IKT-Sicherheitskonferenz: über 4.000 Teilnehmer an den beiden Veranstaltungstagen

Sicher im Cyber-Raum

Die IKT-Sicherheitskonferenz 2023 in Linz zeigte Schwachstellen in der Cyber-Sicherheit auf, aber auch, wie ihnen wirkungsvoll begegnet werden kann.

Bundesministerin für Landesverteidigung Klaudia Tanner wies bei der Eröffnung der am 3. und 4. Oktober 2023 in Linz vom Abwehramt des Bundesheeres organisierten IKT-Sicherheitskonferenz auf die Bedrohung der Infrastruktur durch Cyber-Angriffe hin. Diese hätten sich zu einem Angriffsmittel der Kriegsführung entwickelt. Das Bundesheer fördere die Heranbildung von IT-Spezialisten, denen an der Militärakademie eine Offizierslaufbahn eröffnet wurde.

Die Festrede zum Thema hielt Nobelpreisträger Anton Zeilinger. Neben einer kurzen Darstellung der bisherigen wissenschaftlichen Entwicklung wies er auf die wirtschaftliche und militärische Bedeutung von Quantenkommunikation und Quantenkryptografie hin, um die ein Wettstreit der Nationen entstanden sei. Abhörsichere Kommunikation über verschränkte Photonen kann mittlerweile über Satelliten erfolgen.

Die Kommerzialisierung des Weltraums *(New Space)* stellt neue Anforderungen an die Cyber-Sicherheit und -Resilienz, wie Alexander Siedschlag *(Aeronautical University Embry-Riddle)* aufzeigte. Die IT ist in Weltraumstrukturen den gleichen Problemen ausgesetzt wie terrestrische Systeme.

Die Satellitenkommunikation kann durch Hacking, Spoofing oder Jamming gestört werden. Für einen ethischen Satellitenhack *(Hack-a-Sat)* wurde im Juni 2023 ein spezieller Satellit *(cubesat)* mit nur wenigen Kommunikationsfenstern von *NASA* und *Space X* ins All geschossen. Eine der Aufgaben bestand darin, ihn zum Verlassen seines Orbits zu bringen oder seine Kamera zu hacken. Cyberspace und Space werden von der NATO (Gipfel von Vilnius 2023) als gleichwertige Operationsgebiete wie Land, Meer und Luft angesehen, bis hin zur Beistandsverpflichtung.

„Zwischen Verdun und Stardust" sah Markus Reisner die Situation im derzeitigen Krieg in der Ukraine. Die Bereitstellung von Truppen, wie dies für Durchbrüche in einem Bewegungskrieg erforderlich wäre, wird durch den satellitengestützten Einsatz von Drohnen aufgeklärt, sodass große Truppenbewegungen nicht mehr unentdeckt bleiben. Zudem werden Drohnen als Angriffswaffe eingesetzt. Entscheidend sei ihre Abwehr. Zur Informationsgewinnung werde das gesamte elektromagnetische Spektrum ausgenützt, auch im Weltraum. Ohne diesen „gehe nichts mehr".

IT-Schwachstellen. Nach einer Untersuchung von *Dreamlab Technologies (dreamlab.net)* wurden in Österreich 2023 bei etwa 1,4 Millionen aktiver Internet-Verbindungen und etwa 500.000 aktiven Domains 1,18 Millionen potenzielle Schwachstellen gefunden, deren Gefährlichkeit in etwa

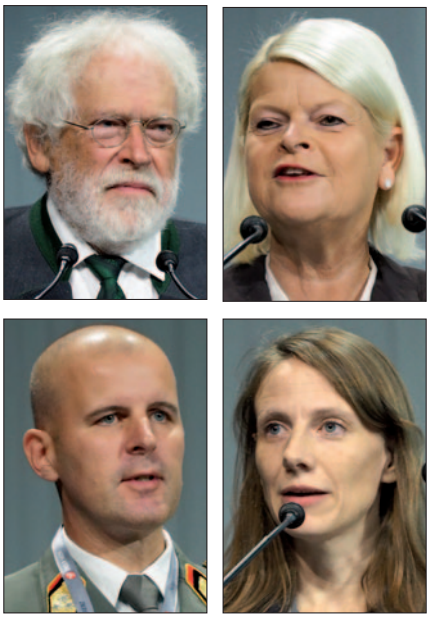
FOTO: KURT HICKISCH

370.000 Fällen als hoch und in knapp 200.000 Fällen als kritisch eingestuft wurde. Es stelle sich, so die beiden Referenten, die Frage, wer hier seinen Job nicht mache und dafür verantwortlich sei.

IT-Angriffe. Volker Kozok, *Verein Netzwerk für Cyber Intelligence e.V.,* berichtete über Deutschlands erste Cyber-Katastrophe, die sich am 6. Juli 2021 um 06.30 Uhr in der Kreisverwaltung Landkreis Anhalt-Bitterfeld, Sachsen-Anhalt, ereignete. „You are fucked", stand auf den Bildschirmen der Mitarbeiter. „Do not touch anything!" Der Angreifer, die „Grief"-Gruppe *(Grief: Gram, Trauer),* hatte die Daten mit einem AES-256-Key verschlüsselt und mit einem RSA-Public-Key verschlüsselt transportiert. Die Originaldateien wurden mit dem Zusatz .payOrgrief ergänzt. Zusätzlich wurde eine gleichnamige Datei .iwant2survive erzeugt, die zur Ransomwareseite führte. Der Lösegeldforderung von 500.000 Euro wurden die voraussichtlichen Kosten für eine Schadensbehebung von 2,5 Millionen Euro gegenübergestellt. „Pay or grief" lautete die angebotene Alternative. Zusätzlich zur Lösegeldforderung wurden auch 200 MB der Daten im TOR-Netzwerk veröffentlicht *(double Extortion* – Verschlüsselung und Erpressung mit der Veröffentlichung der Daten). Nach Ablauf des Ultimatums am 20. Juli 2021 wurden weitere 62 GB an Daten veröffentlicht.

Der Katastrophenfall wurde ausgerufen und es dauerte 206 Tage, bis er wieder aufgehoben wurde. Es sind Kosten von 2,5 Millionen Euro entstanden. Zwei Prozent der Daten gingen verloren. Alle E-Mail-Archive waren gelöscht. Dazu kommt der Reputationsverlust.

Als derzeit unter den Cyber-Bedrohungen herausragend bezeichnete Wolfgang Schwabl, *A1 Telekom Austria,* schadbringende Websites, auf die man beispielsweise durch gefälschte SMS-Nachrichten oder durch Anklicken von QR-Codes am Handy geleitet wird. Zunehmend spielt auch der Identitätsdiebstahl eine Rolle, wodurch Konten geplündert werden können. Berichte in den Medien über einen am 21. August 2023 erfolgten Ransomware-Angriff auf *A1 Telekom* fußten auf Meldungen in einschlägigen Foren und haben sich, wie Chris-



IKT-Sicherheitskonferenz: Nobelpreisträger Anton Zeilinger, Verteidigungsministerin Klaudia Tanner, Markus Reisner und Hanna Wilhelmer

toph Moser als Co-Referent im Zusammenhang mit der sich anschließenden Medienarbeit berichtete, als nicht zutreffend herausgestellt. Immerhin aber wurde bei den Nachforschungen ein schlecht abgesichertes, seit neun Jahren nicht mehr betriebenes Portal eines Subunternehmens entdeckt.

Vor dem Hintergrund, vermeidbare Schwachstellen aufzuzeigen, stellte Sebastian Schreiber, *Syss-GmbH (syss.de),* einen Live-Hacking Angriff auf smarte Thermostate vor. Weiters, mit wie wenig Aufwand man die Code-Sperre bei Krypto-USB-Drivern umgehen, Zeitungsartikel unter Umgehung der Paywall-Sperre lesen oder eine Alarmanlage ausschalten kann. Ähnlich ist das von Martin Herfurt, *IT-Wachdienst (infinite.org)* im Prinzip erläuterte Knacken eines Teslaautos. Der digitale Funkverkehr zwischen dem Fahrzeug und dem Schlüssel wird abgehört. Eine Schwachstelle in der Verschlüsselung ermöglicht dem Angreifer, auf das Fahrzeug zuzugreifen und es in Betrieb zu setzen.

Safety vs. Security. Der Begriff Sicherheit hat im Englischen zwei Bedeutungen, erläuterte Christian Flachberger, CISO *Frequentis Group (frequentis.com). Safety* (funktionale Sicherheit) wird als Vermeidung von Gefahren verstanden (z. B. Unfallverhütung), *Security* hingegen als Schutz vor Angriffen. Einmal sicher zu sein, bedeutet nicht, immer sicher zu sein. Täglich werden neue Schwachstellen aufgedeckt. Das statische Sicherheitsverständnis von *Safety* muss Gefährdungen im Sinn einer ausbalancierten Lösung einbeziehen, um das Gesamtrisiko zu minimieren.

Phishing-Angriffe sind breit gestreute und weitgehend automatisierte, in der Regel per E-Mail erfolgende Angriffe, um persönliche oder sensible Informationen zu erlangen. Eingesetzt werden Methoden des Social Engineerings, wobei sich der Angreifer als seriöse oder vertrauenswürdige Quelle ausgibt. Der Empfänger soll dazu gebracht werden, auf einen Link zu klicken oder den Anhang einer E-Mail zu öffnen. Beim *Spear-Phishing* werden mit größeren Erfolgsaussichten diese Methoden gezielt gegen eine Person oder ein Unternehmen eingesetzt, indem Vertrauensbeziehungen vorgetäuscht werden. Berichtet wurde über wissenschaftliche Untersuchungen an der Universität Innsbruck, wonach der Erfahrungsaustausch innerhalb von Gruppen zu einer messbaren Steigerung der Awareness gegenüber diesen Angriffsformen führt.

Mit dem Forschungsprojekt *Crisam AI* stellten Günther Angerbauer, *Calpana Business Consulting GmbH,* und Robert Kolmhofer, FH Oberösterreich, ein Modell der Risikoidentifikation mit *Chat-GPT* vor.

ECCC. Mit der Verordnung (EU) 2021/887 wurde das *Europäische Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cyber-Sicherheit (ECCC)* in Bukarest mit dem Ziel etabliert, einen neuen europäischen Rahmen für Unterstützung der Innovations- und Industriepolitik in der Cyber-Sicherheit zu schaffen. Hanna Wilhelmer, Bundeskanzleramt, berichtete als Projektleiterin über das auf der EU-Rechtsgrundlage errichtete *Nationale Koordinierungszentrum für Cyber-Sicherheit (NCC-AT; ncc.gv. at).* Die Innovations- und Industriepolitik im Bereich Cyber-Sicherheit stellte Dr. Thomas Stubbings, *Cyber Trust Services GmbH,* dar.

Forschung. Die bisherig gebräuchliche asymmetrische Kryptografie beruht darauf, dass es leicht ist, zwei

FOTOS: KURT HICKISCH

Finale der Cyber-Security-Challenge: Österreichs größter „Hacker-Wettbewerb“

Foto: Kurt Hickisch

Primzahlen miteinander zu multiplizieren, aber sehr schwer, das Produkt wieder in seine Primzahlen zu zerlegen (RSA-Verschlüsselung). Dem Quantencomputer stellt sich durch seine Rechenleistung diese Schwierigkeit nicht. Es wird daher für Verschlüsselungen nach quantenresistenten mathematischen Algorithmen gesucht (Post-Quanten-Kryptografie). Über die Ergebnisse dieser Forschungen berichtete Florian Silnusek vom Verteidigungsministerium.

Dirk Labudde, Hochschule Mittweida in Deutschland, stellte eine aus der Filmbranche kommende Methode vor, bei einer erweiterten, den ganzen Körper erfassenden fotogrammetrischen Erfassung eines Menschen dessen Skelett darzustellen, zu vermessen und in Bewegungsabläufen darzustellen (Skelettanimation – Rigging). Umgekehrt kann aus Bewegungsabläufen, wie sie etwa auf Videoaufnahmen von einem Banküberfall zu ersehen sind, das Skelett des Täters herausgerechnet und mit dem von Verdachtspersonen in einem nachgestellten Handlungsablauf verglichen werden.

Die akademische IKT-Ausbildung von Angehörigen des Bundesheeres erfolgte in den Jahren 2007 bis 2017 an der FH Hagenberg/OÖ im Rahmen des ASICT-Studiengangs (Akademischer Sicherheitsexperte in der Informations- und Kommunikationstechnologie). Der Studiengang war eine Erfolgsstory, die auch von Bundesministerin Tanner gewürdigt wurde. Nunmehr besteht, wie Georg Kunovjanek berichtete, seit zwei Jahren an der Theresianischen Militärakademie der Fachhochschul-Bachelorstudiengang *Militärische informations- und kommunikationstechnologische Führung (FH-BaStg Mil-OKTFü)*. Es handelt sich um eine Ausbildung zum Offizier einschließlich eines breit angelegten, anwendungsorientierten IKT-Schwerpunkts. Die beiden bisherigen Jahrgänge haben technikaffine Menschen aus den verschiedensten Berufen umfasst, darunter jeweils auch eine Frau.

In Kurzreferaten hatten Jungforscher von österreichischen Universitäten und Fachhochschulen Gelegenheit, ihre aktuellen Forschungsergebnisse vorzustellen. Veranstaltet wurde dieser *Young Researcher's Day (YRD)* von der *Österreichischen Computergesellschaft,* Arbeitskreis IT-Sicherheit, zusammen mit *SBA Research*.

Cyber-Security-Challenge. Am zweiten Veranstaltungstag fand das Finale der *Austria Cyber Security Challenge (ACSC)* statt *(verbotengut.at)*. Die 61 Teilnehmerinnen und Teilnehmer an Österreichs größtem „Hacker-Wettbewerb“ hatten in acht Stunden 20 verschiedene, für die IT-Sicherheit relevante Aufgaben zu lösen. Neben herausragenden fachlichen Qualifikationen waren auch Kreativität, Ausdauer und ein hoher Grad an Frustrations-Resistenz gefordert.

Die Siegerehrung in den Klassen Schüler, Studenten, offene Klasse/österreichische Staatsmeisterschaft fand im Rahmen eines Festbanketts statt.

80 Vorträge, 90 Aussteller. Mit über 4.000 Teilnehmern an den beiden Veranstaltungstagen ist die IKT-Sicherheitskonferenz die größte Veranstaltung ihrer Art im deutschsprachigen Raum. Vertreten waren 90 Aussteller. Über 80 Vorträge wurden gehalten. Die IKT-Sicherheitskonferenz 2024 wird, wiederum verbunden mit der *ASCS-Challenge,* am 17. und 18. September 2024 im Congress Messe Wien stattfinden. *Kurt Hickisch*