Vertrauen gewinnen

Wie das Vertrauen nach den Ausspähaffären in die Informations- und Kommunikationstechnik wieder hergestellt werden kann, war ein Kernthema der *it-sa* 2013 in Nürnberg.

Nach einer vom *BITKOM* in Auftrag gegebenen Umfrage im Jahr 2013 bezeichneten 39 Prozent der Befragten ihre Daten im Netz als „eher unsicher“ und 27 Prozent als „völlig unsicher“. „Vor zwei Jahren hatten nur etwas mehr als die Hälfte der Internet-Nutzer diese Sorge um ihre Daten“, berichtete Winfried Holz, Präsidiumsmitglied des *BITKOM* bei der Eröffnung der Sicherheitsmesse *it-sa* am 8. Oktober 2013 in Nürnberg.

Ein Grund für den Anstieg seien bekannt gewordene Ausspähaktionen. Die Folge sei allerdings weniger gewesen, konkrete Maßnahmen gegen Ausspähung zu treffen, wie etwa die Nutzung von Verschlüsselungstechniken oder Anonymisierungsdiensten, sondern eine Abkehr vom Versenden von E-Mails oder der Nutzung einer Cloud – was Einbußen in der Wettbewerbsfähigkeit nach sich ziehe.

Das Bekanntwerden des Einsatzes von Spähprogrammen wie *Prism* und *Tempora* bezeichnete Andreas Könen, Vizepräsident des *Bundesamts für Sicherheit in der Informationstechnik (BSI),* als „Weckruf“ für die User und die Sicherheitsindustrie. Es gelte, sichere Informationstechnologien zur Verfügung zu stellen. Durch die Zertifizierung von IT-Sicherheitsprodukten und -Dienstleistungen leiste das *BSI* seinen Beitrag und stehe dem Bürger und der Wirtschaft beratend zur Verfügung, unter anderem mit dem erweiterten Grundschutzhandbuch.

Das Bindeglied zur Wirtschaft sei die *Allianz für Cybersicherheit*. Pro Tag würden drei bis fünf kritische Angriffe auf Regierungsnetze festgestellt. Für DDos-Angriffe würden mittlerweile an die 10.000 gehackte Server eingesetzt, mit einer Gesamtangriffsleistung bis zu 100 GBit/sec.

Cornelia Rogall-Grothe: „Das Vertrauen in die IKT-Sicherheit muss gestärkt werden.“

Udo Kalinna: „Es sind immer die gleichen Programmierfehler, die Hacker-Angriffe ermöglichen.“

Die Erhaltung und Stärkung des Vertrauens in die Sicherheit und Integrität der IKT bezeichnete Staatssekretärin Cornelia Rogall-Grothe, Beauftragte der Bundesregierung für Informationstechnik, als vorrangiges Ziel. Das IT-Sicherheitsgesetz werde in der neuen Legislaturperiode weiter betrieben, die Aufgaben des BSI würden erweitert und seine Kompetenzen gestärkt, die Forschung zur IT-Sicherheit werde gefördert.

Bei IT-Sicherheitsprodukten müsse sich „made in Germany“ als Qualitätsmerkmal etablieren. Bei öffentlichen Vergaben werde verstärkt auf die sichere IT-Infrastruktur der Auftragnehmer geachtet. Die Betreiber kritischer Infrastruktur würden zu einer Verbesserung des Schutzes ihrer IT-Systeme und zur Verbesserung ihrer Kommunikation mit dem Staat verpflichtet und Telekommunikations- und Telemediendienste stärker in die Verantwortung genommen werden.

Auch Prof. Dr. Claudia Eckert forderte in sich sichere IT-Produkte *(Security by Default)*, vor allem in Bezug auf eingebettete Systeme, wie sie etwa in Industrieanlagen und Produktionsketten zu finden sind. Anders als ein PC können Produktionsanlagen nicht bei laufendem Betrieb gepatcht werden. Durch Fernwartungsmöglichkeiten sind IT-Systeme, etwa solche von Kraftwerksanlagen, nicht mehr wie früher völlig abgeschottet. Um bestehende Anlagen herum müssten virtuelle Schutzmauern gebaut werden.

„Plug and trust“ müsse der Leitgedanke für IT-Entwicklungen sein. Es seien immer die gleichen, altbekannten Programmierfehler, die einen Großteil der Hacker-Angriffe ermöglichen, sagte Univ.-Prof. DI Udo Kalinna von der Hochschule Emden/Leer. Das 2001 gegründete *Open Web Application Security Project (OWASP)* veröffentlicht alle drei Jahre eine Auflistung der zehn größten Risiken für Webanwendungen *(OWASP* Top 10 List). An der Spitze der Fehlerquellen stehen SQL-Injection (in Datenbanken werden über Funktionszeichen – deren Eingabe man leicht sperren könnte – Befehle eingeschleust) und Cross-Site-Scripting (XSS; Schadcode wird über Webanwendungen eingeschleust).

Die Gründe dafür sieht Kalinna darin, dass Webapplikationen aus Wettbewerbsgründen fast immer unter enormem Zeitdruck erstellt würden, das Bewusstsein für Sicherheitsaspekte bei den Entwicklern nur ungenügend vorhanden sei und Qualitätsmanagement kostenmäßig

it-sa

Fachmesse

Die *it-sa* im Messezentrum Nürnberg ist die einzige Fachmesse für IT-Sicherheit im deutschsprachigen Raum. Ideelle Träger sind das *Bundesamt für Sicherheit in der Informationstechnik (BSI), BITKOM* und die Initiative *Deutschland sicher im Netz e.V. (DsiN)*. Bei der 5. it-sa vom 8. bis 10. Oktober 2013 gab es 357 Aussteller (+ 7 %) und 6.900 Fachbesucher. Messebegleitend wurde der 2. Congress@it-sa abgehalten. Die nächste *it-sa* wird vom 7. bis 9. Oktober 2014 in Nürnberg stattfinden.

www.it-sa.de

Fotos: Kurt Hickisch

kaum untergebracht werden könne, zumal meist der Billigstbieter den Auftrag bekomme.

Praktisch vorgeführt wurden derartige Angriffsarten bei den täglichen Live-Hackings, unter anderem von Sebastian Schreiber (*Syss-GmbH)*. Das von ihm schon vor Jahren gezeigte Beispiel einer Manipulation der Preisauszeichnung eines Online-Shops funktioniert immer noch. Neu war ein Angriff auf die dahinterstehende Datenbank durch Manipulation des Barcodes eines Produktes. Dazu kamen eine Fülle von Angriffen auf Handys, Krypto-Sticks und gesperrte Laptops.

Bei Penetrationstests versetzt sich ein Unternehmen in die Rolle eines Angreifers und versucht, beim Auftraggeber Schwachstellen in der IT herauszufinden, um diese in weiterer Folge zu schließen.

Datenverschlüsselung. Der Sicherheit der auf USB-Sticks, Laptops und anderen Geräten abgespeicherten Daten vor fremdem Zugriff kommt nicht nur aus faktischer, sondern auch aus rechtlicher Sicht große Bedeutung zu.

Die nach § 14 DSG erforderlichen Sicherheitsmaßnahmen – zu denen gehört, dass personenbezogene Daten Unbefugten nicht zugänglich sind – gröblich außer Acht zu lassen, stellt nach § 52 Abs. 2 Z 5 DSG eine mit Geldstrafe bis zu 10.000 Euro zu bestrafende Verwaltungsübertretung dar.

Ferner besteht bei unrechtmäßiger Verwendung personenbezogener Daten die Verpflichtung, die Betroffenen zu informieren (§ 24 Abs. 2a DSG). Dazu kommt die Verpflichtung zum Ersatz eines eingetretenen Schadens. Neben sonstigen Vorsichts- und Schutzmaßnahmen ist auch die

Sebastian Schreiber: Manipulation am Barcode.

Verschlüsselung der abgespeicherten Daten in Betracht zu ziehen.

Digittrade (www.digittrade.de) bietet mobile Datenträger (Krypto-Sticks bis 16 GB, Festplatten) an, die hardwaremäßig verschlüsselt sind. Hardwareverschlüsselte USB-3.0- Sticks, die keine zusätzliche Software brauchen, bietet auch Prosoft *(www.prosoft.at)* mit Safe-To-Go an: Alle Daten am Stick sind 256-bit AES verschlüsselt und durch ein Passwort geschützt. Der Stick funktioniert sofort unter *Windows, MAC OS* und *Linux*. Bei Inaktivität sperrt sich der Stick automatisch. Er kann optional über die „Safe-Console" zentral konfiguriert und verwaltet werden.

PDWatch von *itWatch GmbH (www.itwatch.de)* ist eine Softwarelösung, durch die die Verschlüsselung beim Export von Daten auf beliebige Datenträger erzwungen werden kann.

Der „Secure Boot Stick" von *Ecos Technology GmbH (www.ecos.de)* erlaubt, beruflich zu Hause über eine Internetverbindung gesichert mit Firmendaten zu arbeiten, und ist für Telearbeitsplätze interessant. Die private Festplatte wird dabei nicht benützt, der Stick selbst ist das Speicher- und Verarbeitungsmedium, das zentral konfiguriert ist. Gebootet wird vom Stick. Ohne Freigabe durch den Administrator können Daten nicht auf ein externes Speichermedium kopiert oder ausgedruckt werden.

Ein für private Anwendung kostenloses Programm zur Verschlüsselung von Datenträgern, Partitionen oder Ordnern ist *True-Crypt (www.truecrypt.org)*. Als Programmbestandteil weit verbreitet ist der *Bitlocker*.

Sichere Kommunikation. Die *Secusmart GmbH (www.secusmart.com)* hat mit *Secu-SUITE* eine Lösung vorgestellt, bei der mit Hilfe einer in den Slot eines *Blackberrys 10* eingesetzten Micro-SD-Card das Gerät in einen persönlichen und einen geschäftlichen Teil getrennt wird. Dieser Teil (SMS, E-Mails, Adressbuch, Kalendereinträge) wird durch die auf der Karte befindlichen Prozessoren durch Verschlüsselung vor fremdem Zugriff geschützt, ebenso die von diesem Teil abgehende Kommunikation (Sprachtelefonie, SMS, Mails).

Rhode&Schwarz (www.sit.rhode-schwarz.com) bietet mit dem TopSec Mobile ein Gerät für mobile, internetbasierte Telefonie an, das Sprache bereits im Gerät selbst hardwaremäßig verschlüsselt und in dieser Form über Handy oder Internet dem mit einem gleichen Gerät ausgestatteten Gesprächspartner übermittelt. Ein *Man-in-the-Middle* hört nur ein Rauschen.

Produkte. Die Firma *PCS Systemtechnik GmbH (www.pcs.com)* präsentierte bei der *it-sa*-Sonderausstellung „Das perfekte Rechenzentrum" ein Handvenenerkennungssystem für die Zutrittskontrolle.

Das sauerstoffarme venöse Blut absorbiert Infrarotstrahlung, wodurch die an der Handinnenfläche liegenden Adern erkennbar werden. Die Lage dieser Adern ist individuell und unveränderbar. Von diesem Muster wird ein Abbild erstellt, das als errechnetes Template mit einem Datenumfang von etwa 0,8 bis 3 KB gespeichert wird. Mit diesem Template werden die Vergleiche hergestellt, wobei es genügt, die Handinnenfläche vor den Sensor zu halten.

Die Häufigkeit, wie viele nicht berechtigte Personen vom System akzeptiert werden (False Acceptance Rate – FAR) wird mit 0,00001 Prozent angegeben. Es braucht nichts körperlich berührt zu werden, Verschmutzungen sind ohne Einfluss und gegenüber der in der geringen Fehlerrate vergleichbaren Iris-Erkennung entfällt die Sorge vor Schäden am Auge.

Wird bei der Zutrittskontrolle zusätzlich ein maschinlesbarer Ausweis eingesetzt oder die Eingabe einer PIN verlangt, braucht nur die Übereinstimmung überprüft zu werden (Verifikation; One-to-One). Das erfolgt schneller als ein Abgleich mit sämtlichen vorhandenen Datensätzen (Identifikation; One-to-Many).

Ein System zur Abwehr von DDoS-Angriffen, selbst wenn sie von großen Botnetzen aus gefahren werden, bietet die *Link11 GmbH (www.link11.de)* an. Das Unternehmen, das unter anderem den *Eco-Award 2012* für die innovativste DDoS-Schutzlösung erhalten hat, lenkt derartige Angriffe auf seine eigenen Hochleis-

FOTO: KURT HICKISCH

Handvenenerkennungssystem für die Zutrittskontrolle: Die Lage der Venen ist individuell und unveränderbar.

Foto: Kurt Hickisch

tungsserver um, deren Kapazität ausreicht, die Angriffe abzufangen. Durch ein Filtersystem wird nur jener Datenverkehr zum Auftraggeber durchgelassen, der dem üblichen Geschäftsverkehr entspricht.

Brandschutz. *Aero-X* ist ein innovatives Brandschutzsystem auf der Basis von Aerosolen *(www.aerox-vertrieb.de)*. Obwohl auch Rechnerräume als solche abgesichert werden können, ist das System vornehmlich zum Einsatz in den einzelnen Serverschränken gedacht – dort, wo ein Brand am ehesten entstehen kann. Das Löschmittel ist in fester Form in zylindrischen Behältern aus Edelstahl enthalten, an deren oberen Ende sich die Kabelanschlüsse befinden und am unteren die Ausströmöffnungen. Die Behälter werden auf die Schränke aufgesetzt. Bei Aktivierung wird das Löschmittel über einen eingebauten Generator in ein nach unten in den Schrank ausströmendes Aerosol umgesetzt, das die Verbrennungsreaktion unterbindet.

Das Löschmittel ist weder korrosiv noch elektrisch leitend und hinterlässt lediglich Staub als Rückstand. Druckleitungen, Kompressoren und Druckgasflaschen können entfallen. Einige Modelle benötigen nicht einmal eine externe Stromquelle. Speziell für den Einsatz in Schränken zur Brandfrüherkennung wurde von der Datanet Kommunikationsnetze GmbH der *Rack-Sniffer* entwickelt *(www.datanet-networks.de)*. Durch die größere Nähe zur Rauchquelle wird entstehender Rauch früher erkannt als über eine Rauchansauganlage.

Die *AfB Arbeit für Menschen mit Behinderung gemeinnützige GmbH (www.afb-group.eu)* mit Sitz in Essen, die auch in Österreich vertreten ist, verbindet *Green IT* mit der Beschäftigung von Menschen mit Behinderung. Nicht mehr benötigte IT-Hardware aller Art (PCs, Notebooks, Drucker, Handys), die ansonsten entsorgt würde, wird auf Wunsch abgeholt. Die Funktionsfähigkeit der Geräte wird überprüft. Auf Datenträgern noch vorhandene Daten werden nach einem zertifizierten Verfahren zuverlässig gelöscht. Nicht mehr brauchbare Teile werden geschreddert und als Rohstoff wiederverwertet. Verwertbares wird zu funktionsfähigen Geräten zusammengebaut, die als gebrauchte Geräte mit einjähriger Garantie wieder verkauft werden. Diese Arbeiten erfolgen durchwegs von Menschen mit Behinderung. *Kurt Hickisch*