„Mordversuch“ durch Hacking: IT-Sicherheitsexperte Barnaby Jack versuchte auf der „Defence“ zu demonstrieren, wie man per Funk die Funktion einer Insulinpumpe beeinflussen kann.

Gefährliche Schwachstellen

Auch für sicher gehaltene IT-Systeme enthalten Schwachstellen, die Angriffsmöglichkeiten bieten. Das wurde auf der 10. IT-Defense in München deutlich gemacht.

Einige wenige Großunternehmen spielen immer mehr eine Rolle im Leben des Einzelnen, weil sie diesem immer mehr Dienste anbieten, von der Information über Kommunikation bis zur Ablage von Daten in der „Cloud“. Dazu kommt, dass es bereits billiger ist, Daten zu speichern, als diese wieder zu löschen. Bei Zusammenführung aller Daten aus diesen Diensten ergibt sich innerhalb eines Unternehmens ein umfassendes Bild über das Individuum, sein Vorleben, seine Neigungen, sein Verhalten als Konsument. Die vier großen Unternehmen *Google, Facebook, Amazon* und *Apple* würden damit auch zu einer Marktmacht mit politischem Einfluss, sagte IT-Sicherheits-„Guru“ Bruce Schneier bei der 10. *IT-Defense* im München.

„Big Data kommt auf uns zu“, warnte Schneier. Je mehr an Aktivität in das Internet verlagert werde, umso mehr werde sich auch die Kriminalität dorthin verlagern. Das wiederum ziehe eine stärkere gesetzliche Regulierung nach sich, verbunden mit Einschränkungen der Privatsphäre. IT-Experte Schneier wies auf die Gefahr eines Wettrüstens auf dem Gebiet des Cyberwars hin, mit dem Virus *Stuxnet* als der ersten für einen solchen Krieg entwickelten Waffe, und warf die Frage nach einer „Friedensbewegung“ auf diesen virtuellen Kampfplätzen der Zukunft auf.

Über soziologische Auswirkungen in der Arbeitswelt referierte Prof. Dr. Gunter Dueck. Arbeit wird immer mehr in Einzelschritte zerlegt, die von angelernten Kräften billiger erledigt werden. Gleiches gilt für Dienstleistungen: Formulare können aus dem Internet bezogen, Patente über Internet angemeldet werden. Umfassendes Wissen wird nur mehr von jenen verlangt, die für die große Übersicht und Problemfälle benötigt werden – und das werden immer weniger sein, die umso mehr gefordert werden.

Rechtsprobleme. Über Handlungen im Internet, die zu gravierenden Problemen und zu persönlicher Haftung führen können, berichtete Prof. Dr. Thomas Hoeren von der Universität Münster. Whistleblowing – das Aufdecken von Missständen – kann als Verrat von Unternehmens- oder Betriebsgeheimnissen gewertet werden; die Veröffentlichung von Dokumenten (Stichwort: *Wikileaks*) zudem als Eingriff in Urheberrechte.

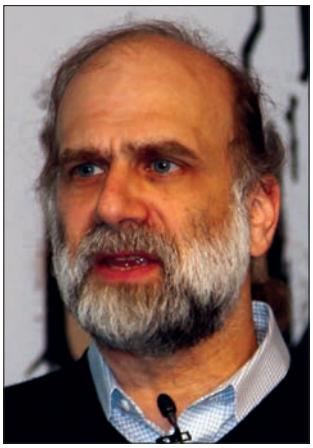
Das eigene Unternehmen in sozialen Medien herabzusetzen, kann als Verletzung der Treuepflicht zur Entlassung führen. Der Verlust personenbezogener Daten muss nach der *Data-*

FOTO: KURT HICKISCH

Adam Laurie: „Hacker können auch Messsysteme manipulieren."

Prof. Gunter Dueck: Soziologische Auswirkungen in der Arbeitswelt.

Timo Kasper: „Seitenkanal-Angriffe auf Smartcards sind möglich."



IT-Sicherheits-Guru Bruce Schneier: „Big Data kommt auf uns zu."

Breach-Notification-RL bekannt gemacht werden; Nichtbeachtung zieht Haftungsfolgen nach sich. Den Laptop, auf dem sich personenbezogene Daten befinden, zur Reparatur zu geben und damit anderen den Zugriff auf diese Daten zu ermöglichen, ist datenschutzrechtlich bedenklich; ebenso, wie derartige Daten in die Cloud auszulagern, oder Data Mining für Werbezwecke oder um Personenprofile zu erstellen.

Wurde in einem Unternehmen auch nur stillschweigend das Schreiben und Empfangen privater E-Mails zugelassen, unterliegen diese dem Schutz des Briefgeheimnisses. Fotos aus dem Internet können wegen des Urheberrechtsschutzes nicht ohne Weiteres verwendet werden. Es ist die Zustimmung des Fotografen und fast immer auch des Abgebildeten erforderlich.

Virales Marketing, das gesteuerte Anpreisen von Produkten in sozialen Medien, kann irreführende Werbung sein. Der Betreiber eines WLANs ist für von dort versendete fremde Inhalte verantwortlich, wenn er das Netzwerk nicht gegen Eindringen von außen abgesichert oder bloß das Passwort des Herstellers belassen hat.

Smart-Metering. Intelligente Stromverbrauchszähler messen nicht nur den Stromverbrauch, sondern speichern auch die Daten und kommunizieren mit dem Versorgungsunternehmen, dem sie beispielsweise diese Daten in Zeitrastern für Abrechnungszwecke übermitteln. Dem Kunden bieten sie die Möglichkeit, auf der Basis dieser Daten Energie effizienter einzusetzen.

Es eröffnen sich allerdings auch neue Angriffsmöglichkeiten, über die Adam Laurie berichtete: Hacker könnten auf der Basis des Stromverbrauchs ermitteln, ob jemand zu Hause ist. Mit kriminellem Hintergrund könnten die Messeinrichtungen manipuliert oder Teilnehmerdaten verändert werden. Letztlich könnte durch Angriffe der Strombezug unterbunden oder das Netz blockiert werden.

Die Systeme sollten Penetrationstests wie bei sonstigen Netzwerken unterworfen werden, um Schwachstellen aufzudecken. Zu bedenken sei, dass die Systeme auf eine lange Betriebsdauer ausgelegt seien und ein Nachhinken im Sicherheitsstandard zu befürchten sei, insbesondere hinsichtlich der kryptografischen Verschlüsselung der Daten.

Online-Bedrohungen. Mikko H. Hypponen, Chief Research Officer bei *F-Secure (www.f-secure.com),* sieht drei Gruppen von Angreifern im Internet: Kriminelle, Hacktivists und Staaten. Extremisten und Terroristen könnten folgen. Wie (organisierte) Kriminelle mit Hilfe des Internet arbeiten, schilderte Hypponen anhand eines Falles, der sich im November des Vorjahres in Dänemark zugetragen hatte: Über Zeitungsanzeigen wurden Mitarbeiter für ein aufstrebendes Versandunternehmen gesucht, die eingelangte Warensendungen dem Gewicht nach zu überprüfen, neu zu frankieren und weiter zu versenden hätten. Die Arbeit könne zu Hause erfolgen. Damit wurden die „Packet Mules" rekrutiert. In einem zweiten Schritt wurde die Online-Ausgabe der drittgrößten dänischen Zeitung nachgeahmt. Beim Anklicken dieser Website lud sich ein kleines Programm (Java-Skript) auf den Rechner, das alle wesentlichen Daten des Betriebssystems abfragte und einen Keylogger installierte, über den bei Online-Bestellungen die Kreditkartendaten ausgespäht und übermittelt wurden.

Mit diesen Daten wurden in Onlineshops begehrte elektronische Konsumgüter wie *iPhones, iPads, Tablet-PCs* bestellt. Das war unverdächtig, da mit einer dänischen Kreditkarte über eine dänische IP-Adresse diese Güter an eine dänische Lieferadresse zu schicken waren. Der Weg dieser Güter wurde auch mit Hilfe eines Transponders nachvollzogen. Der Transport erfolgte zunächst nach Rotterdam und dann per Lkw in einen kleinen Ort in Ostpolen. Er endete dort bei einer alten Frau, die bereits Dutzende solcher Lieferungen erhalten hatte. Nachfragen in diesem Ort ergaben, dass fast alle Dorfbewohner solche Sendungen erhalten hatten. Die Pakete wurden eingesammelt und über die nahe Grenze in die Ukraine verbracht. Letztlich wurden sie auf Märkten in Moskau zum Verkauf angeboten. Andere „Geschäftsmodelle" bestanden darin, von vornherein infizierte Computer zum Kauf anzubieten, oder als Internet-Service-Provider für Kriminelle aufzutreten, mit Abschottung gegenüber behördlichen Nachforschungen.

„Hacktivisten" geht es nicht um Geld, sondern um Protest. Beispiele dafür sind Attacken gegen Websites von zum Feindbild erklärten Unternehmen.

Bei staatlich gelenkten Angriffen stehen Spionage

FOTOS: KURT HICKISCH

und Sabotage im Vordergrund. Zielpersonen sind Regierungsbeamte, Forscher und Entwickler vornehmlich im Verteidigungsbereich. Sie erhalten eine völlig unverdächtig erscheinende E-Mail mit einem Anhang („Sende Ihnen dieses File zur Durchsicht."). Die Adresse des Absenders ist gespooft – er ist nicht der, als der er sich ausgibt. Durch Anklicken des Anhangs wird der Rechner infiziert und ist unter Kontrolle des Angreifers.

Gefährliche Schwachstellen. Barnaby Jack beschäftigt sich als Forscher bei *McAfee* mit Schwachstellen in elektronischen Systemen, die, in Geräten eingebaut und vom Benutzer weitgehend unbemerkt, Überwachungs-, Steuerungs- oder Regelfunktionen übernehmen *(Embedded Systems)*. Solche Minicomputer finden sich bereits in den meisten technischen Lebensbereichen – von Waschmaschinen bis zu Fernsehern und auch in Geräten der Medizintechnik.

Barnaby Jack berichtete über eine Schwachstelle, die von ihm in einer der in den USA meistverwendeten Insulinpumpen entdeckt wurde und die von außen her über Funk unautorisierte Zugriffe auf die Pumpe und die von ihr abgegebene Insulinmenge ermöglichte. Eine Testapparatur wurde aufgebaut und der über eine Richtantenne erfolgende Angriff vorgeführt. Dieser gelingt auch ohne Kenntnis der Seriennummer des Geräts. Er hatte allerdings keinen Erfolg bei der Insulinpumpe eines Tagungsteilnehmers, der sich spontan zur Verfügung gestellt hatte. Wenn auch derartige Angriffsszenarien schon von der Idee und auch wegen der einzusetzenden Apparatur weit hergeholt erscheinen, zeigen sie doch, dass solche Systeme auch aus Sicherheitsaspekten ständig weiterentwickelt werden müssen.

IT-Experten Andrea Barisani, Daniele Bianco: „Kriminelle können Daten auch von Chipkarten unautorisiert auslesen."

Chipkarten, wie sie als Kreditkarten in Bezahlsystemen verwendet werden, sind nicht uneingeschränkt sicher, berichteten Andrea Barisani und Daniele Bianco. Die beiden Referenten zeigten, dass auch von Chipkarten *(Smartcards)* durch eine Form des Skimmings Daten unautorisiert ausgelesen werden können und dass gestohlene Chipkarten auch ohne Kenntnis der PIN verwendet werden können.

Diese Erkenntnisse stehen im Gegensatz zu der gängigen Auffassung, dass die Abhebung eines Geldbetrags zu Lasten desjenigen geht, auf den die Karte ausgestellt wurde, wenn unter Verwendung dieser Karte und der PIN Abhebungen getätigt werden – sei es auch nur deshalb, weil er die PIN entgegen der vertraglichen Verpflichtung nicht genügend geheim gehalten hätte.

Timo Kasper von der Universität Bochum berichtete von einer anderen Angriffsmethode auf Embedded Systems – einen Seitenkanal-Angriff, der auch gegen Smartcards durchgeführt werden kann. Ein solcher Angriff richtet sich nicht direkt gegen den Chip, sondern nützt Nebeneffekte, wie den Stromverbrauch, der mit dem Oszilloskop auf der Zeitachse gemessen wird. Signifikante Schwankungen zeigen Verarbeitungsprozesse an wie etwa eine einsetzende kryptografische Verschlüsselung. Auf diese Weise ist es gelungen, den Schlüssel für ein kontaktlos funktionierendes elektronisches Zahlungssystem zu knacken. Da alle Karten den gleichen Schlüssel hatten (was der Fehler war), konnten Karten mit Bezahlfunktion geklont, im aufgeladenen Geldbetrag verändert und Karten mit neuen Nummern produziert werden. Es war möglich, den Speicherinhalt bis auf eine Entfernung von 30 Zentimetern auszulesen, wobei dieser Vorgang lediglich 20 Millisekunden gedauert hat.

Kevin Mitnick wurde in den 1990er-Jahren in den USA als Hacker wegen Bedrohung der nationalen Sicherheit vor Gericht gestellt. Sein Fall lenkte das öffentliche Interesse auf die Informationssicherheit. Einige Monate nach seiner Entlassung aus einer fünfjährigen Haftstrafe im Jänner 2000 wurde er Berater des US-Kongresses in IT-Sicherheitsfragen. Heute betreibt er ein Unternehmen für Fragen der IT-Sicherheit. *Kurt Hickisch*

FOTO: KURT HICKISCH

IT-SICHERHEIT

IT-Defense

Seit 2003 veranstaltet die auf IT-Sicherheitsdienstleistungen spezialisierte Heilbronner *Cirosec GmbH* jährlich in Deutschland die *IT-Defense*. Die 10. Veranstaltung hat vom 8. bis 10. Februar 2012 in München stattgefunden. Die Teilnehmer kamen aus der Wirtschaft, der öffentlichen Verwaltung, Behörden und Militär. Die zwölf Vorträge boten einen bunten Mix aus Information, Unterhaltung, rechtlichen und hoch spezialisierten Themen. An den beiden Vortagen gab es Hacking-Trainings und es wurden Gegenmaßnahmen diskutiert. In einer „Hacking Area" konnte man sich als Hacker versuchen. In Round Tables am 10. Februar unterhielten sich die Teilnehmer mit den Referenten über spezielle Themen. Die nächste *IT-Defense* findet vom 30. Jänner bis 1. Februar 2013 in Berlin statt.

www.cirosec.de
www.it-defense.de