Sichere Infrastruktur

Bei der „Protekt 2017“ in Leipzig wurde in einer Konferenz und einer Fachausstellung der Schutz kritischer Infrastruktur erörtert.

Cyberangriffe sind die Bomben der Neuzeit“, sagte der Staatssekretär im Sächsischen Staatsministerium des Inneren, Dr. Michael Wilhelm, bei der Eröffnung der *Protekt 2017,* die am 21. und 22. Juni 2017 in der Kongresshalle am Zoo in Leipzig stattfand. Er unterstrich damit die Bedeutung der IKT-Sicherheit beim Schutz kritischer Infrastruktur, auf den sich diese, 2016 erstmals abgehaltene Messe, spezialisiert hat. 2016 seien 1.400 Cyber-Angriffe auf die sächsische Verwaltung verhindert worden, um 63 Prozent mehr als im Jahr zuvor. In Zusammenarbeit mit der TU Dresden sei ein Abwehrsystem auf der Basis von „Honeypots“ entwickelt worden.

Cybercrime. Die Gewinne aus Cybercrime übersteigen die aus dem Drogenhandel, sagte Peter Vahrenhorst vom LKA Nordrhein-Westfalen. Der Drogenhandel wird weitgehend über das Internet abgewickelt. Das Internet of Things (IoT), das „Smart Home“, vernetzte Fahrzeuge, Wirtschaft 4.0, werden neue Angriffsmöglichkeiten für Kriminelle eröffnen.

Wer die Sprachsteuerung seines Fernsehgerätes nutzen will, muss nicht nur umfangreiche AGBs akzeptieren, sondern auch, dass in dem betreffenden Raum zur Auswertung etwaiger Sprachsignale ständig über Internet mitgehört wird.

Sogar Tötungshandlungen über das Tatmittel Internet könnten nicht mehr ausgeschlossen werden, etwa über die Fernwartung von medizinischen Geräten (Beatmungsgeräte, Insulinpumpen). Manipulierte IT könnte die Ursache sein, dass ein Auto gegen einen Baum fährt und der Lenker getötet wird. „Fast jedes Delikt ist machbar“, sagte Vahrenhorst. Im Netz finden sich Kontaktbörsen für *Crime-as-a-Service (CaaS)*. Die Täter sind hochprofessionell, es herrsche ein „hochdynamisches Deliktsfeld“. Gezielte Cyber-Angriffe *(Advanced Persistent Threats, APT)* werden langfristig vorbereitet.

Fachmesse „Protekt 2017“: 29 Aussteller von Sicherheitsprodukten, über 200 Kongress-Besucher.

Foto: Kurt Hickisch

Im Fall eines CEO-Frauds, der im August 2016 einen deutschen Autozulieferer betroffen hatte, war, wie ermittelt werden konnte, der betrügerisch herausgelockte und überwiesene Geldbetrag von 40 Millionen Euro innerhalb einer Stunde auf Tausende Konten verteilt, um die Geldwäschebestimmungen zu unterlaufen. Das zeige, wie akribisch derartige Aktionen vorbereitet werden. Demgegenüber sind Angriffe mit Erpressungssoftware (Ransomware) breit gestreut und aus Sicht der Angreifer Zufallstreffer. In Hinkunft wird, sagte Vahrenhorst, vermehrt mit Cyber-Angriffen auf Flughäfen, die Bahn, Kraftwerke, Krankenhäuser und die IT-Industrie zu rechnen sein.

Stefan Strobel, *cirosec GmbH (www.cirosec.de),* ging aus technischer Sicht auf die Bedrohung durch APTs ein, wie derartige Angriffe erkannt und verhindert werden können. Herkömmliche, auf Signaturen basierende Virenscanner reichen nicht mehr aus. Oberstes Prinzip müsse sein, Maßnahmen der Prävention hochzufahren. Die sonst möglichen technischen Maßnahmen (Sandboxing, Simulation eines Angriffsziels – Honeypotting, Verhaltensanalyse, Vortäuschen von Schwachstellen, Einsatz von „Künstlicher Intelligenz“ …) würden zwar weitergehenden, aber eben doch nicht vollständigen Schutz bieten.

Prävention. „Aus der Untergrundliteratur ist seit Jahren bekannt, dass dezentrale Institutionen über ihre Strom- und Datenleitungen verwundbar sind“, sagte Rainer von zur Mühlen, *Mühlen’sche Sicherheitsberatung*. Nur teilweise sind die Leitungen redundant. Allerdings, wenn es brennt oder schwelt, erfolge dies normgerecht, ebenso wie der Verlauf von flächendeckenden Stromausfällen, Ausfälle von Rechenzentren und Versorgungsbetrieben. Die Probleme und Lösungsmöglichkeiten seien deshalb weit weniger aufwendig, als man glaube. Gefährdungs- und Schwachstellenanalysen seien keine „Zauberei“, sondern Denkarbeit, was auch für die KRITIS-Festigkeit in der IT gelte.

Prof. Timo Kob stellte den Wirtschaftsgrundschutz vor *(www.wirtschaftsschutz.info)*. Durch diesen wird, aufbauend auf dem IT-Grundschutz des BSI, ein ganzheitliches Schutzmodell entwickelt, das über die IKT hinaus weitere Aspekte wie physische Sicherheit oder Schutz von Geschäfts- und Betriebsgeheimnissen, Kunden- und Lieferantenmanagement einschließt. Mit Bausteinen können konkrete Lösungen für ein Problem erarbeitet werden.

Über 55 Prozent der Cyber-Attacken gehen auf Insider zurück, berichtete Eckhard Neumann, *Signum Consulting GmbH*. Der Personalauswahl kommt somit große Bedeutung zu, doch würden Spezialisten oft unter Zeitdruck eingestellt. Erst später stelle sich ihre kriminelle Neigung heraus. Aus Angst vor Reputationsverlust würde fast die Hälfte der Unternehmen von einer gerichtlichen Verfolgung absehen.

Bewerbungen werden den Angeboten angepasst. In Lebensläufen werden nach den Erfahrungen des Unternehmens aus der Untersu-

chung von 5.000 Überprüfungen in 28 Prozent der Fälle Abweichungen festgestellt, die wiederum zu 80 Prozent die Beschäftigungszeiten betreffen. Kurze Beschäftigungszeiten werden zusammengefasst, um einen häufigen Jobwechsel zu kaschieren. „Diploma-Mills“ produzieren Abschlusszeugnisse von Universitäten, sogar von solchen, die es gar nicht gibt. Auf behördliche Überprüfungen können nicht alle Unternehmen zurückgreifen. Zudem würden diese Überprüfungen lange dauern und bei Ermittlungen im Ausland vielfach ins Leere gehen. Über US-Anbieter können gegen Entgelt Auskünfte aus über 1.400 Datenbanken eingeholt werden. Probleme ergeben sich daraus, die ermittelten Daten eindeutig dem zu Überprüfenden zuzuordnen.

Die Grenzen, die der Überprüfung einer Person durch den Datenschutz gesetzt werden, erläuterte Dr. Niels Leperhoff, *Xamit BewertungGmbH*. Die Verarbeitung personenbezogener Daten muss entweder auf die Einwilligung des Betroffenen oder eine gesetzliche Grundlage zurückgeführt werden können. Der Grundsatz der Datenminimierung muss eingehalten werden und die Notwendigkeit der Erhebung dokumentiert werden. Die Daten müssen sachlich richtig und auf dem neuesten Stand sein. Die Speicherungsdauer ist auf den Verwendungszweck beschränkt.

IT-Sicherheitsgesetz.

Nach Vorarbeiten im Rahmen einer öffentlich-privaten Partnerschaft von Betreibern kritischer Infrastruktur (KRITIS) und dem Bund *(UP KRITIS; www.upkritis.de),* ist am 25. Juli 2015 in Deutschland das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) in Kraft getreten. Es verpflichtet – gesetzestechnisch durch eine Novellierung des BSI-Gesetzes – die Betreiber kritischer Infrastruktur, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme zu treffen (Einhaltung von Mindeststandards).

Das österreichische Unternehmen FAAC präsentierte auf der „Protekt 2017“ in Leipzig Produkte für Zufahrtssicherheit.

Die Erfüllung dieser Anforderungen ist mindestens alle zwei Jahre nachzuweisen. Treten erhebliche Störungen ein, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der betriebenen Infrastruktur führen oder führen könnten, haben die Betreiber dies über eine von ihnen zu benennende Kontaktstelle dem *Bundesamt für Sicherheit in der Informationstechnik (BSI)* zu melden. Dieses wiederum hat alle zur Gefahrenabwehr wesentlichen Informationen zu sammeln und auszuwerten, ein Lagebild zu erstellen und die Betreiber von KRITIS sowie die jeweiligen Aufsichtsbehörden zu unterrichten. Vom Hersteller der betroffenen informationstechnischen Produkte und Systeme kann, soweit erforderlich, die Mitwirkung an der Beseitigung oder Vermeidung einer Störung verlangt werden.

Zunächst wurden durch die am 3. Mai 2016 in Kraft getretene BSI-Kritis-Verordnung Kriterien (Schwellenwerte) für die Sektoren Energie, Wasser, Informationstechnik und Telekommunikation sowie Ernährung („1. Korb“) festgelegt und damit, welche Anlagen und Dienstleistungen wegen ihrer Bedeutung als kritisch anzusehen sind. Der Erfassungsvorgang ist mittlerweile abgeschlossen und umfasst rund 1.000 Unternehmen bzw. Anlagen. Durch die am 30. Juni 2017 in Kraft getretene Erste Verordnung zur Änderung der BSI-Kritis-Verordnung wurden die Kriterien für die Sektoren Gesundheit, Finanz- und Versicherungswesen, Transport und Verkehr („2. Korb“) festgelegt.

Krankenhäuser mit mehr als 30.000 Behandlungsfällen pro Jahr zählen in Deutschland zur kritischen Infrastruktur und sind den Regelungen des IT-Sicherheitsgesetzes unterworfen, berichtete Thorsten Schütz, Leiter IT des Klinikums Itzehoe. Da in Krankenanstalten Gesundheitsdaten von Patienten verarbeitet werden, ist auf die Sicherheit dieser Daten besonderer Wert zu legen – nicht zuletzt wegen der hohen Strafsätze, die die am 25. Mai 2018 in Kraft tretende DSGVO mit sich bringen wird.

Als spezifisches datenschutzrechtliches Problem in Krankenhäusern sieht Schütz die zunehmende Verwendung von mobilen Geräten, auf denen Untersuchungsergebnisse und Dokumentationen abgespeichert werden. Durch die Verwendung dieser Geräte wird die Anfälligkeit gegenüber Angriffen immer größer. Weitere derartige Risiken stellen der Einsatz von Robotern zu Transport und Pflege dar sowie die maschinell erfolgende, intelligente Auswertung von Befunden bis zum Schreiben des Arztbriefes.

Cyber-Security-Management erfordere, wie Florian Haake, *Innogy SE,* aus Sicht eines Energieversorgers ausführte, eine gesamtheitliche Betrachtungsweise durch Staat und Gesellschaft. Auch die Hersteller seien verant-

Foto: Kurt Hickisch

Marina Bauer: „Unternehmen tragen die Verantwortung für die Lebensmittelsicherheit auf allen Produktionsstufen.“

Timo Kob: „Ein ganzheitliches Schutzmodell schließt physische Sicherheit oder Schutz von Geschäftsgeheimnissen mit ein.“

Florian Haake: „Unternehmen sollten Maßnahmen setzen, um das Sicherheitsbewusstsein der Mitarbeiter für IKT-Risiken zu heben.“

Eckhard Neumann: „Über 55 Prozent der Cyber-Attacken gehen auf Insider zurück. Daher ist die Personalauswahl wichtig.“

wortlich, indem sie zeitnah Sicherheitslücken zu kommunizieren und Sicherheitsupdates zur Verfügung zu stellen hätten. Wichtig sei die „Human Firewall“: Der Mensch stehe als wichtigster Sicherheitsfaktor im Mittelpunkt. E-Learning, gemeinsame Mittagessen in kollegialem Kreis zu verschiedenen Themen („lunch and learn“), Online-Videos, Workshops, könnten dazu beitragen, das Sicherheitsbewusstsein der Mitarbeiter für IKT-Risiken zu heben.

Lebensmittelsicherheit. Die Risiken in der Lebensmittelindustrie spannen sich, wie Marina Bauer von der *AFC Risk Crisis Consult GmbH* aufzeigte, vom – oftmals in anderen Ländern oder auf anderen Kontinenten befindlichen – Produzenten bis zum Verkauf im Handel. Nach der VO (EG) Nr. 178/2002 tragen Unternehmen auf allen Produktions-, Verarbeitungs- und Vertriebsstufen, die unter ihrer Kontrolle stehen, die Verantwortung für die Lebensmittelsicherheit.

Die Rückverfolgbarkeit ist in allen diesen Produktionsstufen sicherzustellen. Dazu sind jeweils die unmittelbaren Vorlieferanten und Abnehmer zu dokumentieren (Art. 17 und 18). Der Vermeidung von Gefahren im Zusammenhang mit Lebensmitteln dient das HACCP-Konzept (Hazard Analysis and Critical Control Points), dessen Einhaltung nach der VO (EG) Nr. 852/2004 über Lebensmittelhygiene von den einschlägigen Unternehmen gegenüber der Behörde nachzuweisen ist. Die Lieferkette ist bedroht durch Ernteausfälle, Lieferantenstreiks, Kampagnen, gezielte Sabotage und durch Lebensmittelbetrug (Food Fraud). Weitere Risiken liegen in Schimmelpilzgiften, Rückständen von Antibiotika und Pflanzenschutzmitteln. Auch sind ethische und moralische Bedenken wie etwa Kinderarbeit und Massentierhaltung zu berücksichtigen. Für kritische Lebensmittel besteht ein europäisches Schnellwarnsystem. Die Vermeidung von Risiken entlang der Lieferkette sei nur durch Zusammenarbeit möglich, verbunden mit Lieferanten-Audits und verpflichtender Zertifizierung.

Krise. Als Krise bezeichnete Franz Schönrock, *Grayling Deutschland GmbH,* ein Ereignis, das wahrscheinlich schwerwiegende Auswirkungen auf ein Unternehmen hat und Maßnahmen erfordert, die nicht mehr mit den bestehenden organisatorischen Strukturen und Prozessen bearbeitet werden können.

Es gelte, das in einem Krisenfall rasch entstehende Informationsvakuum zu füllen. Die Medien verlangen Schnelligkeit. Nach spätestens einer Stunde sollte von dem betroffenen Unternehmen eine erste Stellungnahme abgegeben werden.

„Die öffentliche Meinung entscheidet über das Ausmaß einer Krise“, sagte Schönrock. Die herkömmliche, um sachliche Information, Expertensicht, Aufklärung, bemühte Kommunikation stößt auf emotionale Opfersicht; Gerüchte; die Suche nach Schuldigen, was ein professionelles Kommunikations-Management erfordere. *Kurt Hickisch*

PROTEKT 2017

IT-Sicherheit

Vorrangiges Thema der Messe ist der Schutz kritischer Infrastruktur, sowohl in physischer als auch im Hinblick auf die IT-Sicherheit. 29 Aussteller einschlägiger Produkte waren vertreten. Die Messe wurde an beiden Tagen von einer Fachkonferenz begleitet, die von über 200 Personen besucht wurde. Die über 20 Referate wurden teilweise in zwei parallel verlaufenden Vortragsreihen (Tracks) gehalten. Die Inhalte der Vorträge wurden von den Moderatoren zum Ende des Tages überblicksweise zusammengefasst. Bei einem Round Table wurde auf breiter Basis das Spannungsfeld zwischen Regulation und Wirtschaftlichkeit im Bereich von KRITIS diskutiert. In den jeweiligen Mittagspausen hatten Aussteller im „Pitching Corner“ Gelegenheit, in Form von Kurzvorträgen sich und ihre Produkte vorzustellen.

Die Schirmherrschaft über die Protekt hatten Bundesinnenminister Dr. Thomas de Maizière und der Sächsische Ministerpräsident Stanislaw Tillich übernommen. Ideelle Träger waren der *ASW Bundesverband Allianz für Sicherheit in der Wirtschaft e.V.* und der *Verband für Sicherheitstechnik e.V. (VfS). www.protekt.de*

Fotos: Kurt Hickisch