt auch einen Schwerpunkt der Politik der Europäischen Kommission dar, berichtete Dr. Rudolf W. Strohmeier, der Kabinettchef der zuständigen Kommissarin Dr. Viviane Reding. Es handle sich um jene Netze, IKT-Systeme und Dienste, die die Erfüllung essenzieller gesellschaftlicher Funktionen ermöglichen, wozu das Internet zähle. Kernelement des Europäischen Programms für den Schutz kritischer Infrastrukturen (EPSKI) sei die Richtlinie 2008/114/EG über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen. Zudem habe die Kommission die Mitgliedstaaten aufgefordert, nationale Notfallpläne aufzustellen und regelmäßige Übungen durchzuführen.

„Sicherheit darf keinen Ärger machen“, forderte Prof. Dr. Gunter Dueck, Cheftechnologe von IBM Deutschland, und verwies auf den „Schilderwald“ im Straßenverkehr. Wenn es zu viele Verbote gebe, würden diese übertreten. Der Bürger erwarte sich einfach, dass der Internet-Verkehr sicher gestaltet werde. „Warum wird der elektronische Ausweis nicht gleich auch mit der Kreditkarte verbunden, zusammen mit einer abgestuften Abrufbarkeit der gespeicherten Daten, um Bestellungen über das Internet einfacher durchführen zu können?“, fragte er. Rechnungen könnten in einem einheitlichen, elektronisch verarbeitbaren Format ausgestellt und in dieser Form gleich an die Bank weitergeleitet werden. Müsse es sein, dass die elektronische Steuererklärung genau derjenigen in Papierform entspricht; könnte sie nicht individuell auf die bisherigen aktenkundigen Einkunftsarten des Steuerpflichtigen zugeschnitten werden? Die E-Mail-Adresse eines Menschen ist weltweit einzigartig – könnte sie nicht als Konto-Nummer herangezogen werden? Warum könne man bei einem Wechsel des Kreditinstituts nicht auch, wie bei einer Handy-Nummer, die Konto-Nummer mitnehmen?

E-Personalausweis. Eine Vortragsreihe war der zum 1. November 2010 geplanten Einführung des elektro-

nischen Personalausweises *(ePA)* in Deutschland gewidmet. In das Projekt sind 5.700 Personalausweisbehörden eingebunden; pro Jahr werden etwa acht Millionen Personalausweise ausgegeben und es wird eine eigene Infrastruktur (PKI) aufgebaut.

Der *ePA* ist ein Reise- und Ausweisdokument und enthält einen berührungslos auslesbaren Chip, in dem die persönlichen Daten sowie das Lichtbild gespeichert sind. In diesen Chip können auf Wunsch – dies ist dem Bürger freigestellt – auch die Abdrücke der beiden Zeigefinger aufgenommen werden.

Diese Option aufzugreifen, wird empfohlen, da derzeit in Deutschland 2,2 Millionen gültige Ausweise als verloren oder gestohlen gemeldet sind und pro Jahr etwa 220.000 dazu kommen. Durch die Aufnahme der Fingerabdrücke wird, wie beim E-Pass, der Missbrauch des Ausweises und seine Benützung durch sich ähnlich sehende Personen erschwert.

Der *ePA* wird auch eine elektronische Identitätsfunktion (eID) besitzen, durch die er im E-Business und E-Government verwendet werden kann („Internet-Ausweis“). Der Bürger kann, wenn er diese Funktion beanspruchen will, seinen Wohnort eintragen lassen und logische Verknüpfungen mit diesem und mit seinem Alter zulassen.

Neben der Möglichkeit, sich im Internet gegenüber Geschäftspartnern und Behörden auszuweisen, wird eine automatisierte Unterscheidung möglich sein, ob der Ausweisinhaber jünger als 18 oder älter als 65 Jahre ist, ob also bei Geschäftsabschlüssen beispielsweise Bestimmungen des Jugendschutzes entgegenstehen oder Altersrabatte in Frage kommen. Wenn Angebote speziell auf seinen Wohnort zugeschnitten sind, werden ihm auch nur solche übermittelt.

IT-Sicherheitskongress: Über 500 Teilnehmer aus Verwaltung, Industrie und Wissenschaft.

Dem Bürger wird es nicht nur freistehen, diese – reversibel gestaltete – Funktion nach der Ausstellung des Personalausweises anzunehmen oder abzulehnen, er allein bestimmt, welche Daten er weitergibt. Bei der Aufnahme von Geschäftsbeziehungen im Internet wird sich der angefragte Geschäftspartner als Erster ausweisen müssen, was wieder eine behördliche Zulassung voraussetzt. Wenn jeder Partner sich der Identität des anderen sicher sein kann, ist eine vertrauensvolle Geschäftsabwicklung möglich und es bestehen Anzeichen dafür, dass sich auf dieser Basis neue Geschäftsmodelle entwickeln werden.

Der Chip ist für eine elektronische Signatur vorbereitet. Die Funktion zu aktivieren, sodass Dokumente signiert und damit vom Inhalt her fälschungssicher sind sowie auch verschlüsselt übertragen werden können, wird der privaten Initiative und den kommerziellen Trust-Centern überlassen.

Mit dem ePA enthält der Antragsteller von der Personalausweisbehörde einen Brief, in dem ihm seine PIN und PUK mitgeteilt werden sowie ein Sperrcode, mit dem er den Personalausweis bei Verlust sofort sperren lassen kann, auch online.

Cybercrime. „Die dem Bundeskriminalamt angezeigten erfolgreichen Fälle von Phishing sind von 4.500 im Rekordjahr 2007 auf etwa 1.800 im Jahr 2008 zurückgegangen“, berichtete Kriminalhauptkommissar Mirko Manske vom BKA. „Das ist auf die flächendeckende Einführung der E-TANs zurückzuführen, und es war interessant, im Internet zu beobachten, wie auf Seite der Kriminalität Projektgruppen gebildet wurden, um Gegenstrategien zu entwickeln.“

Das Problem, das sich Cyberkriminellen stellt, ist, dass es durch die von den Banken entwickelte Sensorik immer schwerer wird, „Finanzagenten“ für die Geldwäsche („Money Mules“ – Geldesel) aufzutreiben.

Das Muster, jemanden gegen eine prozentuelle Beteiligung dazu zu bringen, über sein Konto Geld beispielsweise nach Russland zu überweisen, funktioniert nicht mehr, denn über die Strafverfolgung wegen Geldwäsche hinaus droht dem Einzelnen auch der Verlust seines Kontos und es wird schwer werden für ihn, eine neue Hausbank zu finden.

Eigene Tätergruppen beschäftigen sich damit, gutgläubige Opfer zu rekrutieren. Da werden von Profis Geschichten erfunden: Der in Deutschland lebende, frisch geschiedene Mittfünfziger, der über eine Internet-Plattform Anschluss sucht, erhält Tage später eine E-Mail samt Foto einer attraktiven, in Russland lebenden jungen Dame, die ihm im weiteren Briefverkehr mitteilt, ihn als Mann ihrer Träume gerne besuchen zu wollen, aber leider das Geld dafür nicht zur Verfügung zu haben. Nicht, dass er ihr den Flug bezahlen solle, keineswegs, aber sie habe in Deutschland gearbeitet, allerdings schwarz, ob er nicht dieses Geld überwei-

Wolfgang Schäuble: „Mit der IT-Sicherheit steht und fällt die Funktionsfähigkeit unserer Gesellschaft.“

Mirko Manske: „Es wird immer schwerer, Finanzagenten für die Geldwäsche aufzutreiben.“

Fotos: Kurt Hickisch

11. Deutscher IT-Sicherheitskongress: Stand des Bundesamts für Sicherheit in der Informationstechnik.

sen könnte, jedoch nicht an sie, weil sie sonst Schwierigkeiten bekommen könnte, sondern an ihre Cousine ...

Identitätsdiebstahl. Die für Phishing ausgebrachte Malware löst nicht nur Finanz-Transaktionen aus, sondern kann Menschen ihre digitale Identität stehlen. Menschen verlieren nicht nur die Verfügungsmacht über ihr Bankkonto, sondern es werden auf ihren Namen und ohne ihr Wissen Bankkonten für die Geldwäsche eröffnet.

Sie verlieren die Kontrolle über ihre E-Mail-Zugänge, den Zugang zu Online-Händlern; über ihre beruflichen Fernwartungszugänge können Betriebsvorgänge gesteuert werden. Völlig neue Tatbegehungsmöglichkeiten tun sich auf, wie etwa Transportdiebstähle, wenn beispielsweise über einen zum Opfer gewordenen, nichts ahnenden Disponenten eines Transportunternehmens Einblick in die Logistik des Betriebs, die transportierten Güter und die Ruhezeiten der Fahrer gewonnen werden kann.

Die Gegenmaßnahmen bestehen darin, die Infektion des Opfers zu verhindern. Technische Sicherungsmaßnahmen helfen in solchen Fällen nur bedingt; es muss eine Veränderung im Verhalten der Internet-Nutzer erfolgen – sie müssen vorsichtiger und aufmerksamer werden. *Kurt Hickisch*

FOTO: KURT HICKISCH

IT-SICHERHEITSKONGRESS

Sicherheitslösungen

Die Vorträge des in der Stadthalle Bonn-Bad Godesberg vom 12. bis 14. Mai 2009 abgehaltenen Kongresses wurden großteils parallel in zwei Sälen abgehalten. In einer den Kongress begleitenden Ausstellung präsentierten Unternehmen Sicherheitslösungen für den IT-Bereich. Nach der Verleihung des „Best Student Awards“ an einen von fünf nominierten jungen Forschern, die über ihre Arbeiten referiert hatten, wurde der Kongress mit einer Podiumsdiskussion abgeschlossen, an der unter anderem der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, teilnahm.

www.bsi.bund.de/kongress2009