Sicherheit im Cyber-Raum

Bei der IKT-Sicherheitskonferenz 2022 des Bundesheeres wurde die Notwendigkeit der Absicherung elektronischer Systeme besonders hervorgehoben.

Die IKT-Sicherheitskonferenz des Bundesheeres fand am 14. und 15. September 2022 im *Congress Center* der *Messe Wien* statt. 2020 und 2021 hatte die ansonsten seit 2002 jährlich stattfindende, vom Abwehramt des Bundesheeres organisierte Veranstaltung, wegen der Pandemie abgesagt werden müssen.

An den beiden Veranstaltungstagen nahmen jeweils 1.700 Personen teil. Es gab 83 Vorträge, 85 Aussteller waren mit Produkten und Dienstleistungen aus dem Bereich der IKT-Sicherheit vertreten. Nach Begrüßung der Anwesenden durch den Leiter des Abwehramtes, Brigadier Reinhard Ruckenstuhl, eröffnete am ersten Tag die Bundesministerin für Landesverteidigung, Mag. Klaudia Tanner, die Konferenz, wobei die Ministerin, wie auch in einer anschließenden Pressekonferenz, die Bedeutung der Heranbildung von IT-Experten hervorhob. Die Eröffnung am zweiten Tag erfolgte durch den designierten Chef des Generalstabs, Generalmajor Rudolf Striedinger und den Staatssekretär im Finanzministerium Florian Tursky, MBA, MSc.

Einige Blöcke der Vorträge wurden entweder eingeleitet oder abgeschlossen von Kurzvorträgen *(Enlightening Talks),* in denen neun Doktoranden und Jungforscher verschiedener Universitäten, Fachhochschulen und Forschungseinrichtungen die Ergebnisse ihrer wissenschaftlichen Arbeit vorstellten. Ausgewählt wurden diese Arbeiten vom Arbeitskreis IT-Sicherheit der *Österreichischen Computer-Gesellschaft (OCG, ocg.at),* die sich ihrerseits an alle österreichischen Hochschulen mit Schwerpunkt IT- bzw. Informationssicherheit um Nominierung einschlägiger, aktueller Forschungsarbeiten gewendet hatte.

Foto: Kurt Hickisch

Teilnehmer der vom Abwehramt des BMLV organisierten IKT-Sicherheitskonferenz.

Blackout. „Vernetzung steigert die Komplexität und damit die Verwundbarkeit nicht nur der Systeme, sondern auch der Gesellschaft“, führte Herbert Saurugg, Präsident der *Österreichischen Gesellschaft für Krisenvorsorge (gfkv.at),* aus. Es treten unerwartete Rückkoppelungen auf. Aus kleinen Ursachen wie dem Ausfall von Steuerelementen könnten weitreichende Folgen entstehen; es kann zu Kettenreaktionen kommen. Betriebswirtschaftliche Optimierungen hätten zu mangelnder Diversität geführt, was sich derzeit in einer Verknappung und damit Verteuerung der Preise von Gas und Strom bemerkbar mache. Da sich bei der Stromversorgung Erzeugung und Verbrauch innerhalb enger Grenzen die Waage halten müssen, seien zum Ausgleich von Lastspitzen Gaskraftwerke und damit die Gasversorgung für die Stabilität des Stromnetzes von essenzieller Bedeutung. Eine temporäre Strommangellage für wenige Stunden wird nach Auffassung des Experten beherrschbar sein, kaum aber, wenn längerfristig zu wenig Energie zur Verfügung stehen würde. Über geplante Stromabschaltungen gebe es noch keine Erfahrungswerte. Bei totalem Stromausfall sei nach wenigen Tagen mit Ausfall der Telekommunikation und Versorgungsschwierigkeiten bis zum Kollaps von Lieferketten zu rechnen. Die Haushaltsversorgung sollte für 14 Tage reichen.

Cyber-Angriffe. Nach einer Untersuchung von Nicolas Mayencourt und Mark K. Peter vom Schweizer Unternehmen *Dreamlab* wies der österreichische Cyber-Raum zum Zeitpunkt der Präsentation 1,18 Millionen Schwachstellen auf, von denen 206.124 als kritisch und 358.887 als hoch eingestuft wurden. Es fehle weitgehend an grundlegender Cyber-Hygiene, stellten die beiden Referenten fest. „Irgendjemand macht seinen Job nicht“, betonte Mayencourt.

„Phishing-Mails sind nach wie vor das größte Einfallstor für Schadsoftware“, sagte DI Wolfgang Schwabl

vom Mobilfunkanbieter *A1*. Das Unternehmen hat für seine Mitarbeiter genaue Handlungsanweisungen *(Playbooks)* eingeführt, wie beim Auftreten dieser und anderer Bedrohungen der IT-Sicherheit vorzugehen ist. Im Einzelnen ging Schwabl auf die von einem internationalen Botnet im Mai 2021 gestartete, gegen Geräte (Smartphones, Tablets) mit *Android*-Betriebssystem gerichtete *FluBot*-Attacke ein. Es wurden, um die Empfänger neugierig zu machen, Millionen von SMS etwa über die angeblich bevorstehende Lieferung eines Pakets versendet, gefolgt von einem Link, der zum Download des Schadprogramms führt, das Kreditkarteninformationen und Zugangsdaten zum Online-Banking des Opfers ausspäht. Durch internationale Zusammenarbeit wurde das Netz zerschlagen, doch kursieren immer noch derartige SMS.

Ein einer Bestellung beigefügter Gewerbeschein ist noch keine Bestätigung dafür, dass das angebliche Unternehmen tatsächlich existiert. Vorsicht ist auch geboten bei Mails, wonach die Kontonummer des Unternehmens geändert worden sei. Selbst wenn das Erscheinungsbild der Mail vertraut aussieht – der Webauftritt könnte nachgebaut sein. Es sollte auf firmenmäßiger Zeichnung solcher Mitteilungen bestanden werden.

Es geht sogar so weit, dass Webauftritte von Banken nachgebaut werden, mit Mailadressen, die sich nur geringfügig von denen bestehender Institute unterscheiden. Diese gefakten Seiten werden ins Internet gestellt. Da die Reihung in Suchmaschinen von der Anzahl der Aufrufe abhängt, werden durch gesteuerte gleichartige Aufrufe diese Seiten an die erste Stelle gepusht. Dem flüchtigen User, der sich nach Möglichkeiten des Online-Bankings umsehen will, springen sie als erstes ins Auge.

Als allgemein einzuhaltende Vorsichtsmaßnahmen sind zumindest 14-stellige Passwörter zu empfehlen, unter Einschluss von Umlauten, Groß- und Kleinschreibung sowie Zahlen und Sonderzeichen. Abgegangen ist man bei *A1* davon, einen periodischen Wechsel von Passwörtern vorzuschreiben. Dies hat sich als nicht ökonomisch erwiesen, da immer wieder, besonders bei Benutzung mehrerer Geräte, Fristen für die Ummeldung übersehen wurden und Logins nach Fristablauf nicht mehr möglich waren. Verlangt wird aber eine Multifaktor-Identifikation der Mitarbeiter. Unabdingbar ist eine vollständige und aktuelle Übersicht über die vorhandene Hard- und Software, wobei diese auf dem letzten Stand zu halten ist *(„Patch me, if you can")*.

Data Loss Prevention (DLP), Logfile-Analysen *(SIEM)* sowie die Einrichtung eines *Security Operations Center (SOC)* sind weitere zu ergreifende Maßnahmen. Über allen technischen und organisatorischen Maßnahmen steht aber der Grundsatz „be prepared".

Fakes. Marco Di Filippo zeigte die vielfältigen Möglichkeiten des Phishings auf, also sich, mit welchen Absichten auch immer, in einer elektronischen Kommunikation als vertrauenswürdiger Partner auszugeben. Beispielsweise durch Mails, deren Absender auf den ersten Blick unbedenklich erscheint. Dem flüchtigen Betrachter wird der Unterschied zwischen „telekom.com" und „telekom.com" nicht auffallen, auch nicht zwischen „zoom.in" und „z00m.in", doch handelt es

Referenten bei der IKT-Sicherheitskonferenz 2022 in Wien: Verteidigungsministerin Klaudia Tanner, Staatssekretär Florian Tursky, Generalstabschef Rudolf Striedinger, Oberst Markus Reisner (BMLV), Resilienz-Experte Herbert Saurugg, IT-Sicherheitsexperten Marco di Filippo, Volker Kozok und Wolfgang Schwabl.

sich hiebei um verschiedene Domänen. Ganz einfach wird es, jemanden, sei es aus Jux oder böser Absicht, auf eine gewünschte Website zu bringen, indem man deren QR-Code durch massenhaft verteilte Aufkleber mit Aufforderungen wie „Scan me“ oder „Add me“ unter die Leute bringt.

Wie gefährlich USB-Sticks hinsichtlich der Ausspähung von Daten sein können, zeigte Di Filippo an Hand des *Rubber Ducky* auf, der eine MicroSD entsprechenden Speichervolumens enthält. Die mit dem gedankenlosen Anstecken von USB-Sticks verbundenen Gefahren scheinen sich allerdings bereits herumgesprochen zu haben. Bezeichnenderweise wurden bei keinem der Aussteller USB-Sticks mit darauf enthaltenem Werbematerial angeboten. Vorsicht ist geboten, wenn Bewerbungsschreiben USB-Sticks beigelegt sind.

In weiterer Folge ging Di Filippo auf die Manipulation von Medieninhalten (Audio, Bild, Video) unter Einsatz von künstlicher Intelligenz ein *(Deep-Phishing)*. Beim *Video-Fake* wird die Segmentierungsmaske, die aus 26 miteinander in geometrischer Verbindung stehenden Punkten besteht, über das Referenzbild gelegt. Die Daten der Maske werden auf das zu manipulierende Bild gelegt. In ähnlicher Weise wird mit Audio-Dateien verfahren. Die Tonquelle wird mit Daten aus einer Datenbank zu einer synthetischen Sprache umgeformt und mit Text überlagert, sodass eine Audiosequenz generiert wird. Sowohl für die Verfälschung von Sprache als auch von Videos gibt es frei verfügbare Tools. Videodaten können beispielsweise aus Videoanrufen oder -konferenzen gewonnen werden.

Um Videofakes zu erkennen, muss man auf Details und Artefakte achten. Es ist beispielsweise schwierig, Zähne darzustellen oder Haare. Brillenfassungen können unterschiedlich abgerundet sein. Die Fake-Technik stößt zwar auf technische Grenzen wie Unschärfen, mangelnde Bandbreite, Störgeräusche, doch ist hier durch die schlechte Qualität von Videokonferenzen schon ein gewisser Gewöhnungseffekt eingetreten. Zur Echtheitsprüfung könnte man als Softwarelösung digitale Wasserzeichen einsetzen oder festgelegte Verifizierungsprozesse über einen separaten Kanal; oder man ersucht den angeblichen Gesprächspartner, die Hand vor dem Gesicht zu bewegen.

Über die Abwehr von Cyber-Angriffen unter Gefechtsbedingungen berichtete DI Florian Silnusek, Bundesministerium für Landesverteidigung (BMLV). Bei der Übung *Locked Shields 2022* waren die 25 *Blue-Teams* aus mehr als 35 Nationen zwei Tage lang mehr als 8.100 Attacken von 90 *Red-Teams* ausgesetzt. Über 2.000 Cyber-Experten aus aller Welt waren eingebunden.

Cyber War. Oberst Markus Reisner (BMLV) bezeichnete den Krieg in der Ukraine als Abnützungskrieg. Kriege dieser Art würden fast nicht an der Front, sondern im Hinterland entschieden, inwieweit also die jeweilige Bevölkerung noch bereit sei, die Kriegsziele mitzutragen. Aus dieser Sicht seien die Maßnahmen gegen die Ukraine und sie unterstützende Staaten zu sehen, die durch die Bedienung von Ängsten (Nahrungsmittelknappheit, Nuklearkatastrophen, ökonomischer Kollaps) diesen Widerstandswillen zu untergraben suchen würden. Auf der anderen Seite stehe eine im Wesentlichen abgeschottete, informationsmäßig gleichgeschaltete Gesellschaft.

Hybrid-Warfare. Wie sich der Krieg in der Ukraine im Cyberspace widerspiegelt, schilderte Volker Kozok. Altbekannte russische Hackergruppen wie *APT 28, Fancy Bears, Killnet* und *Nobelium* greifen auf ihren jeweiligen Spezialgebieten ukrainische Cyber-Ziele wie Infrastruktureinrichtungen an. In umgekehrter Weise agieren ukrainische Gruppierungen.

Sogar die Cyber-Kriminalität hat sich durch den Krieg in zwei einander feindlich gegenüberstehende Gruppen aufgespalten. Die Frage sei, ob die westliche Welt genügend Resilienz gegen den russischen Informationskrieg habe; ob sie *Hybrid Warfare* „könne“ und welche Optionen sie im Cyber-Raum habe. Wie könnten Menschen erreicht werden, die keinen Zugang zum freien Internet hätten, und man müsse sich die Frage stellen, ob wir die Narrative beherrschen oder diese uns.

„Nicht jeder Portscan ist gleich ein Angriff und nicht jeder Cyber-Angriff ein Cyberwar“, rückte Manuel Atug, Datenschutzexperte des *Chaos Computer Club*, Begrifflichkeiten zurecht. Zwar seien Cyber-Operationen wie Desinformation über soziale Medien *(Fake News)*, Spionage, Veränderungen von regierungseigenen Websites *(Defacement)*, Beeinträchtigung der Führungsfähigkeit, Blockade des nationalen Zugangs zum Internet Bestandteil einer hybriden Kriegsführung im Bereich Aufklärung und Wirkung, aber noch kein Cyber War. Im Cyber-Raum würden sich Militär und Zivilgesellschaft, Kriminelle und Destruktive; Kritische Infrastrukturen, Wirtschaft, Wissenschaft und Forschung, bewegen.

Die beste Absicherung sei Cyber-Resilienz, die Angriffe durch Basis-Maßnahmen wirkungslos verpuffen lassen würde. Im Alltag seien derartige Vorkehrungen aber häufig nicht oder nur unzureichend vorhanden.

Die *IKT-Sicherheitskonferenz 2023* und die Cyber Security Challenges 2023 werden am 4. und 5. Oktober 2023 in Linz stattfinden.

Kurt Hickisch

bundesheer.at
verbotengut.at

FOTOS: KURT HICKISCH