Interpol Global Complex for Innovation in Singapur: Im „Cyber Fusion Centre“ arbeiten Vertreter von Polizeibehörden mit Wissenschaftlern und Experten aus der Privatwirtschaft zusammen.

FOTO: WALLACE WOON/EPA/PICTUREDESK.COM

Sicherheit im Netz

Bei der IKT-Sicherheitskonferenz 2016 des Abwehramtes des Bundesheeres wurde die Notwendigkeit und Wichtigkeit der Sicherung des Cyberraums betont.

Bei der Cyber-Sicherheit sind die Kompetenzen zwischen dem BMI und dem BMLVS klar aufgeteilt“, sagte General Mag. Othmar Commenda bei der Eröffnung der 15. IKT-Sicherheitskonferenz des Abwehramtes, die am 11. und 12. Oktober 2016 im Kongresshaus in St. Johann im Pongau stattgefunden hat. Für das Bundesheer ist die Cyber-Sicherheit Teil der militärischen Landesverteidigung. Organisatorisch wird der Bedeutung dieser Aufgabe durch die Errichtung eines Kommandos „Führungsunterstützung und Cyber-Defense“ im BMLVS Rechnung getragen werden. Beim Abwehramt ist ein Cyber-Verteidigungszentrum im Ausbau.

Veranstaltungen wie die Sicherheitskonferenzen, die seit 2012 in jeweils einem anderen Bundesland abgehalten werden, dienen der Schulung von Experten und Mitarbeitern. Zudem wurde in Zusammenarbeit mit dem Bundeskriminalamt und der *Cyber Security Austria (CSA)* während der Veranstaltung an vier Schulen in St. Johann und Bischofshofen Aufklärungsarbeit zur IT-Sicherheit geleistet. An den beiden Tagen fand das nationale Wettkampffinale für die „Internationale Cybersecurity-Challenge 2016“ statt.

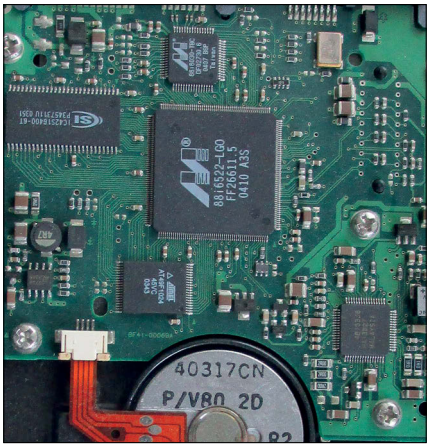
Neue Bedrohungen. „Die Abhängigkeit von der IT führt zu neuen Bedrohungen“, betonte Brigadier General J. M. Hans Folmer vom D*efence Cyber Command* der Niederlande. Auseinandersetzungen zwischen Staaten würden zunehmend im Cyberraum ausgetragen, doch könne nicht klar unterschieden werden, wer hinter diesen Angriffen stecke. In Frage kämen auch staatlich gelenkte Organisationen. Folmer erwähnte den Hackerangriff auf die ukrainische Stromversorgung zu Weihnachten 2015. Angesichts der diffusen Bedrohungslage helfe nur, sich bestmöglich zu verteidigen. In den Niederlanden sei hiezu das *Defence Cyber Command* entwickelt worden. Man sei bemüht, die besten IT-Spezialisten zu gewinnen; junge Menschen, die ihr Hobby zum Beruf machen, in Zusammenarbeit mit Forschungseinrichtungen, anderen öffentlichen Diensten und anderen Staaten.

Auf die Abhängigkeit vom Internet wies Dr. Thomas Grüter hin. In seinem Buch „Offline“ beschreibt er ein „Ende des Internets“ und den möglichen „Untergang der Informationsgesellschaft“. Internetdienste bestimmen zunehmend die sozialen Beziehungen und das Konsumverhalten der Menschen. Die Wirtschaft funktioniere ohne Internet kaum

noch, wobei die Abhängigkeit in den nächsten Jahrzehnten noch zunehmen werde. Auch die Wissenschaft sei ohne Internet kaum noch denkbar. Die Stromversorgung erfolge über Smart Grids, die das Angebot und die Nachfrage nach Strom ständig im Gleichgewicht halten müssen. Kann dieses nicht erreicht werden, bricht das Netz zusammen. „Das Internet ist die komplexeste Infrastruktur, die je errichtet wurde." Wäre deren Zusammenbruch mit dem fast vollständigen Verlust an Schriften am Ende der Spätantike vergleichbar? Drohen Gefahren durch Naturkatastrophen oder solare Magnetstürme, durch den Klimawandel oder die Kriegsgefahr in Asien? Das Internet werde zum Kriegsschauplatz werden, betonte Grüter. Die Sabotage von lebenswichtigen Einrichtungen sei wahrscheinlich. In Anbetracht künftiger Gefahren müsse die Wartung und Verbesserung der Infrastrukturen höchste Priorität erhalten. Die Ausfallsicherheit müsse verbessert und die Komplexität verringert werden. Wichtige Hightech-Komponenten (Computerchips) müssten regional hergestellt und die Herstellungsverfahren vereinfacht werden. Die Energieversorgung müsse sichergestellt werden.

Cyber-Angriffe. Wie leicht industrielle Anlagen angegriffen werden können, führte Marco Di Filippo bei einem Live-Hacking vor, beginnend im Kleinen beim Smart-Home, indem Einfluss auf die Beleuchtung und das Steuern von Geräten genommen wurde. Es wurden Manipulationen von Solarstromanlagen vorgeführt, bis hin zu simulierten Angriffen auf Verkehrssteuerungsanlagen. Alle im Internet vernetzten Systeme sind angreifbar – von der Energieversorgung, der Produktion, über das Transportwesen bis zum Finanzwesen.

Menschliche Verhaltensweisen können ausgenützt werden, um virtuell oder physisch in ein Unternehmen einzudringen *(Social Engineering)*, sich also beispielsweise Zutritt zu geschützten Räume zu verschaffen. Beispiele für letzteres brachte Ivano Somaini, *Compass Security (www.csnc.ch)*. Aus Höflichkeit und Hilfsbereitschaft wird einem anderen eine Tür offen gehalten, die nur über Zutrittskontrolle hätte passiert werden dürfen *(Piggybacking,* zum Unterschied vom *Tailgaiting*, bei dem jemand dem Öffnenden unmittelbar nachfolgt). Umso eher wird man dem Nachfolgenden die Tür offen halten, wenn sich dieser zuvor in der Cafeteria gegenüber einem selbst so zuvorkommend verhalten hat. Oder wenn er ein voluminöses Paket trägt, das ihm beim Türöffnen sichtlich Schwierigkeiten bereitet, oder er vor der geschlossenen Tür intensive Telefonate mit jemandem im geschützten Bereich führt, den er dringend treffen will. Entsprechende Vorbereitung über den Gesprächspartner ist dabei Voraussetzung, um solche Fake-Telefonate für den tatsächlich Zutrittsberechtigten soweit glaubhaft erscheinen zu lassen, dass er auch dem anderen ohne weitere Überprüfung den Zutritt ermöglicht.



IKT-Sicherheit: Die Abhängigkeit von der IT führt zu neuen Bedrohungen.

Suchmaschinen und soziale Medien bieten genügend Möglichkeiten, sich einen Einblick über die innere Struktur von Unternehmen und die Lebensgewohnheiten von Mitarbeitern zu verschaffen. Während in früheren Jahren das Internet vornehmlich dazu benützt wurde, Inhalte herunterzuladen, geht derzeit die Tendenz zum Uploading. Man stellt Inhalte (Fotos, Videos, persönliches Erleben) ins Netz, die ausgewertet und zu Angriffen durch Social Engineering ausgenützt werden können. Über gemeinsame Interessen kann sich ein Außenstehender Vertrauen erschleichen und dieses zum Schaden des Unternehmens missbrauchen – beispielsweise, jemanden dazu zu verleiten, einen infizierten Mail-Anhang zu öffnen oder eine Website mit Malware anzuklicken. Oder der Angreifer hat in Erfahrung gebracht, wann ein Entscheidungsträger nicht erreichbar ist, etwa wegen einer Urlaubsreise.

Automatisiert erstellte Abwesenheitsnotizen können aufschlussreich sein. Mit dem weiteren Wissen über Unternehmeninternes und durch zusätzlichen Aufbau von Stress wegen angeblicher besonderer Dringlichkeit können unter Vortäuschung der Autorität des Entscheidungsträgers betrügerische Vermögenstransaktionen herbeigeführt werden *(CEO-Fraud)*.

Während die Vorsicht gegenüber E-Mails zuzunehmen scheint, ist laut Sonaini das Vertrauen in SMS offenbar nach wie vor gegeben, obwohl ein falscher Absender leicht vorgetäuscht werden kann *(Mail-Spoofing)*. Der angebliche Chef, der behauptet, seine Büroschlüssel verlegt zu haben, bittet die Sekretärin per SMS, ihm einen Schlüssel zum Büro an einer bestimmten Stelle außerhalb zu hinterlegen.

Gunnar Porada, *InnoSec GmbH (www.innosec.eu)*, stellte einen Trojaner vor und zeigte vor, dass Dateien von mehreren hundert MB innerhalb weniger Sekunden über ein nur 7,5 Kilobyte großes (Ransomware-)Programm so verschlüsselt werden können, dass sie nicht mehr verwendbar sind.

Meinungsbeeinflussung. Am Beispiel jüngster Konflikte in Südosteuropa arbeitete Volker Kozok an Hand offener Quellen heraus, wie Angriffe im Cyber-Raum eingeleitet werden. Im Vorfeld geht es um Meinungsbildung und -beeinflussung. Es werden *GONGOs (government organized non-governmental organizations)* gebildet, wogegen NGOs als „Foreign Agents"

ABWEHRAMT

IKT-Sicherheitskonferenz

Die Teilnahme an der jährlichen, zweitägigen IKT-Sicherheitskonferenz des Abwehramtes erfolgt über Einladung und ist kostenlos. Im Plenum werden Vorträge allgemeinen Inhalts gehalten und parallel dazu gibt es „Sessions" zu Fachthemen.

Bei der 15. IKT-Sicherheitskonferenz in St. Johann im Pongau war jeder Tag mit jeweils 900 Teilnehmern ausgebucht. Es gab rund 50 Vorträge und 30 Aussteller. Die 16. IKT-Sicherheitskonferenz wird am 26. und 27. September 2017 im Kongresshaus Villach (Kärnten) stattfinden.

www.bundesheer.at

Referent bei der IKT-Sicherheitskonferenz: Gunnar Porada, Hans Folmer, Ivano Somaini, Marco di Filippo, Othmar Commenda, Thomas Grüter, Walter Unger und Thomas Herko.

unterdrückt werden. Zur psychologischen Kriegsführung in den Kommentaren von Web-Anwendungen und sozialen Medien werden bezahlte Blogger und Internet-Trolls (provokative Störer in einer Internet-Kommunikation) eingesetzt. Ein und derselbe Troll kann unter verschiedenen Identitäten im Internet auftreten („Sockenpuppen"), um Meinungen zu vervielfältigen und bedeutsamer erscheinen zu lassen. In „Troll-Fabriken" werden automatisiert Antworten auf Einträge in sozialen Medien erzeugt, wenn dort bestimmte Stichworte aufscheinen. Es wird getrachtet, eigene internationale Massenmedien gezielt auf andere Staaten auszuweiten und nationale Medien aufzukaufen. Gruppierungen beginnen Cyber-Attacken gegen den Zielstaat. Von dort wird in ähnlicher Weise geantwortet. Websites werden gehackt und verändert *(Web Defacement)*. Tatsachen werden in Medien verdreht dargestellt und Facebook-Seiten verfälscht. „Es ist leichter, einer beruhigenden Lüge zu folgen als der unbequemen Wahrheit", betonte Kozok.

IGCI in Singapur. Über die Rolle von Interpol bei der Cybercrime-Bekämpfung berichtete Dr. Thomas Herko, Assistant Director des *Interpol Global Complex for Innovation (IGCI)* in Singapur. Interpol, mit 190 Mitgliedstaaten nach den Vereinten Nationen die zweitgrößte internationale Organisation, ist keine supranationale Behörde, sondern ein *Global Faciliator,* der den einzelstaatlichen Polizeibehörden eine Plattform für den Informationsaustausch zur Verfügung stellt. Derzeit bestehen 17 Datenbanken, darunter solche für gesuchte Personen, gestohlene Fahrzeuge und gestohlene oder verlorene Reisedokumente.

Schwerpunkte des IGCI sind die Bekämpfung der organisierten Kriminalität, des Terrorismus und von Cybercrime. Von den rund 100 Mitarbeitern sind 90 für Interpol tätig, von denen 38 von den insgesamt 23 beteiligten Staaten entsendet sind.

Im „Cyber Fusion Centre" des IGCI arbeiten Vertreter von Polizeibehörden mit Wissenschaftlern und Experten aus der Privatwirtschaft zusammen, um Bedrohungen im Internet zu verfolgen, zu analysieren und Trends zu erkennen. In der Cybercrime-Investigation werden Ermittlungen zur Cyber-Kriminalität koordiniert und gemeinsame Operationen vorbereitet. Im „Digital Forensics Laboratory" wird Malware analysiert und es werden die Daten von Festplatten und Mobiltelefonen ausgelesen. Das Forschungslabor arbeitet eng mit der Privatwirtschaft, Forschungseinrichtungen und internationalen Organisationen zusammen. Die Schwerpunkte bei Cybercrime liegen derzeit bei der Erpressung mit Ransomware sowie bei Betrug durch Business-E-Mail-Compromise (BEC; auch als *CEO-Fraud* oder *Fake-President-Trick* bezeichnet). Die Schadenssumme bei dieser Betrugsart wird vom FBI weltweit mit mehr als 3,1 Milliarden US-Dollar beziffert. Durch die Aufklärungsarbeit des Fusion Centers konnten in Nigeria einschlägige Täter verhaftet werden. Ein Teil der fast einer Milliarde US-Dollar wurde sichergestellt, die im Februar 2016 von der Zentralbank von Bangladesh über Transaktionen von Hackern abgezogen worden waren. Forschungsarbeit wird auch betrieben zur Aufhellung des *Darknet* und zu Anbietern von *Crime-as-a-Service*. Schwierigkeiten liegen darin, dass sich die Cyber-Kriminalität kaum in nationalen Grenzen hält, ständig neue Technologien entwickelt werden und unterschiedliche Rechtsordnungen zu beachten sind.

Das Abwehramt des Bundesheeres stellt pro Tag etwa 15.000 *Indicators of Compromise (IoC;* „Einbruchsspuren" wie auffällige Hash-Werte, IP-Adressen, Angriffs-Tools) fest, berichtete OberstdG Mag. Walter Unger. Etwa zehn Fälle davon sind von Relevanz und erfordern spezielle Maßnahmen. Als cyberkritisch betrachtet werden „Abuses" (Missbrauchsdaten wie Schadprogramme, Phishing, Spam, Botnetze, DDos-Angriffe) sowie „Vulnerable Services" (Schwachstellen von Diensten wie DND, Mail, NTP). In diesen Fällen erfolgen Warnmeldungen. Die Herausforderungen liegen in der Erkennung und der Abwehr von unbekannten Bedrohungen, etwa fortgesetzten Angriffen (APTs) zu Spionagezwecken; in der Abwehr von auf Sabotage abzielenden DDoS-Angriffen und von Bot-Nets, die als fernsteuerbare Angriffsbasen eingesetzt werden.

Kurt Hickisch

FOTOS: KURT HICKISCH

ABWEHRAMT

Cyber Security Challenge

Zur Förderung des Nachwuchses an IT-Talenten startete das Abwehramt mit dem Verein *Cyber Security Austria* im Jahr 2012 die *Cyber Security Challenge (www.verbotengut.at)* als Wettbewerb der besten „Hacker". Der Teilnehmerkreis wurde 2013 von Schülern auf Studenten ausgedehnt. Im gleichen Jahr schloss sich die Schweiz dem Wettbewerb an, ein Jahr später Deutschland. 2015 kamen Großbritannien, Spanien und Rumänien hinzu. Das österreichische Team gewann 2015 den Wettbewerb. Bei der von der ENISA unterstützten *3. European Cyber Security Challenge 2016* in Düsseldorf waren zusätzlich Estland, Irland, Griechenland und Liechtenstein vertreten. Die Finalisten des österreichischen Teams (je zehn Schüler und Studenten) wurden während der IKT-Sicherheitskonferenz in St. Johann ermittelt. Das Team wurde am 9. November 2016 in Düsseldorf Vierter.