Sicherer ohne Web

Der Cyber-Sicherheit wird in der Gesellschaft immer mehr Bedeutung zugemessen. Das zeigte sich auch bei der IKT-Sicherheitskonferenz 2017 am 26. und 27. September 2017 in Villach.

Beim Bundesheer werde ein Cyberkommando aufgebaut, man stehe dabei im Wettstreit mit der Wirtschaft, Fachleute zu gewinnen, sagte Verteidigungsminister Mag. Hans Peter Doskozil bei der Eröffnung der IKT-Sicherheitskonferenz, die am 26. und 27. September 2017 in Villach stattgefunden hat. Die Kompetenz des Bundesheeres liege in der Cyberdefense als Teil der Landesverteidigung, die des Innenministeriums in der Abwehr von Cybercrime, betonte Doskozil. Die Schnittstellen seien mitunter fließend; dem Bundeskanzleramt komme eine koordinierende Funktion zu.

Bei der friedlichen Nutzung des Cyberraums seien in den letzten Jahren Rückschläge zu verzeichnen gewesen, sagte Wolfgang Röhrig von der Europäischen Verteidigungsagentur *(European Defense Agency)*. Offen sei die Frage der Anwendung des Völkerrechts und die der Menschenrechte im Cyberraum.

Bedrohungsbild. DI Dr. Sabine Herlitschka, Vorstandsvorsitzende der *Infineon Technologies Austria AG,* verwies in ihrer Keynote auf die *KPMG*-Studie 2017 zur Cybersecurity in Österreich. Demnach wurden 72 Prozent der Unternehmen in den vergangenen zwölf Monaten Opfer von Cyberangriffen, 87 Prozent davon Industrieunternehmen. 36 Prozent der Befragten wussten nicht, welche Auswirkungen der Angriff hatte. Im *Infineon Cyber Defense Center* wurden im ersten Halbjahr 2017 2,6 Milliarden Attacken und 6,8 Millionen Spam-Mails blockiert. 48.000 Virus-Attacken wurden verhindert. Trotz dieser vielen Angriffe kam es zu keinen kritischen Vorfällen. Derzeit ist erst ein Prozent der Gegenstände, die in einem Netzwerk verbunden sein könnten, auch tatsächlich mit diesem verbunden. Bis 2020 wird es 50 Milliarden vernetzte Geräte/Systeme geben.

IKT-Sicherheitskonferenz: Gerät zur Drohnendetektion.

Foto: Kurt Hickisch

Der Halbleiterindustrie kommt als Bindeglied zwischen der realen und der digitalen Welt eine Schlüsselstellung zu. 2020 werden Halbleiter zwischen 30 bis 45 Prozent zum europäischen Bruttoinlandsprodukts beitragen. Auf Industrie 4.0 werden zwischen 15 und 20 Prozent entfallen. Digitalisierung ermöglicht Mehrwert und schafft Wachstum, doch sei Sicherheit dabei das zentrale Element.

DI Harald Leitenmüller, CTO *Microsoft Österreich,* präsentierte Weltkarten mit den Regionen, aus denen verschiedene Arten von Bedrohungen kommen. Man müsse immer vom Vorhandensein von Angreifern ausgehen und sich darauf vorbereiten. Nicht die Ausfallssicherheit sei mehr das Ziel, sondern die Resilienz. Das System müsse schnell wieder funktionieren. War früher das Ziel, jeden möglichen Angriff zu verhindern, liegt der Schwerpunkt auf Schutz, Erkennen eines Angriffs und Setzen von Abwehrmaßnahmen.

John Matherly, Entwickler der auf Steuerungssysteme spezialisierten Internet-Suchmaschine *Shodan,* machte in Form einer Kartierung des Internets deutlich, dass das, was vom Internet bekannt ist, nämlich Messenger-Dienste, Suchmaschinen, soziale Netzwerke, nur „die Spitze eines Eisbergs“ sei. Unter der üblicherweise sichtbaren Oberfläche befinden sich, einem bisher wenig erschlossenen Neuland gleich, unzählige ans Internet angeschlossene Webcams, eingebettete Systeme (embedded systems), Industrieanlagen, Kraftwerke. Sicherheitslücken dieser vielfach nur trivial abgesicherten Systeme ermöglichen Angriffe von außen.

Auf welch raffinierte Weise Angreifer vorgehen, zeigte Oberstleutnant Volker Kozok vom deutschen Bundesministerium der Verteidigung an Hand von *Advanced Persistent Threats (APT)* auf. Es handelt sich dabei um lang vorbereitete, zielgerichtete und mit hoher fachlicher Qualifikation der Täter durchgeführte Cyber-Angriffe. Die aus Russland kommende APT 29 Gruppe nutzt Anti-Forensik-Techniken und beobachtet die Bemühungen der Opfer zur Schadensbegrenzung.

Die ihr zugeschriebene Malware Hammertoss stellt erst in etlichen Verfahrensschritten, unter anderem durch das Hochladen eines Bildes, das steganografisch verschlüsselt einen Programmiercode enthält, eine Verbindung her, die Daten aus dem Opfersystem in die Cloud verschickt. Ähnliche Gruppierungen sind die Dukes-Gruppe *(„Cozyduke“, „Hammerduke“, „Cloudduke“).*

Live-Demos. Marco di Filippo *(Koramis GmbH, www.koramis.de)* führte in Live-Hackings Angriffe auf Fotovoltaikanlagen und Hausautomatisierungssysteme vor. Bei einem dieser Systeme konnte die ganze Alarmanlage unter Kontrolle gebracht werden. Um zu beobachten, wie häufig Angriffe auf Smart Homes erfolgen, wurde aus Komponenten verschiedener Hersteller derartiger Systeme ein „Geisterhaus“ (Haunted House) aufgebaut und ins Netz gestellt. Innerhalb von sechs Wochen wurden über 70.000 Angriffe gezählt, ein Viertel davon aus China.

Mit einem Industrieroboter demonstrierte Sascha Herzog, *NSIDE Attack Logic GmbH (www.nside-*

attacklogic.de) im Zusammenwirken mit dem *Fraunhofer IGCV,* welche Auswirkungen es hat, wenn Steuerungsdaten eines solchen Roboters verändert werden. Das 1,5 Tonnen schwere Gerät war von Pionieren des Bundesheeres auf die Bühne des Saales des Congresszentrums transportiert worden.

Etwa 150 solcher Roboter werden in den Fertigungshallen eines großen deutschen Automobilherstellers eingesetzt und arbeiten vollautomatisch in nach außen abgeschotteten Netzen. Der zur Schau gestellte Roboter hatte allerdings eine Schwachstelle: Er wurde von einer mit dem Internet verbundenen Kamera (Webcam) überwacht. Durch Untertunnelung konnten über dieses Einfallstor Parameter der insgesamt auf sechs Achsen laufenden Steuerung verändert werden.

Das nur mit einem Bruchteil seiner tatsächlichen Leistung arbeitende Gerät wurde „wild" und zerdrückte zwei unter ihm liegende Schaufensterpuppen – symbolisch für die Ohnmacht des Menschen gegenüber dem außer Kontrolle geratenen Wüten der Maschine. In der Praxis könnten ganze Produktionsstrecken zerstört werden.

Die Folgen von Fehlsteuerungen wären noch schwerwiegender, wenn die Produktion in Chemiewerken (Kesselsteuerung) beeinflusst werden würde oder Krankenhäuser, Wasser- und Energieversorger betroffen wären. Die Lösung ist nur in einer völligen Trennung vom Internet zu sehen, was auch Fernwartung ausschließt oder Zugänge über angesteckte Medien. Auch jemand, der sich als Servicetechniker ausgibt, muss nicht einer sein.

Volker Schnapp (*Fink Secure Communications GmbH (www.fink-secure.com)* schilderte an Hand einer fiktiven Dienstreise, wie eine Zielperson, beginnend vom Visums-Antrag über den Access-Point im Flugzeug bis zu der mit Fingerabdruck und Foto erfolgenden Grenzkontrolle überwacht und bis ins Hotelzimmer abgehört und ausgespäht werden kann.

IKT-Konferenz: Demonstration der Folgen der Fehlsteuerung eines mit dem Internet verbundenen Industrieroboters.

Zum Abhören genügen Lüftungsanlagen, in die Mikrofone eingebaut werden. Lautsprecher lassen sich in Umkehrung des physikalischen Prinzips als Mikrofone verwenden. Drahtlose Mikrofone können abgehört werden. Abhören von außen wird möglich, indem hochfrequente oder Laserstrahlung auf Fensterscheiben gerichtet wird. Die durch Schallschwingungen der Fensterscheiben erfolgende Modulation der reflektierten Wellen kann hörbar gemacht werden. Eine einfache Abwehrmöglichkeit besteht darin, die Jalousien zu schließen.

Rechtslage. Der Datenschutzaktivist Mag. Max Schrems hob jene Bestimmungen der am 25. Mai 2018 in Kraft tretenden Datenschutz-Grundverordnung (DSGVO) hervor, die die Datensicherheit betreffen. Durch ihren technologieneutralen Ansatz und ihre eher abstrakten Regelungen ist diese Verordnung der EU auf lange Lebensdauer angelegt. Abgesehen von den hohen Strafdrohungen ergeben sich weitere Risiken aus Schadenersatzforderungen, für die es als Eingriff in die Privatsphäre reicht, wenn personenbezogene Daten in den Besitz anderer gelangen. Es werden Sammelklagen möglich, was zur Herausbildung von Geschäftsmodellen führen könnte. Zum Unterschied von Strafen, bei deren Bemessung mildernde Umstände zu berücksichtigen sind, ist Schadenersatz unabhängig von solchen Gesichtspunkten zu leisten. Schadenersatzforderungen könnten verhängte Geldstrafen erheblich übersteigen.

Die von Art. 32 DSGVO geforderte – und gegebenenfalls vor Gericht zu beweisende – Sicherheit der Verarbeitung von Daten nach dem „Stand der Technik" wird sich aus den ISO Normen 27000f ableiten lassen, aus nationalen und Industrie-Normen sowie Handbüchern. Mit einer Zertifizierung nach Art. 42 wird nachgewiesen werden können, dass bei Verarbeitungen die Bestimmungen der DSGVO eingehalten werden. Verletzungen des Schutzes personenbezogener Daten, die voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen, sind binnen 72 Stunden der Aufsichtsbehörde zu melden (Art. 33). Hat die Verletzung ein hohes Risiko für diese Rechte und Frei-

FOTO: KADMY/FOTOLIA

CYBERSECURITY

IKT-Sicherheitskonferenz

Die vom Abwehramt des Bundesheeres organisierte IKT-Sicherheitskonferenz am 26. und 27. September 2017 im Congress-Center in Villach wurde von 2.703 registrierten Teilnehmern besucht. An beiden Veranstaltungstagen wurden, im Wesentlichen inhaltsgleich und aufeinander zeitlich abgestimmt, im Plenum allgemeine und in Nebensälen vertiefende (Fach-)Vorträge zu den Themen Cybersecurity, kritische Infrastruktur und Industrie 4.0/Cybersecurity abgehalten. Insgesamt gab es etwa 60 Vorträge. In den Foyers waren etwa 50 Aussteller mit ihren IT-Sicherheitsprodukten und -dienstleistungen vertreten. Drei sechzehnjährige Schüler aus Niederösterreich führten das autonome Fliegen von Drohnen vor. Die Schüler hatten mit ihrem System die Weltmeisterschaft im autonomen Fliegen mit Drohnen gewonnen. Eine Drohne warf über ein programmiertes Ziel ein Rettungspäckchen mit Wasserflasche, Verbandszeug und Aludecke ab. Simuliert wurde damit die Erstversorgung eines Verunglückten, der seinen Lageort mit GPS-Daten mitgeteilt hatte.

Die nächste IKT-Sicherheitskonferenz wird am 16. und 17. Oktober 2018 in Alpbach in Tirol abgehalten.

heiten zur Folge, hat der Verantwortliche die betroffene Person unverzüglich von der Verletzung zu benachrichtigen (Art. 34). Es wird sich empfehlen, alle diesbezüglichen Vorgänge, auch jene, die zum Data Breach geführt haben, gerichtsfest zu dokumentieren.

Ausblick. Die Informationstechnologie ermöglicht die totale Transparenz. Das könnte auch totale Überwachung ermöglichen. „Das Geheimnis ist der Grundpfeiler der Freiheit", betonte Michael George, Leiter des Bayerischen Landesamtes für Verfassungsschutz.

Die Grenze der Transparenz müsse definiert werden, gegenüber anderen und gegenüber dem Staat. Transparenz nach oben sei ein Merkmal von Demokratien, von oben nach unten ein Kennzeichen von Diktaturen. Horizontale Transparenz ergebe sich aus den großen Datenbeständen von Suchmaschinen, Online-Versandhäusern und Social-Media-Unternehmen.

George bezeichnete die vernetzte globale Welt als ein Eldorado für Nachrichtendienste. Die Kontrolle über die Systeme sei verloren gegangen. Man habe kaum eine Ahnung, was im Netz vorgehe. Die Geschwindigkeit der technischen Entwicklung steige exponenziell. Heute könnten vielleicht über 60-Jährige mit der Entwicklung (z. B. Online-Banking) nicht mehr Schritt halten – was aber ist die Folge, wenn im Erwerbsleben stehende 40-Jährige nicht mehr mithalten können?

Referenten bei der IKT-Sicherheitskonferenz: Sascha Herzog, Michael George, John Martherly, Volker Kozok.

Wer in dieser Altersgruppe kennt sich beispielsweise mit Blockchain-Technologie oder Kryptowährungen aus? Was ist, wenn sich das Wissen zunehmend auf Experten verengt und Entscheidungen Algorithmen überlassen werden?

Es gelte, das Verständnis für die IT in die Breite zu tragen und die Mittel dazu bereitzustellen. Auch könne man bei der Abwehr von Cyber-Angriffen nicht mehr so weitermachen wie bisher, mit einer Reihe von Ämtern mit fest umrissenen Zuständigkeiten. Ein Angriff könne zu einem Fall für den Verfassungsschutz werden, wenn er sich gegen kritische Infrastruktur richtet. Ein Angreifer habe „alle Zeit der Welt", seinen Angriff vorzubereiten, wogegen der Verteidiger keinen Tag zu spät mit Gegenmaßnahmen reagieren dürfe. Vor diesem Hintergrund wurde 2013 in Bayern beim Verfassungsschutz das Cyber-Allianz-Zentrum Bayern (CAZ) als Single Point of Contact und vertraulicher Ansprechpartner für betroffene Unternehmen eingerichtet.

„Alles, was sich digitalisieren lässt, wird digitalisiert", sagte der Leiter des Cyber-Defense-Centrums des BMLVS, ObstdG Mag. Walter Unger, abschließend. Durch die Digitalisierung können Kosten gesenkt und Menschen von schwerer oder eintöniger Arbeit entlastet werden.

Auf 1.000 Arbeitsplätze entfallen in Österreich 138 Roboter. In Deutschland sind es um 100 mehr. Die Länder mit vielen Robotern im Arbeitsprozess hätten eine hohe Beschäftigung. Die durch die Maschinen abgelösten Menschen würden anderswo gebraucht, wenn auch mit anderer Qualifikation. In drei Jahren werden im Internet of Things (IoT) rund 50 Milliarden Geräte miteinander verbunden sein. Voraussetzung dafür ist die IT-Sicherheit, zumindest in einem solchen Ausmaß, dass das Risiko getragen werden kann. Angriffe auf das IoT sind insofern zu erwarten, als die Geräte als solche wenig gesichert sind.

Es gilt, die Angriffsflächen zu reduzieren. Es braucht nicht alles ins Netz gestellt zu werden, und es braucht auch keine riesigen Software-Programme, die nur zum Teil genützt werden. Die lebenswichtigen Systeme dürfen von außen nicht erreicht werden können.

Die Verteidigung gegen Angriffe aus dem Cyber-Raum muss automatisiert werden, weil der Mensch nicht schnell genug reagieren kann. Für das Bundesheer gilt es, die eigenen Systeme zu schützen und die Landesverteidigung im Cyberraum zu sichern. Die seit 2013 in Österreich bestehende Cyber-Strategie wird bis zum Frühjahr 2018 evaluiert. Das NIS-Gesetz ist in Vorbereitung.

Kurt Hickisch

HACKER-BEWERB

Cyber-Security-Challenge

Im Rahmen der IKT-Sicherheitskonferenz fand das Finale der österreichischen Cyber-Security-Challenge und die Nominierung der zehn österreichischen Teilnehmer für die 4. Europäischen Cyber Security Challenge statt. 466 hatten sich angemeldet, 20 davon kamen – in zwei Altersklassen – in die Endausscheidung.

Die Austrian Cyber-Security-Challenge ist 2012 aus einer Initiative des Vereins *Cyber Security Austria (www.csa.at)* entstanden, unterstützt vom Abwehramt, dem BMI, Bundeskanzleramt und Sponsoren.

Die besten Hacker sollten sich untereinander messen können mit dem Ziel, Nachwuchstalente für die IKT-Sicherheit zu gewinnen. 2013 hat sich auch die Schweiz an diesem Wettbewerb beteiligt, 2014 ist Deutschland dazugekommen. Bei dem in Fürstenfeld ausgetragenen, als 1. Europäische Cyber-Security-Challenge bezeichneten Wettbewerb siegte das österreichische Team, ebenso bei der 2. Europäischen Challenge 2015 in Luzern, an der sich auch Hacker aus Großbritannien, Spanien und Rumänien beteiligt hatten.

Bei der 3. Challenge 2015 in Düsseldorf waren zusätzlich Teilnehmer aus Estland, Irland, Griechenland und Liechtenstein vertreten. Mit den 2017 dazugekommenen Nationen Tschechien, Zypern, Dänemark, Italien und Norwegen werden bei der 4. European Cyber Security Challenge, die vom 31. Oktober bis 3. November in Malaga/Spanien ausgetragen wird, die Teams von insgesamt 15 Nationen gegeneinander antreten.

www.verbotengut.at

FOTOS: KURT HICKISCH