Digitaler Umbruch

Beim 12. Österreichischen IT-Sicherheitstag am 15. Oktober 2015 in Klagenfurt erörterten Experten Probleme, die durch die fortschreitende digitale Vernetzung entstehen.

Wohin gehen unsere Daten? Antworten darauf gab DI Robert Schoblick, Redaktionsbüro SRG.at, beim 12. Österreichischen IT-Sicherheitstag am 15. Oktober 2015 in Klagenfurt. Die in verschiedenen Systemen erfassten Datenmengen werden zu „Big Data“ und machen Auswertungen möglich. Menschen teilen über soziale Netzwerke ihre Fitnesswerte mit. Die Personenwaage ist über Bluetooth mit dem Handy verbunden, ein Schrittzähler postet die täglichen Jogging-Leistungen. Zur Risikoeinschätzung sind derartige Daten wichtig für Krankenversicherer, aber auch für Pharmavertreter oder Lifestyle-Berater.

Im Automotive-Bereich werden über Sensoren übermittelte technische Daten bis hin zu Fahrverhalten und Positionsangaben gespeichert. Es können Bewegungsprofile erstellt und die Daten zur Berechnung von Versicherungsprämien herangezogen werden. Fahrzeuge werden künftig miteinander in Verbindung treten *(Car2Car-Connectivity),* um Unfälle zu vermeiden. Die Kommunikation bleibt aber nicht auf die interagierenden Fahrzeuge beschränkt, sondern kann zu einer Verkehrsüberwachung führen, wie sie etwa bei der Videoüberwachung auf Autobahnen bereits besteht.

Im „Smart Home“ wird künftig alles vernetzt und über das Smartphone steuerbar sein. Was ist, wenn in die Systeme eingedrungen wird und nicht nur Alarmanlagen ausgeschaltet, sondern sogar elektronisch gesteuerte (Garagen-)Toren und Türen

„Smart Home“: Die Steuerung von Anlagen in einem Haus mit einem Smartphone birgt auch Sicherheitsrisiken.

geöffnet werden und so Zutritt zum Gebäude erlangt wird? Die Lebensgewohnheiten von Menschen werden über vernetzte Systeme offenbar und eröffnen neue Angriffsmöglichkeiten.

Bei Industrie 4.0, wenn also in der Fertigungstechnik und der Logistik Maschinen mit Maschinen kommunizieren, wird der IT-Sicherheit noch mehr Bedeutung zukommen. Manipulationen in der Fertigungstechnik können zu Produktsabotage führen, die ihrerseits teure Rückrufaktionen und Image-Schäden nach sich zieht. „Digitale Welten sind grundsätzlich angreifbar“.

Das gemeinsame Netzwerk für die fortschreitende Digitalisierung aller Lebensbereiche ist das „Internet der Dinge“. Bei ungewollt oder bewusst herbeigeführten Störungen drohen ernst zu nehmende Folgeschäden. „Die Anforderungen an die Sicherheit des Netzes steigen, aber die Angriffstechniken werden weiter verfeinert“, sagte DI Robert Jankovics, *Kapsch BusinessCom AG*. Die Erkennungsrate von klassischen, auf Erkennungsmustern (Signaturen) aufbauenden Antiviren-Schutzprogrammen sinkt, indem Malware mit sich selbstständig veränderndem Schadcode eingesetzt wird (Polymorphismus), der Code verschlüsselt wird (Encrypted Payload) und komplexe Angriffsmuster verwendet werden, etwa, indem nach einer Erstinfektion der tatsächliche Schadcode nachgeladen wird. Eine Lösung bietet unter anderem die dynamische Verhaltensanalyse. In einer „Sandbox“ wird das Verhalten des Codes analysiert.

Honeypots. Ein derartiges Verfahren ist die von DI Fabian Mittermair von *Sec Consult (www.sec-consult.com)* vorgestellte *CyberTrap (www.cybertrap.com)*. Den Angreifern, besonders jenen, die gezielte Attacken durchzuführen beabsichtigen *(Advanced Persistent Threats – APT),* wird über eine Schwachstelle als Köder eine attraktive Falle *(Honeypot)* gestellt. In einer kontrollierten Umgebung wird das Verhalten des Schadprogramms nicht nur beobachtet, sondern der Angreifer wird auch mit scheinbar wichtigen Informationen versorgt, um ihn möglichst lange in der Falle zu halten. Ziel ist zu erkennen, worauf es der Angreifer abgesehen hatte, und seine weiteren Schritte bis zum Auftraggeber zurückzuverfolgen. Dabei werden Erkenntnisse über die verwendeten Tools und die angewendeten Methoden gewonnen.

Die *Deutsche Telekom* betreibt mit dem Projekt *sicherheitstacho.eu (www.sicherheitstacho.eu)* ein Honeypot-Netz, aus dem sich, aufgezeichnet von 180 Sensoren, unter anderem Rückschlüsse auf Angriffsmuster und Angreiferverhalten ableiten lassen.

Bedrohlich sei, dass das benötigte Wissen zum Ausnützen von Schwachstellen immer geringer wird, sagte Thomas Haase von der *T-Systems Multimedia Solutions GmbH (www.t-systems.com)*. Statt bloßer Baukästen für Viren und Trojaner kann man mittlerweile über professionelle Services zielgerichtete Attacken mieten oder kaufen; erstklassige Kundenbetreuung inbegriffen.

Die Angriffe (APT) werden immer zielgenauer; Angriffsziele, wie etwa industrielle SCADA-Netzwerke, werden durch die Entwicklung neuer Suchmaschinen leichter gefunden. In Unternehmen eingesetzte Applikationen sowie individuelle

FOTO: FOTOLIA/ARTUR MARCINIEC

Robert Jankovics: „Internet der Dinge ist das Netz für die fortschreitende Digitalisierung aller Lebensbereiche."

Stefan Jakoubi: „Kleine und mittlere Unternehmen sollten eine ISO-27001-Zertifizierung anstreben."

Peter Mader: „Der Stein der Weisen ist für Zahlungen im Onlinehandel noch nicht gefunden."

Thomas Haase: „Man kann über professionelle Services zielgerichtete Attacken mieten oder kaufen."

Software sollten nach international anerkannten Verfahren einem Qualitätstest unterzogen und das Bestehen eines solchen Tests bescheinigt werden.

Kleine und mittlere Unternehmen (KMUs) sollten eine Zertifizierung *ISO 27001* anstreben, regte Stefan Jakoubi von der *SBA Research gGmbH (www.sba-research.org)* an. Nicht nur, dass eine solche Zertifizierung in Ausschreibungen oder von Kunden verlangt wird, kann eine Zertifizierung auch einen Wettbewerbsvorteil darstellen. Zudem führt das Verfahren durch die strukturierte Vorgangsweise zu einem eine Gesamtschau bietenden Informationssicherheits-Management-System, das kontinuierlich fortzuführen und weiterzuentwickeln ist, um auf dem aktuellen Stand zu bleiben.

Awareness. Neben dem Ausnützen von technischen Schwachstellen ist Social Engineering eine Möglichkeit, in ein Unternehmensnetz einzudringen. Marcus Leeb von der *EPEIOS-Group* der *Alpen-Adria Universität Klagenfurt (www.-epeios-group.com)* schilderte die Herangehensweise: In der Phase passiver Informationsbeschaffung wird versucht, sich über Suchmaschinen, Webseiten und soziale Netzwerke ein möglichst umfassendes Bild über das anzugreifende Unternehmen zu verschaffen. Wird festgestellt, dass über die Website Stellen ausgeschrieben werden, kann in den per E-Mail gezielt an die Chefsekretärin übersendeten Unterlagen noch ein Schadprogramm verpackt werden, mit dem es gelingt, im Unternehmen Fuß zu fassen, nach und nach weitere Rechner zu übernehmen und Daten abzuschöpfen. Der Chef kann wegen seiner Vorliebe für Smartphone-Apps auf eine geklonte Website gelockt und veranlasst werden, sich unbewusst ein Tool herunterzuladen, mit dem nicht nur persönliche Informationen und Daten kopiert, sondern auch Kamera und Mikrofon gesteuert werden. Solche Angriffe werde man nicht vollständig verhindern können. Sie könnten aber durch Sensibilisierung der Mitarbeiter zumindest erschwert werden, sagte Leeb.

Social Engineering sei nur eine Art, über Mitarbeiter zu Informationen zu gelangen, berichtete Erik Rusek von der *Awarity Training Solutions GmbH (www.awarity.at)*. Häufig wird das Risiko nicht bedacht, wenn scheinbar achtlos herumliegende USB-Sticks angesteckt, dubiose Links angeklickt oder Anhänge zu eigenartig erscheinenden E-Mails geöffnet werden, oder wenn aus Bequemlichkeit Rechner während einer Kaffeepause oder sonstiger kurzer Abwesenheit nicht gesperrt werden.

Um aus Mitarbeitern eine „Human Firewall" zu bilden, können verschiedene Methoden der Bewusstseinsbildung eingesetzt werden, wie etwa klassisches Lernen mit einem Trainer und Zusammenkunft aller an einem Ort oder als E-Learning, das von Ort und Zeit unabhängig ist. Planspiele können die Lehrinhalte vertiefen.

Bei Gamifikation werden spielerische Elemente zum Transport von Lehrinhalten herangezogen. Es gibt Punkte und Belohnungen für herausragende Leistungen; man tritt in Interaktion mit anderen Teilnehmern und dem System. Die Bewältigung einer Aufgabe und das erhaltene positive Feedback sowie der gegenseitige Wettbewerb steigern die Motivation. Allerdings muss darauf geachtet werden, dass die Konkurrenzsituation nicht in tatsächlichen Streit ausartet und das Betriebsklima beeinträchtigt.

Bezahlen im Web. Univ.-Prof. Dr. Peter Mader, Universität Salzburg, berichtete über die Vor- und Nachteile einiger gängiger, im Netshopping verwendeter Bezahlverfahren. Bei dem am häufigsten angewendeten Verfahren, der Zahlung unter Angabe der Nummer der Kreditkarte und des Ablaufdatums, fordert der Leistungserbringer (Verkäufer) vom Kartenaussteller unter Abzug einer zuvor vereinbarten Vergütung jenen Betrag ein, für den der Karteninhaber dem Kartenaussteller die entsprechende Anweisung erteilt hat.

Nach Bezahlung hat der Aussteller einen Ersatzanspruch gegenüber dem Inhaber – wenn dieser tatsächlich die Anweisung erteilt hat. Bei einem Missbrauch der Kartendaten hat der Kartenaussteller dem Inhaber den abgebuchten Betrag wieder gutzuschreiben, sofern den Inhaber kein Verschulden an der missbräuchlichen Verwendung trifft bzw. ihm ein solches nicht nachgewiesen werden kann.

Das System ist von der Anwendung her einfach, bietet jedoch kaum Sicherheit vor Datenmissbrauch. Deshalb wird vielfach die Angabe des *Card Validation Codes (CVC)* verlangt, der

FOTO: KURT HICKISCH

auf der Kreditkarte nicht eingeprägt, sondern aufgedruckt ist und den Richtlinien nach nicht verarbeitet werden dürfte. Bei unsicheren Verbindungen oder Speicherung wird dieses Sicherheitsmerkmal nutzlos. Für den Verkäufer – der im Missbrauchsfall vom Kartenaussteller wieder rückbelastet wird – ist das Risiko insofern hoch, als er die Identität seines Kunden kaum nachprüfen kann und nicht einmal eine unterschriebene Anweisung vorliegt.

Beim System *Kreditkarte und PIN* ist eine unbefugte Verwendung zwar auch möglich, doch ist die rechtliche Situation für den Karteninhaber insofern anders, als ihm im Missbrauchsfall vorgeworfen werden kann, die PIN nicht geheim gehalten zu haben. Insofern besteht damit für den Verkäufer Zahlungssicherheit.

Bei *Maestro Secure-Code* wird nach erfolgter Registrierung beim E-Banking der eigenen Bank die Maestro-Bankomatkarte zum Bezahlen im Internet eingesetzt. Dem Verkäufer werden Kartennummer, Ablaufdatum und CVC angegeben. Über SMS wird ein sechsstelliger Secure-Code (Einmal-Passwort; mTAN) übermittelt, durch dessen Eingabe die Zahlung bestätigt wird.

Sofort Überweisung, ein aus Deutschland kommendes System, baut auf einem schon bestehenden Online-Banking-Account des Kunden auf. Dieser meldet sich – für den Shopbetreiber nicht einsehbar – mit allen Online-Banking-Zugangsdaten (einschließlich Benutzername und Passwort) auf der Webpage von Sofortüberweisung an. Das Unternehmen führt eine Kontodeckungsprüfung durch und gibt die Zahlung mittels TAN frei. Nach dem Zahlungsdienstegesetz (ZaDiG; BGBl I 2009/66, zuletzt BGBl I 2015/68) hat

Vorsicht vor Datendiebstahl: Computer sollten in einem Unternehmen nicht unbeaufsichtigt sein.

der Käufer in diesem Fall keine Rücktrittsmöglichkeit mehr, sodass für den Verkäufer Zahlungssicherheit gegeben ist. Problematisch ist, dass Zugangsdaten an einen Dritten weitergegeben werden.

Das Online-Zahlungsverfahren der österreichischen Banken, „eps“ *(e-payment standard),* wird ebenfalls über einen aktivierten Online-Banking-Zugang des Käufers abgewickelt. Über einen Link im Netshop stellt dieser die Verbindung zu seiner Bank her. In der ihm vertrauten Überweisungsmaske legitimiert er sich gegenüber dem System, nimmt die Zahlung vor und bestätigt sie durch Eingabe der TAN. Der Verkäufer erhält eine elektronische Bestätigung der Zahlung.

Wird vom Verkäufer die Zahlungsmöglichkeit per *Paybox* angeboten, wird dem Käufer, der bei *Paybox* registriert ist und diese Möglichkeit nutzen will, auf der Internet-Bestellseite eine Maske präsentiert, in die er seine Mobiltelefon-Nummer eingibt. Der Verkäufer sendet die Transaktion über eine gesicherte Datenleitung an *Paybox*. Von dort wird der Käufer unter der angegebenen Rufnummer zurückgerufen. Durch Eingabe der erhaltenen PIN wird der Kaufbetrag freigegeben, der vom Girokonto abgezogen und, unter Abzug eines Disagios, dem Verkäufer überwiesen wird. Im Prinzip sind bei diesem Verfahren nicht mehr als ein Girokonto und ein Handy erforderlich. Rechtlich gesehen, liegt allerdings lediglich eine Einzugsermächtigung vor, die widerrufen werden kann.

Bei *PayPal* hinterlegt der Kunde dort die Daten seiner Kreditkarten und/oder seines Bankkontos. Ohne diese Daten dem Verkäufer bekanntzugeben, wird auf dieser Grundlage der Zahlungsvorgang von *PayPal* durchgeführt. Für die Freigabe des Zahlungsbetrages sind lediglich Mail-Adresse und Passwort bzw. ein einer mTAN entsprechender „SMS-Sicherheitsschlüssel“ erforderlich. Es werden auch ein virtuelles Konto angeboten, das mit einem Guthaben aufgeladen werden kann sowie ein „Käuferschutz“.

„Alle Systeme haben Vor- und Nachteile“, sagte Mader. „Der Stein der Weisen ist für Zahlungen im Onlinehandel noch nicht gefunden.“ Online-Banking bietet gute Sicherheit vor Missbrauch. Das Risiko liegt durch das ZaDiG grundsätzlich beim Zahlungsdienstleister; das des Kunden ist eher gering.

Ass.-Prof Dr. Sonja Janisch (Universität Salzburg) wies in ihrem Vortrag über die gesetzlichen Regelungen für Fernabsatz- und Auswärtsgeschäfte (siehe „Öffentliche Sicherheit“, Nr. 3-4/15, Seite 91) insbesondere auf die Konsequenzen hin, die sich für den Verkäufer ergeben, der die vorgeschriebenen Informationspflichten über das Bestehen und die Modalitäten zur Ausübung des Rücktrittsrechts nicht einhält, nämlich Verlängerung der Rücktrittsfrist um zwölf Monate, Verlust des Anspruchs auf Ersatz für Wertverlust sowie auf eine anteilige Vergütung für eine erst teilweise erbrachte Dienstleistung. Bei vollständig erbrachter Dienstleistung verliert der Unternehmer seinen Anspruch auf das Honorar. Wurde über die Pflicht zur Tragung der Rücksendekosten nicht informiert, geht dieser Ersatzanspruch verloren.

Wolfgang Feiel von der *RTR-GmbH* berichtete über den Schutz der Netzwerke auf legislativer Ebene. Hiezu zählen der Vorschlag der EU über eine Richtlinie zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union (NIS-RL), das IT-Sicherheitsgesetz in Deutschland und, was etwa den Schutz kritischer Infrastruktur betrifft, das in Österreich in parlamentarischer Beratung stehende Polizeiliche Staatsschutzgesetz – PStSG (RV 763 BlgNR 25. GP), das am 1. Juli 2016 in Kraft treten soll. Auch Netz- und Dienstebetreiber müssen an der Umsetzung von Schutzmaßnahmen mitwirken, betonte Feiel.

Veranstalter des begleitend zur *IT Carinthia* abgehaltenen *12. Österreichischen IT-Sicherheitstages war* das Institut für Informatik, Forschungsgruppe Systemsicherheit *(www.syssec.at)* der Alpen-Adria-Universität Klagenfurt in Kooperation mit den *Kärntner Messen*. *Kurt Hickisch*