Sicherheit als Basis der IT

Cybersecurity, Daten- und Netzwerksicherheit: Wie wichtig die Sicherheit für die Entwicklung der Informationstechnik ist, wurde bei der it-sa im Oktober 2017 in Nürnberg deutlich.

Hat man früher bei einem Auto als Motor mit Rädern gesprochen, muss man jetzt von einem Hochleistungszentrum für Kommunikation auf Rädern reden“, sagte *Bitkom*-Präsidiumsmitglied Winfried Holz bei der Eröffnungspressekonferenz der *it-sa,* die vom 10. bis 12. Oktober 2017 im Messezentrum Nürnberg stattgefunden hat. Holz bezog sich auf die einige Wochen zuvor in Frankfurt abgehaltene Automobilmesse, bei der autonom fahrende Fahrzeuge vorgestellt wurden. Allerdings wird niemand ein solches Fahrzeug benützen, wenn er sich nicht auf dessen sicheren Betrieb verlassen kann. Und dieser wiederum ist von der Sicherheit, der Verfügbarkeit und Integrität der dahinterstehenden Informationstechnologie abhängig.

Bei einer Befragung von *Bitkom (www.bitkom.org)* von 1.000 Internet-Usern bezeichneten nur fünf Prozent der Befragten das Internet als „sehr sicher“. Nicht nur Hacker bedrohen das Netz, sondern auch Cyber-Kriminelle und Nachrichtendienste.

Nach einer Untersuchung des *Bitkoms* und des *Bundesamts für Verfassungsschutz (BfV)* entsteht der deutschen Wirtschaft durch digitale Angriffe ein jährlicher Schaden von 55 Milliarden Euro. Klein- und Mittelbetriebe sind überdurchschnittlich oft betroffen. 70 % der Angriffe betreffen Kundendaten, 41 % Kommunikationsdaten, 36 % Finanzdaten, 11 % Patente und 10 % Daten über Mitarbeiter.

IT-Sicherheitsmesse: Sebastian Schreiber, *Syss GmbH,* zeigte ein Gerät zum Abhören von Funktastaturen.

Über Passwörter, Firewalls und Antivirenschutzprogramme hinaus ist anspruchsvolle IT-Sicherheitstechnik eher selten anzutreffen. Auch in organisatorischer Hinsicht besteht laut *Bitkom* Nachholbedarf, insbesondere bei der Personalauswahl und bei Sicherheitschecks der Mitarbeiter.

Im Hinblick auf die ab 25. Mai 2018 geltende DSGVO sei noch viel zu tun, mahnte Holz. Erst 13 % der Unternehmen hätten entsprechende Maßnahmen umgesetzt.

Neben dem *Bitkom* ist das *Bundesamt für Sicherheit in der Informationstechnik (BSI; www.bsi.bund.de)* der zweite ideelle Träger der *it-sa*. *BSI*-Präsident Arne Schönbohm wies darauf hin, dass das Grundschutzhandbuch komplett überarbeitet und Bausteine insbesondere für KMUs als Leitfaden für eine Basis-Absicherung entwickelt worden seien.

Der 2012 gegründeten *Allianz für Cyber-Sicherheit mit der Wirtschaft* haben zum Zeitpunkt der *it-sa* 2.500 Unternehmen angehört und täglich würden es um 15 mehr.

Einem „Need-to-know“ stellte Schönbohm ein „Need-to-share“ gegenüber. Erkenntnisse, die bei der Abwehr von Cyber-Angriffen gewonnen werden, sollen allen Mitgliedern der Allianz zugute kommen. Durch die Zertifizierung von IT-Produkten wird in diese Wertschöpfung integriert.

Das *BSI* wird um weitere 180 auf 840 Mitarbeiter erweitert und ist damit nach den Worten Schönböhms die mit Abstand größte Organisation dieser Art in Europa. Mit der Kampagne „Wir wollen deine digitale Seite“ werden Interessenten für offene Stellen gesucht.

Dr. Steve Purser, Head of Core Operations Department der *ENISA,* gab einen Ausblick auf Sicherheitsanforderungen im Internet der Dinge.

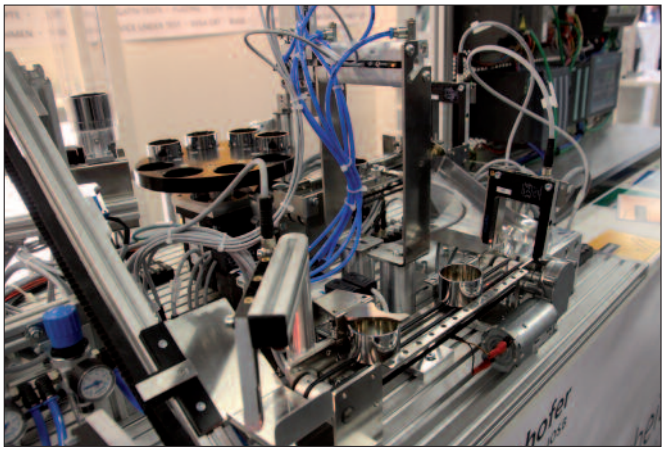
Angriffe. Beim *Congress@it-sa* machte Stefan Strobel, *Cirosec GmbH (www.cirosec.de)* an Beispielen deutlich, wie angreifbar das Internet der Dinge ist. Wer die Zugangsdaten einer günstig angebotenen IP-Kamera abfangen könne, sei in der Lage, in das gesamte Heimnetz des Anwenders zu gelangen. Angreifbar sei auch die Video-Glocke bei der Haustür, über die man über das Handy mit dem Besucher sprechen könne. Durch das Lösen zweier von außen zugänglicher Schrauben könnte das Gerät ausgelesen und in das private Netz eingedrungen werden. Über das Handy dynamisch steuerbare Stimmungslichter könnten von außen abgeschaltet werden.

Eine Spielzeugpuppe, die einem Kind auf Fragen Antworten gibt, leitet die über Mikrofon aufgenommene Sprache des Kindes über WLAN in die Cloud weiter, wo sie über Spracherkennungssysteme logisch ausgewertet wird. Passende Antworten werden an die Puppe rückgesendet und von dieser wiedergegeben. Die Rechenkapazität der Puppe reicht dafür nicht aus. Das Mikrofon nimmt auch alle anderen Gespräche im Raum auf und sendet sie in die Cloud. Zu wenig Intelligenz im Schlüssel kann ein elektronisches Schloss, das per Smartphone über eine App gesteuert wird, angreifbar machen. Die Entscheidungen werden in der Cloud getroffen, wo der geheime Schlüssel ausgelesen werden kann.

Schon um zwei Euro könne man Geräte internetfähig und damit „smart“ machen, betonte Strobel. Die Sicherheit bleibt auf der Strecke. Es besteht der Zwang, schnell und billig am Markt zu sein. Höhere

FOTO: KURT HICKISCH

IT-SA 2017 in Nürnberg: Stand des Bundesamts für Sicherheit in der Informationstechnik.



Industrieanlagen sind zunehmend an das Internet gebunden, miteinander vernetzt und damit angreifbar.

Sicherheit erfordert stärkere Chips, die nicht nur teurer sind, sondern auch mehr Strom verbrauchen und mehr Wärme erzeugen. Die Verletzlichkeit der IT-Sicherheit wurde auch in Live-Hackings demonstriert. Sebastian Schreiber, *Syss GmbH (www.syss.de),* zeigte vor, dass mit einem um 18 Dollar erhältlichen Gerät („Crazy Radio“) Funktastaturen abgehört und somit auch Passwörter mitgelesen werden können. Damit wäre der Weg zur Installation von Malware offen. Über eine Funkarmbanduhr kann eine Funkalarmanlage deaktiviert werden, einschließlich des Panik-Buttons. Geräte, die Funktechnologie verwenden, sind zwar klein und handlich, aber es schlummern Gefahren in ihnen.

„Bei Funktechnologie ist Vorsicht geboten“, betonte Schreiber. Mit einem WLAN-Jammer um 50 Dollar können bestimmte oder alle derartigen Netze im Umkreis gestört und damit funktionsunfähig gemacht werden.

Produkte. Zur schnellen Analyse von Anomalien stellt *IBM* mit *QRadar Advisor with Watson* die künstliche Intelligenz von *Watson* zur Verfügung. Damit kann innerhalb weniger Minuten auf die Gesamtmenge an sicherheitsrelevanten Informationen inclusive Forschungsergebnissen zurückgegriffen werden.

Proofpoint (www.proofpoint.com) bietet cloudbasierte Tools zum Erkennen und Blockieren schädlicher Anhänge von E-Mails an. Verdächtige, aber bisher noch unbekannte Anhänge kommen in eine Sandbox und werden dort analysiert. Das Unternehmen hat auch Lösungen entwickelt, um CEO-Fraud zu unterbinden.

Sicherheitslösungen für E-Mails werden auch von *GBS (www.gbs.com)* angeboten. Selbstlernende Textanalysen erkennen vertrauliche Inhalte von Mails und Anhängen noch vor dem Versand und stoppen diesen.

Für Klein- und Mittelbetriebe gedacht ist *Vulcom* von *Hackner Security Intelligence (www.hackner-security.com)*. Das Programm führt regelmäßig Schwachstellen-Scans durch und zeigt die Ergebnisse an. Bei erkannten Schwachstellen werden in verständlicher Form die zugehörigen Risiken beschrieben, kategorisiert und Empfehlungen zur Behebung gegeben. Bei neu identifizierten Risiken erfolgt eine Alarmierung.

Sind die üblichen Sicherheitsbarrieren bereits überwunden, stellt *Cyber-Trap (www.cybertrap.com)* dem Angreifer über Köder eine Falle, in der Informationen über den Angreifer gesammelt werden. Dieser erhält falsche Informationen.

Forcepoint Insider Threat (www.forcepoint.com) analysiert automatisiert Aktivitäten auf den Computern von Nutzern. Erreichen Anomalien im Benutzerverhalten ein bestimmtes Niveau, wird auf den Mitarbeiter aufmerksam gemacht. Mit diesem Hintergrund kann dann eine weitere personenbezogene Kontrolle begründet werden.

Die letzte Verteidigungslinie gegenüber Cyber-Angriffen, zugleich das schwächste Glied ist der Mitarbeiter. Vor allem über Phishing dringen Angreifer in Netze ein. Um diese Art von Angriffen erkennen zu können, bietet *PhishMe (www.phisme.com)* Schulungsprogramme an, in denen Angriffszenarien wie Spear-Phishing, Social Engineering, Anhänge von E-Mails mit Schad-Software, Drive-by-Infektionen, simuliert werden können, wobei eine Anpassung der Programme an die firmeninterne Situation erfolgen kann. Über eine Hotline können die Nutzer ihnen verdächtig erscheinende E-Mails an ein Sicherheitsteam weiterleiten, das die weitere Überprüfung vornimmt.

Wissen vermitteln und Verhalten schulen, steht bei den von *Kaspersky (www.kaspersky.de)* entwickelten interaktiven Schulungsprogrammen im Vordergrund. Lernen erfolgt spielerisch, indem Teams bei der Bewältigung simulierter IT-Gefahrensituationen gegeneinander antreten.

Die Spiele sind auf die jeweiligen Ebenen der Unternehmenshierarchie zugeschnitten – für die Geschäftsleitung Simulation der Auswirkungen eines Cyber-Angriffs, für Bereichsleiter Managementspiele und für die Mitarbeiter interaktive Schulungen unter anderem mit simulierten Phishing-Angriffen.

Beim Auslagern von Daten in die Cloud, etwa bei Nutzung von cloudbasierter Software (SaaS), können sich datenschutzrechtliche Probleme ergeben. Der physische Standort der Server ist ja kaum bekannt. Eine Abhilfe bietet, die Daten verschlüsselt in der Cloud abzulegen.

Lösungen hierzu bieten *Eperi (www.eperi.com), Owncloud (www.owncloud.com)* und das Start-Up-Unternehmen *Lucky-Cloud (www.luckycloud.de),* das in Open-Source-Programmierung sogar die Verbindung in die Cloud offen legt.

IT-Forensik, speziell zur Aufklärung wirtschaftskrimineller Handlungen im IT-Umfeld, bietet das Bera-

Fotos: Kurt Hickisch

Stefan Strobel: „Wer die Zugangsdaten einer IP-Kamera abfangen kann, kann in das gesamte Heimnetz des Anwenders gelangen."

Daniel Domscheit-Berg: „Neuronale Chips werden Gedächtnisleistung übernehmen und selbstlernend Kreativität entwickeln."

Arne Schönbohm: „Erkenntnisse bei der Abwehr von Cyber-Angriffen sollen Mitgliedern der Allianz für Cyber-Sicherheit zugute kommen."

Winfried Holz: „Der deutschen Wirtschaft entsteht durch digitale Angriffe ein jährlicher Schaden von 55 Milliarden Euro."

tungsunternehmen *Warth & Klein Grant Thorton AG (www.wkgt.com) an*.

Das 2004 gegründete gemeinnützige Unternehmen Arbeit für Menschen mit Behinderung *(AfB; www.afb-group.eu)* sammelt nicht mehr gebrauchte IT- und Mobilgeräte ein und überprüft sie auf weitere Verwendungsfähigkeit. Nicht mehr verwendungsfähige Geräte werden geschreddert und dem Rohstoffmarkt zugeführt. Auf Geräten oder Einzelkomponenten, die noch vermarktet werden können, werden alle noch vorhandenen Daten zertifiziert gelöscht und die Geräte werden verkauft.

Zukunft. In seiner Keynote („Blick über den Tellerrand") verglich der Netzaktivist und ehemalige *Wiki-Leaks*-Sprecher Daniel Domscheit-Berg das Internet in seiner gesellschaftlichen Bedeutung mit der Erfindung des Buchdrucks. Durch diesen sei das Wissen aus der Herrschaft weniger Privilegierter befreit worden.

Durch das Internet stünde dem Einzelnen heute fast das gesamte Wissen der Menschheit zur Verfügung. Ähnlich, wie sich damals der Mensch als Individuum erkannt habe, geschehe das heute über die sozialen Medien. Menschen stellten sich dar; ihre Autobiografien ließen sich über soziale Medien nachlesen. Alle seien überall erreichbar, und es sei die Frage, wie diese Zukunft gestaltet werden solle. Es werde eine Herausforderung sein, das Internet der Dinge so zu gestalten, dass daraus Sinnstiftendes entsteht, und es müsse sichergestellt werden, dass die Menschen damit umgehen können.

Grundlegende Veränderungen werden sich im Verkehrs- und Transportwesen ergeben, betonte Domscheit-Berg. In den Städten wird der Verkehr über sich autonom bewegende Fahrzeuge abgewickelt. Transportleistung wird gefragt sein, das Eigentum am Transportmittel werde nebensächlich.

Der Bestand an Fahrzeugen könnte sich bis auf zehn Prozent des derzeitigen Werts verringern. Dadurch freigewordene Flächen könnten neu erschlossen werden. Senkrecht startende und landende, autonom fliegende Drohnen werden als Taxis Menschen befördern. Bei der Weltausstellung 2020 in Dubai werden solche Taxis als Transportmittel eingesetzt werden.

Nicht nur Fahrzeuge, sondern auch Häuser und deren Inneneinrichtung werden im 3D-Druck gebaut werden, und alte Häuser recycelt. Im Moleküldrucker werden Moleküle jeglicher Art zusammengesetzt und im Bio-Printing-Verfahren Körperteile wie Nasen oder Ohren hergestellt werden. Künstliche Herzen aus dem 3D-Drucker könnte es in zehn Jahren geben.

Neuronale Chips wie A11 von *Apple* oder *TrueNorth* von *IBM,* letzterer mit einer Million Neuronen und 256 Millionen Synapsen, würden Gedächtnisleistung übernehmen und selbstlernend Kreativität entwickeln. Nach einer Studie des Weltwirtschaftsforums würden zwei Drittel der Berufe, die ein heutiger Grundschüler später ergreifen kann, derzeit noch nicht existieren. Domscheit-Berg: „Schließt sich im Berufsleben für den Einzelnen eine Tür, gehen dafür fünf andere auf."

Kurt Hickisch

IT-SA

Europas führende IT-Sicherheitsmesse

Die IT-Sicherheitsmesse *it-sa* vom 10. bis zum 12. Oktober 2017 im Messezentrum Nürnberg wurde zum neunten Mal abgehalten – mit wesentlich größerer Ausstellungsfläche. Die Messe gilt als die führende Veranstaltung ihrer Art in Europa und als eine der wichtigsten Fachmessen zur IT-Sicherheit weltweit.

Es gab 630 Aussteller (2016: 489) aus 24 Ländern und 12.780 Besucher (2016: 10.182). Auf der Sonderfläche *Startups@it-sa* präsentierten sich junge Unternehmen und auf dem *Campus@it-sa* akademische Bildungseinrichtungen.

Auf vier Foren, je zwei für Technik und Management, wurden im Viertelstundentakt insgesamt 320 frei zugängliche Vorträge abgehalten. Die meisten davon können als Video und/oder PDFf-Dokument auf der Website der Messe abgerufen werden. Im *Congress@it-sa* wurden 14 Vortragsreihen veranstaltet.

Die nächste *it-sa* wird vom 9. bis 11. Oktober 2018 wiederum im Messezentrum Nürnberg stattfinden. *www.it-sa.de*

FOTOS: KURT HICKISCH