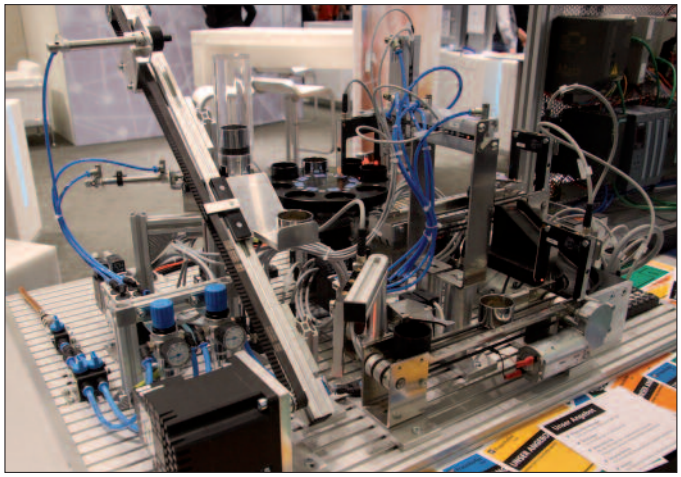

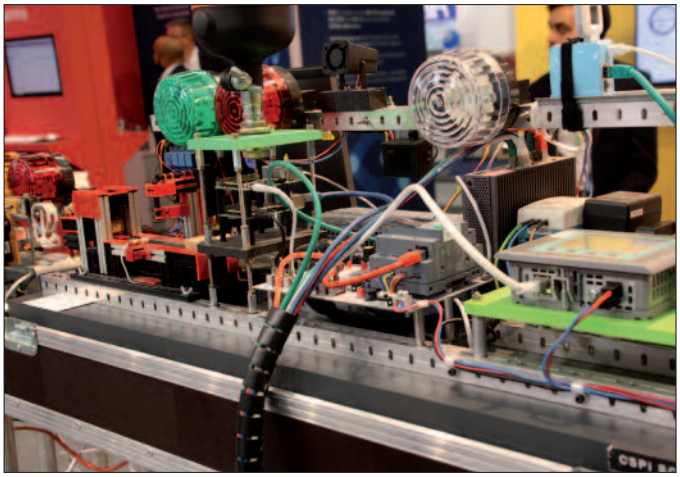

Innovationen auf der IT-Sicherheitsmesse it-sa 2018 in Nürnberg: SCADA-Modelle.

Neuheiten und Gefahren

Bei der IT-Sicherheitsmesse it-sa in Nürnberg wurden Neuheiten in der digitalen Welt präsentiert und es wurde auf aktuelle Gefahren für die IT-Sicherheit eingegangen.

Die Gefährdung der Cyber-Sicherheit ist in Deutschland nach wie vor hoch; Cyber-Sicherheit ist Chefsache in der Bundesregierung“, sagte Andreas Könen, Leiter der Abteilung Cyber- und Informationssicherheit im Bundesministerium des Innern, für Bau und Heimat, am 9. Oktober 2018 bei der it-sa in Nürnberg.

Mit dem IT-Sicherheitsgesetz sei ein nationaler Rechtsrahmen für die IT-Sicherheit von Unternehmen der kritischen Infrastruktur geschaffen worden, doch „was heute gut ist, ist keine Garantie für morgen“. Derzeit stehe die Versorgungssicherheit im Vordergrund. In einem künftigen IT-Sicherheitsgesetz 2.0 würden IT-Mindeststandards und Meldepflichten auch für jene Unternehmen festgelegt, deren Ausfall nicht unmittelbar zu Versorgungskrisen führe, wie etwa für die produzierende Großindustrie und die Zulieferer für Unternehmen der kritischen Infrastruktur. Zur Herstellung einer digitalen Souveränität würden gemeinsam mit der Wirtschaft Schlüssel-Technologien in jenen Bereichen gefördert, in denen man in hohem Maße vom Ausland abhängig sei.

Als weiterer Meilenstein sei daran gedacht, zum Schutz der Konsumenten, aber auch zur Erhöhung der IT-Sicherheit allgemein, ein IT-Sicherheits-Kennzeichen zu entwickeln. Zunächst auf freiwilliger Basis durch die Hersteller, soll dieses Gütesiegel ein Kriterium für die Kaufentscheidung werden sowie eine Abgrenzung im Markt erzeugen. Letztlich werde an eine flächendeckende europäische Lösung gedacht.

Zumeist durch Cyber-Angriffe sei der deutschen Industrie in den vergangenen zwei Jahren ein Schaden von 55 Milliarden Euro entstanden, sagte Susanne Dehmel, Mitglied der Geschäftsleitung *Recht & Sicherheit, BITKOM e.V.* Die Angriffe werden professioneller und würden vor allem Mittelständler treffen, da sich Großkonzerne besser schützen könnten. Der Präsident des *Bundesamtes für Sicherheit in der Informationstechnik (BSI),* Arne Schönbohm, forderte, „IT-Sicherheit made in Germany“ müsse zu einem Markenbegriff werden. Er wies auf die Leistungen des BSI als Zentralstelle für Standardisierung und Zertifizierung und die Zusammenarbeit mit den Betreibern kritischer Infrastruktur hin. Das BSI mit seinen derzeit 940 Mitarbeitern leiste auch Forschungsarbeit bei der Entwicklung des 5G-Netzes und im Bereich des Quanten-Computings. Die Verschlüsselung von Nachrichten müsse in die Fläche gebracht werden. Maschinelles Lernen (künstliche Intelligenz) werde eingesetzt, um die Cyber-Sicherheit zu erhöhen.

In Bayern wurde am 1. Dezember 2017 das *Landesamt für Sicherheit in der Informationstechnik (www.lsi.bayern.de)* mit Sitz in Nürnberg errichtet, das, wie auch das BSI, mit einem Informationsstand auf der Messe vertreten war. Bayern ist das erste deutsche Bundesland mit einer derartigen Einrichtung, die vom Präsidenten dieser Behörde, Daniel Kleffel, vorgestellt wurde. Ziel

IT-SICHERHEITSFACHMESSE

14.290 Besucher

Auf der weltgrößten IT-Sicherheitsfachmesse it-sa vom 9. bis 11. Oktober 2018 in Nürnberg waren 696 (2017: 630) Aussteller aus 27 (24) Ländern vertreten. Die Ausstellungsfläche wurde um 20 Prozent vergrößert. Die Zahl der Fachbesucher erhöhte sich auf 14.290 (2017: 12.780) aus über 50 Nationen (44). Beim messebegleiteten *Congress@it-sa* gab es in den 20 Veranstaltungen vertiefte Informationen. In fünf offenen Foren wurden während der gesamten Messedauer etwa 350 Vorträge zu Sicherheitsthemen sowie Live-Hackings geboten. Von den meisten Vorträgen in den Foren sind die Folien der Präsentationen im Internet abrufbar sowie Video-Streams *(www.it-sa.de/programm)*. Die nächste *it-sa* wird vom 8. bis 10. Oktober 2019 wieder im Messezentrum Nürnberg stattfinden.

www.it-sa.de

Fotos: Kurt Hickisch

Kongress zur it-sa 2108 mit 350 Vorträgen über Sicherheitsthemen: Referenten Daniel Kleffel, Arne Schönbohm, Udo Schneider, Horst Görtz, Andreas Könen und Burkhard Even.

ist der Schutz der staatlichen IT-Infrastruktur (Abteilung 1, Cyber-Sicherheit Technik). Im Bereich der Abteilung 2 (Sicherheitsberatung) soll der bayerischen Staatsverwaltung, öffentlichen Unternehmen und den 2.056 Gemeinden in Bayern, die mit unterschiedlichsten IT-Rahmenbedingungen arbeiten, auf bewährten Grundlagen wie der ISO 27001 und dem IT-Grundschutz des BSI ein *Informationssicherheits-Management-System (ISMS)* zur Hand gegeben werden. In den BayernLabs sollen Bürger, Schulen, Kommunen und Wirtschaft zu Fragen der IT-Sicherheit beraten werden. Bis Ende 2020 wird der Personalstand des LSI auf rund 200 Mitarbeiter steigen.

Cybercrime. Dr. Burkhard Even vom *Bundesamt für Verfassungsschutz (BfV)* wies auf die Gefahr durch Wirtschaftsspionage hin, die „nur einen Mausklick von der Wirtschaftssabotage entfernt sei". Cyber-Angriffe seien kostengünstig, hätten eine hohe Erfolgswahrscheinlichkeit, könnten vielfältig verschleiert werden und müssten keine Landesgrenzen überwinden. Zwei Drittel der Fälle von Datendiebstahl seien auf Innentäter zurückzuführen, die entweder ahnungslos oder unachtsam seien, aus Neugierde oder vorsätzlich handeln würden. Die „menschliche Firewall" versage in diesen Fällen, nicht zuletzt durch Lücken in der Schulung der Mitarbeiter. Wirtschaftsspionage koste Geld, Arbeitsplätze, Reputation und bedeute den Verlust von Know-how. Dahinter stünden auch wirtschaftsstrategische und -politische Interessen. Das europäische Stromnetz mit seinen Kraftwerken und Leitungen sowie die Infrastruktur stünden im Fokus von Cyber-Sabotage.

Einen Überblick über die Bedrohungs- und IT-Sicherheitslage in Europa gab Wolfgang Gröller von *RadarServices (www.radarservices.com)*. Das Unternehmen mit Sitz in Wien hat mit dem *Global Risk Score* für Groß- und Mittelstandsunternehmen in Europa ein Verfahren zur Klassifizierung von Cyber-Risiken entwickelt. Die Messzahlen liegen zwischen 0 (geringes Risiko) und 10 (sehr hohes Risiko) und werden errechnet aus dem Verhältnis von neu erkannten und geschlossenen Incidents, der ermittelten Schwachstellen und der Dauer der Fehlerbehebung. Je länger diese dauert, umso schlechter wird der Score. Dadurch können Maßnahmen evaluiert und Vergleiche zu anderen Unternehmen gezogen werden.

Besonders gefährdet erscheinen Industrieunternehmen, am wenigstens der Handel. „Die Zeit der Skript-Kiddys ist vorbei, man will Geld verdienen", begründete Wolfgang Gröller den Trend zu erpresserischen Cyber-Angriffen auf die Industrie, deren Systeme zudem mehr Schwachstellen aufweisen. Das Unternehmen betreibt nach eigenen Angaben das größte Cyber-Defence-Center in Europa. Künstliche Intelligenz werde nach einer Studie des Unternehmens für die IT-Sicherheit zunehmend einsatzfähiger werden, was bei der Zuweisung von Ressourcen eingeplant werden sollte.

Florian Kellermann von *F-Secure* zeigte am Beispiel von *Alexa* auf, dass künstliche Intelligenz alltagstauglich geworden ist. Über *Alexa* können Geräte durch Sprachbefehle gesteuert werden. Die Spracherkennung erfolgt in der Cloud und beruht auf maschinellem Lernen. Diese Technik kann zum Komponieren von Musikstücken eingesetzt werden *(www.aiva.ai)* oder um in Fotos oder Videos die Gesichter gegen die anderer Personen auszutauschen *(Deepfake)*. Der humanoide, einer Frauengestalt nachgebildete Roboter *Sophia,* hinter dem ein großer Cloud-Cluster steht, ist der weltweit erste Roboter, dem eine Staatsbürgerschaft – die von Saudi-Arabien – verliehen wurde. Künstliche Intelligenz kann eingesetzt werden, Angriffe im Netz zu erkennen, indem das „Grundrauschen" im Netz unterdrückt wird.

Sicherheitspreis. Bereits zum siebenten Mal, aber erstmalig auf der *it-sa,* wurde der mit 200.000 Euro dotierte deutsche Sicherheitspreis der *Horst-Görtz-Stiftung* verliehen. Der erste Preis ging an eine Forschergruppe, die ein mittlerweile patentiertes Verfahren entwickelte, die Integrität der Hardware eines Computers über die Ermittlung eines Hashwertes sicherzustellen. Veränderungen an der Hardware führen zu einer Änderung des Hashwertes – dem Computer kann dann in seiner Physikalität nicht mehr vertraut werden. Die Sicherheit der Hardware ist vor allem für Unternehmen der kritischen Infrastruktur von Bedeutung. Bisher konnte sie nur in kleinem Ausmaß, etwa bei Smart-Cards, gewährleistet werden.

CEO-Betrug. Durch CEO-Fraud sei laut FBI weltweit ein Schaden von 12 Milliarden US-Dollar entstanden, mit einer durchschnittlichen Schadenssumme von 159.000 Dollar pro Fall, sagte Udo Schneider von *Trend-Micro (www.trendmicro.com)*. Bei dieser auch als *Business E-Mail Compromise (BEC)* bezeichneten Betrugsart werden Mitarbeiter eines Unternehmens durch gut gefälschte E-Mails dazu gebracht, hohe Geldbeträge an ausländische Bankverbindungen zu überweisen. Die Mails stammen angeblich von einem hochrangigen Mitglied der Unternehmensführung. Die Überweisungen werden als sehr dringlich und absoluter Geheimhaltung unterliegend bezeich-

FOTOS: KURT HICKISCH

Preisträger des Deutschen IT-Sicherheitspreises 2018 der Horst-Görtz-Stiftung.

IT-Sicherheitsmesse it-sa: 700 Aussteller aus 27 Ländern präsentierten Sicherheitsprodukte und -dienstleistungen.

net, wodurch psychologischer Druck aufgebaut wird. Den Angriffen gehen umfangreiche Erhebungen über Firmeninterna voraus. Die Täter schöpfen aus offenen Quellen (Firmenbuch, Handelsregister, Geschäftsberichte), sozialen Medien wie LinkedIn oder XING, Informationen über die Zielpersonen und „ernten" E-Mails ab, um sich Kenntnis über den Aufbau und das Format der Firmen-Mails zu verschaffen (*siehe auch „Öffentliche Sicherheit", Nr. 5-6/16, S. 6-8)*.

Wie in diesem Zusammenhang auch aus anderen Vorträgen von Firmen, etwa von *Retarus (www.retarus.com),* hervorging, wird zunehmend bei Mails zur Täuschung des Empfängers der Name des Absenders so manipuliert, dass bei flüchtigem Lesen sein Name vertraut erscheint. Es werden in seiner tatsächlichen Mail-Adresse ähnlich oder gleich aussehende Schriftzeichen (Homoglyphen) verwendet, wodurch vom Schriftbild her Abweichungen schwer erkennbar sind. So wird rn leicht mit m verwechselt, vv mit w, O mit 0, oder I(da) mit l(kleines L) oder Í. Bei der Verwendung verschiedener Alphabete (kyrillische Schrift) wird die Verwechslungsgefahr noch größer.

Abgesehen von firmenspezifischen Schutzprogrammen, bietet Schutz, Nachrichten zu signieren und zu verschlüsseln. Letztlich kommt der „menschliche Faktor" zum Tragen, nämlich verdächtig erscheinende Nachrichten zu prüfen und zu hinterfragen.

Fehlende Verschlüsselung von E-Mails könnte Folgen nach den Artikeln 32 bis 34 DSGVO nach sich ziehen, wovor ein Vertreter der auf den Schutz elektronischer Kommunikation spezialisierten *Totemo AG (www.totemo.com)* warnte.

Produkte. Nicht nur nach Spoof-Domains, sondern überhaupt nach verschwundenen (geleakten) Daten sucht die *Digital Shadows GmbH (www.digitalshadows.com),* und ist dabei spezialisiert auf das Darknet. „Darknet ist ein Internet ohne Google", meinte Stefan Bange, Vertriebsleiter in Deutschland des in England und den USA etablierten Unternehmens. „Man braucht Fachwissen, um sich dort bewegen zu können und sich auszukennen." Gesucht wird nach Schlüsselwörtern (Namen, Adressen, Marken- und Produktnamen), nach gefälschten Social-Media-Zugangsdaten, Tweets oder Links, die für Social-Engineering verwendet werden. Auf ungesicherten Servern wurden 1,5 Milliarden Dokumente gefunden. Das Unternehmen wird laut Bange auch von Staatsanwaltschaften und Ermittlungsbehörden beauftragt.

Die IT-Sicherheit der Steuerungssysteme von Industrieanlagen hinkt der Entwicklung in der übrigen IT-Welt nach. ICS- und SCADA-Systeme werden bei der langen Lebensdauer der Anlagen oft mit veralteter Software betrieben. Updates sind bei laufender Produktion nur schwer möglich und werden unterlassen. *Spike Reply* (www.reply.com) bietet eine Nachrüstung der Steuerungssoftware von Industrieanlagen an.

Die *Ubirch GmbH (www.ubich.com)* setzt Blockchain-Technologie gegen Datenverlust oder -verfälschung ein. Gleichgültig, woher die Daten stammen, ob von der Messung physikalischer Größen durch Sensoren, der Zählung von Besucherströmen oder die Durchführung der Schneeräumung – sie werden durch diese Technologie gleichsam versiegelt und können nicht mehr unbemerkt verändert, gelöscht oder dupliziert werden.

Start-ups. Die *Securai GmbH* aus Ingolstadt *(www.securai.de),* eines der 18 Start-up-Unternehmen auf der Messe, bietet eine Überprüfung des Inhalts von Festplatten an, einschließlich des Reverse-Engineerings von Firmware, also der Software, die in elektronischen Geräten eingebettet ist. Das Unternehmen berät auch bei der Entwicklung von Programmen und führt Pentests durch. *Chronos* von *Agile Response Technologies (www.agileresponse.com)* ist ein cloudbasiertes Tool, mit dem Computer und Server untersucht werden können, ob darauf Schad-Software abgelagert ist.

Mitarbeitersensibilisierung und Awarenesstraining werden vom Schweizer Unternehmen *Lucy Security AG (www.lucysecurity.com)* angeboten. Simulierte Angriffe können, etwa bei Phishing-Attacken, auf die spezielle Unternehmenssituation zugeschnitten werden, beispielsweise unter Verwendung jener Kontakte, die das betreffende Unternehmen hat.

IT-Seal (www.it-seal.de) setzt *Open Source Intelligence (OSINT)* ein, um anhand von Kennzahlen zu ermitteln, wie bedroht ein Unternehmen durch öffentlich zugängliche Informationen ist, etwa aus sozialen Medien. Die Informationen (Hobbies der Mitarbeiter, Betriebsausflüge, Urlaubsreisen u. a.) werden zur Schulung der Mitarbeiter in verschiedenen Schwierigkeitsgraden zu Spearfishing-Attacken verwendet.

Kurt Hickisch

Fotos: Kurt Hickisch