Achillesferse Internet

Bei der IT-Sicherheitsmesse it-sa 2016 in Nürnberg zeigten Experten die Notwendigkeit auf, das Sicherheitsbewusstsein für Informationstechnologie zu heben.

Das Netz ist die Achillesferse der Zukunft", sagte der EU-Kommissar für Digitale Wirtschaft und Gesellschaft, Günther Oettinger, am 18. Oktober 2016 in seiner über Video aus Brüssel übertragenen Grußbotschaft zur Eröffnung der *it-sa* 2016. Oettinger verwies darauf, dass Angriffe auf die digitale Infrastruktur eine Gesellschaft lahmlegen könnten. Die Hard- und Software zur Beseitigung dieser Schwächen seien vorhanden. Man müsse aber informieren und in Sicherheit investieren. Cybersecurity sei wichtig für den Marktauftritt von Unternehmen und die Grundlage für die digitale Gesellschaft von morgen.

Peter Batt, Leiter der IT-Abteilung im Bundesministerium des Innern, bezeichnete den Weg in die digitale Wissens- und Informationsgesellschaft als unumkehrbar. Die globale Vernetzung eröffne neue Horizonte und sei unverzichtbar. Dies setze aber Vertrauen in die Sicherheit der digitalen Welt voraus. Man werde sich keinen intelligenten Kühlschrank kaufen, wenn zu befürchten sei, dass er wegen eines Software-Fehlers abtaut, oder kein autonom fahrendes Auto, das mangelhaft programmiert ist. Sicherheit sei ein Bedürfnis, das erst dann als Wert wahrgenommen werde, wenn es fehle. Die digitale Verwundbarkeit gehe allerdings auch Hand in Hand mit Sorglosigkeit: „Mir-wird-schon-nichts-passieren-User", denen vom Anti-Bot-Zentrum mitgeteilt wird, dass ihre Rechner Teil eines Botnetzes sind, setzen den Rechner oft nicht neu

Sicherheitsmesse it-sa: 490 Aussteller aus 19 Ländern waren vertreten; es wurden über 10.000 Fachbesucher gezählt.

auf, weil ihnen das zu mühsam ist. Zwar habe der Staat auch im Internet eine Schutz- und Garantiefunktion, doch könne dem Einzelnen das Bewusstsein für Sicherheit nicht abgenommen werden. Das im Juli 2015 in Kraft getretene IT-Sicherheitsgesetz lege IT-Standards und Meldepflichten für Unternehmen der kritischen Infrastruktur fest. Die Umsetzung des Gesetzes durch Verordnungen sei für die Bereiche Energie, Wasser, Ernährung und IKT bereits erfolgt. Die übrigen Bereiche mit den Sektoren Transport, Verkehr, Gesundheit sowie Finanz- und Versicherungswesen würden folgen. Nach der zweijährigen Übergangsfrist werde Anfang 2019 die Anpassung an die Gesetzeslage abgeschlossen sein.

Arne Schönbohm, Präsident des *Bundesamtes für Sicherheit in der Informationstechnik (BSI),* bezeichnete die Cyber-Sicherheit als unverzichtbar für die Digitalisierung. Allerdings werde auch die Kriminalität digital. So würden Angriffe immer professioneller. Im Frühjahr 2016 seien in Deutschland 60 Krankenhäuser mit Ransomware erpresst worden. Dieser Trend nehme zu. Die Angriffe würden sich zunehmend gegen industrielle Produktionssysteme richten. Die IT-Sicherheitsexperten seien gefordert, die Probleme allgemein verständlich darzulegen, um die Anwender anzusprechen.

IT-Sicherheitsstudien.

Winfried Holz, Mitglied des *Bitkom*-Präsidiums, berichtete, dass nach einer Studie des *Bitkom* in den vergangenen zwölf Monaten 47 Prozent der Internet-Nutzer Erfahrungen mit Cybercrime gemacht hätten. Fast ebenso viele hätten einen finanziellen Schaden erlitten. Jeder fünfte Befragte sei bereits bei einem Geschäft im Internet betrogen worden. Jeder Achte berichtete, dass seine persönlichen Daten illegal verwendet wurden. Jeder vierte Smartphone-Nutzer war von einen Sicherheitsvorfall betroffen. Jeder Zehnte hatte sich einen Virus eingefangen. Bei drei Prozent wurde das Smartphone von Erpressern verschlüsselt. Die Folge sei laut Holz, dass drei Viertel der Internetnutzer aus Sicherheitsgründen auf bestimmte Aktivitäten wie Online-Banking, Teilnahme an sozialen Netzwerken oder Cloud-Computing verzichteten. Dadurch verbreiteten sich innovative Dienste langsamer, als dies ansonsten möglich wäre.

Nach einer weiteren Bitkom-Studie wurden in Deutschland in den vergangenen zwei Jahren 51 Prozent der Unternehmen Opfer von Datendiebstahl, Wirtschaftsspionage oder Sabotage. Bei den Industrieunternehmen waren es 69 Prozent. Am häufigsten betroffen waren der Maschinen- und Anlagenbau, gefolgt von Chemie und Pharma, Elektrotechnik und Automobilbau. Sicherheit sollte bereits während der Produktentwicklung berücksichtigt werden (Security by Design), forderte Holz. Auf neue Risiken müsse rasch reagiert werden, etwa mit schnellen Updates. Das Sicherheitsbewusstsein der Nutzer müsse durch die Wirtschaft, den Staat oder Verbände geschärft werden. Die Nutzer müssten ihren Teil insofern beitragen, indem sie sich bewusst mit Themen wie Spam-Mails, Absicherung von Smartphones oder Betrügereien im Internet auseinandersetzen.

Norbert Luckhardt, Chefredakteur der Zeitschrift *Kes,* gab einen Überblick über die Ergebnisse der *Kes*/*Microsoft*-Sicherheitsstudie, die auf die Befragung von 267 teilnehmenden Unternehmen zurückgeht und seit 1985 alle zwei Jahre durchgeführt wird. Malware,

FOTO: KURT HICKISCH

Arne Schönbohm: „Ransomware-Angriffe richten sich zunehmend gegen Krankenhäuser und industrielle Produktionssysteme."

Winfried Holz: „Drei Viertel der Internetnutzer verzichten aus Sicherheitsgründen auf Online-Banking oder Teilnahme an sozialen Netzen."

Max Schrems: „Bei Datenschutzverletzungen wird zu beweisen sein, dass Schutzmaßnahmen dem Stand der Technik entsprochen haben."

Christiane Bierekoven: „Die Pflicht zur Datensicherung muss durch Technik und Verfügbarkeit sichergestellt werden."

die hauptsächlich über E-Mail verbreitet wurde, wurde als größte Gefahr bezeichnet, wobei die Infektionen zur Hälfte auf mobile Endgeräte zurückgeführt wurden. Bei Großunternehmen wurden die Kosten pro Virus-/Wurm-Infektion mit durchschnittlich 41.000 Euro angegeben. Als größtes Hindernis bei der Verbesserung der Informationssicherheit wurde ein fehlendes Sicherheitsbewusstsein bei den Mitarbeitern angesehen. 35 Prozent der Unternehmen hatten allerdings nie Awareness-Schulungen durchgeführt. Wie angreifbar die digitale Welt nach wie vor ist, wurde bei den Live-Hackings vorgeführt. Sebastian Schreiber, Experte für Penetrationstests *(Syss GmbH, www.syss.de)*, füllte von seinem Laptop aus die WLAN-fähige Speicherkarte eines nicht vernetzten Fotoapparats mit Katzenbildern auf. Es hätten aber auch Bilder anderer Art hinauf- oder heruntergeladen werden können. Schreiber zeigte auch auf, dass erfolgreiche Angriffe auf verschlüsselte Funktastaturen möglich sind.

Informationssicherheit. Seit 2015 wird zur Heranbildung von Cyber-Cops Polizisten in Bayern die Möglichkeit geboten, im Fernstudium ein Informatik-Studium zu absolvieren, mit Abschluss BA und Master in IT-Forensik. Während der Studiendauer wird die Dienstverpflichtung herabgesetzt. Entsprechende Studiengänge bieten etwa die Friedrich-Alexander Universität Erlangen-Nürnberg (FAU) und die Hochschule Albstadt-Sigmaringen an *(www.digitale-forensik-studium.eu)*.

Um die Erhöhung der Cyber-Sicherheit in Deutschland bemühen sich Institutionen wie *Deutschland sicher im Netz e.V. (DsiN; www.dsin.de)*, die *Allianz für Cyber-Sicherheit (www.allianz-fuer-cybersicherheit.de)*, *Teletrust (www.teletrust.de)*, die Initiative Wirtschaftsschutz *(www.wirtschaftsschutz.info)* und seit 2012 der *Cyber-Sicherheitsrat Deutschland e.V. (www.cybersicherheitsrat.de)*.

Die Rechtsanwältin Dr. Christiane Bierekoven aus Nürnberg, hob bei der Darstellung der Rechtslage nach der DSGVO die Pflicht zur Pseudonymisierung und Verschlüsselung personenbezogener Daten als Mittel zur Gewährleistung eines hohen Schutzniveaus hervor. Es besteht eine spezielle Pflicht zur Datensicherung. Durch Technikgestaltung müssen Verfügbarkeit und Belastbarkeit sichergestellt werden.

Der österreichische Datenschutzaktivist Maximilian Schrems stellte dar, inwieweit mehr Datenschutz durch sichere IT-Strukturen zu erreichen ist. Bei Verletzungen des Schutzes personenbezogener Daten (Data Breach) wird zu beweisen sein, dass die getroffenen Maßnahmen dem Stand der Technik entsprochen haben und dem Risiko angemessen waren. Die Vorgänge und Maßnahmen sind zu dokumentieren.

Produkte. Firewalls und Antiviren-Software helfen nicht gegen Social-Enginee-

FOTOS: KURT HICKISCH, TELEKOM.DE

IT-SA

IT-Security-Messe

Seit 2009 findet jährlich Turnus die *it-sa* (IT-Security Area) im Messezentrum Nürnberg statt. Sie ist in Europa die führende IT-Security-Messe und eine der beiden größten dieser Art weltweit.

Bei der *it-sa* 2016 vom 18. bis 20. Oktober 2016 waren 490 (2015: 428) Aussteller aus 19 Ländern vertreten. Es wurden über 10.000 Fachbesucher (2015: 9.015) gezählt.

In drei offenen Foren wurden in viertelstündigem Abstand über 230 Vorträge zu Fragen der IT-Sicherheit, Bedrohungen und Branchenentwicklungen geboten. Die Vorträge können zum Großteil heruntergeladen bzw. als Videostream angesehen werden.

Einen Tag vor der Messe startete das viertägige Kongressprogramm *Congress@it-sa* mit 15 Vortragsreihen. Spezielle Ausstellungsthemen waren auf Sonderflächen zusammengefasst, wie *Identity- und Access-Management (IAM)* und Start-up-Unternehmen. Aussteller aus Israel und Frankreich waren jeweils in Länderpavillons vertreten.

Die nächste it-sa wird auf zwei Hallen erweitert und vom 10. bis 12. Oktober 2017 wieder im Messezentrum Nürnberg stattfinden.

www.it-sa.de

Peter Batt: „Der Staat hat zwar Schutzfunktionen, er kann dem Einzelnen das Bewusstsein für Cyber-Sicherheit aber nicht abnehmen.“

ring-Angriffe wie dem CEO-Betrug (siehe „Öffentliche Sicherheit“, Nr. 5-6/16). Mit unverdächtig erscheinenden Mails wird deren zuvor ausgekundschafteter Empfänger veranlasst, Geldbeträge zu überweisen, ohne dass Schadprogramme implementiert werden. *Proofpoint (www.proofpoint.com/de)* hat eine Lösung entwickelt, einlangende Mails inhaltlich nach Mustern zu analysieren und Überprüfungen durchzuführen, die den Grad der Wahrscheinlichkeit eines Betruges anzeigen.

LightCyber (www.lightcyber.com) beobachtet den Netzwerkverkehr eines Unternehmens und erkennt anhand von Abweichungen vom statistischen Kommunikationsverhalten gezielte Angriffe. Ebenso kann die interne Verbreitung individueller Malware erkannt werden.

Die *Threat-Intelligence-Platform (TIP) ThreatConnect (www.threatconnect.com)* sammelt und analysiert Informationen über Angreifer, ihre Tools und Techniken. Diese Informationen werden den Anwendern zur Verfügung gestellt und ermöglichen ihnen, bereits im Voraus Abwehrmaßnahmen zu treffen.

Awarity (www.awarity.at) bietet Lernprogramme zur Hebung des Sicherheitsbewusstseins von Mitarbeitern an. Die Inhalte werden unter anderem mit spieltypischen Elementen wie Bonus-Punkten vermittelt (Gamifikation). „Mit dem Auftreten von Krypto-Trojanern wie Locky, die Daten verschlüsseln und erst nach Zahlung eines Lösegeldes wieder freigeben, ist die Nachfrage nach Cyber-Versicherungen stark angestiegen“, berichtete Dirk Kalinowski von der *AXA Versicherung AG*. Bei Schadenshöhen, die in die Millionen gehen können, wächst die Verantwortung der Geschäftsführung wegen mangelnder Risikovorsorge. Ein IT-Risiko-Check wird unter *www.axa.de/cyber-versicherung* angeboten. Als wichtig wurde eine Versicherung gegen Betriebsunterbrechung bezeichnet, wenn also kein direkter Schaden eingetreten ist, aber beispielsweise aus dem Lager durch IT-Ausfall nicht mehr geliefert werden kann. Mit dem als Neuheit vorgestellten *Clouditor* des *Fraunhofer-Instituts für angewandte und integrierte Sicherheit (AISEC; www.aisec.fraunhofer.de)* kann überprüft werden, ob in der Cloud abgelegte Daten tatsächlich der Dienstleistungsvereinbarung (Service-Level-Agreement; SLA) entsprechend verarbeitet werden, beispielsweise auch vom geografischen Ort her.

Das *Fraunhofer Institut für Sichere Informationstechnologie* bietet mit dem Projekt *Volksverschlüsselung (www.volksverschluesselung.de)* eine kostenlose Ende-zu-Ende-Verschlüsselung von E-Mails und Daten an. Durch hohe Benutzerfreundlichkeit soll Sicherheit durch Verschlüsselung für alle so selbstverständlich werden „wie das Anlegen des Sicherheitsgurts im Auto“. *Kurt Hickisch*

FOTO: KURT HICKISCH