Gefahren, Schwachpunkte, Schutz

Sicherheit der kritischen Infrastruktur, Cyber-Angriffe, Wirtschaftsspionage, Krisenkommunikation und -vorsorge waren unter anderem Themen beim 10. D-A-CH–Sicherheitsforum in Tirol.

Etwa 70 Teilnehmer aus der Wirtschaft, der Sicherheitsbranche, dem Banken- und Versicherungswesen, der Forschung und der Landesverteidigung nahmen am 14. und 15. November 2023 beim *Stanglwirt* in Going in Tirol an dem von der *Simedia GmbH (simedia.de)* veranstalteten *D-A-CH-Sicherheitsforum* teil. Moderiert wurde die Veranstaltung von Teresa Mayerhofer, *VASBÖ (vasboe.at),* und Peter Stürmann, *Simedia*.

10. D-A-CH–Sicherheitsforum in Tirol: Schutz und Sicherheit in der Informations- und Kommunikationstechnik.

Informationssicherheit.
Manuel „HonkHase“ Atug, Gründer und Sprecher der *Arbeitsgruppe kritische Infrastruktur (AG KRITIS; ag.kritis.info),* stellte dar, wie es um die Sicherheit der kritischen Infrastruktur steht. In rechtlicher Hinsicht ist auf EU-Ebene vom Cyber-Security-Act auszugehen, von dem sich, was die physische Sicherheit betrifft, die RCE-CER-Richtlinie und, auf IT-Ebene, die NIS-2-Richtlinie ableiten. Als nationale Ausführungsgesetze sind in Deutschland das KRITIS-Dachgesetz und das NIS-2- Umsetzungsgesetz in Arbeit, beide terminisiert mit Oktober 2024. Die kritische Infrastruktur ist in Deutschland auf zehn Sektoren aufgeteilt.

Die Schwachpunkte der Steuerung von physischen Prozessen *(Operational Technology; OT)* liegen darin, dass diese seit Jahrzehnten unverändert in Betrieb ist. Als Beispiel führte Atug das Ergebnis der Untersuchungen nach einem im Februar 2021 (möglicherweise auch nur vermeintlichen; Anm.) Cyber-Angriff auf das Wasseraufbereitungswerk Oldsmar in der Nähe von Tampa, Florida, an. Das Wasser wäre durch übermäßigen Zusatz von Natronlauge vergiftet worden. Es stellte sich heraus, dass das Passwort für die in Fernwartung betriebene Anlage allseits bekannt war; *mit Windows 7* ein Betriebssystem verwendet wurde, für das kein Support mehr bestand; der Fernzugriff ohne Firewall dazwischen erfolgen konnte und in Betrieb war, obwohl ein Operator anwesend war.

Den typischen Ablauf von Ransomware-Angriffen schilderte Atug so, dass die Schadsoftware entweder über E-Mail mit Verweis auf einen Link oder als Anhang zu einer Mail in das Netz des Opfers gelangt. Durch jeweiliges Anklicken wird zunächst ein *Dropper* geladen, der die Zugänge eröffnet. Durch die nachgeladene Ransomware kommt es zur Verschlüsselung der Daten und Lösegeldforderung. Ungepatchte, im Internet erreichbare Systeme werden von einem *Initial Access Broker (IAB)* kompromittiert. Der dadurch eröffnete Zugang wird an eine Ransomware-Gruppe verkauft, die sich ihrerseits eines Ransomware-as-a-Service-Dienstleisters bedient, mit dem eine Gewinnbeteiligung um die 20 Prozent vereinbart wird.

„Für die Bevölkerung ist nicht relevant, was die Ursache für eine Katastrophe ist“, meinte Atug. „Cyber-Resilienz herbeizuführen, ist Menschenschutz.“ Der deutschen *Bundesanstalt Technisches Hilfswerk (THW),* einer Zivil- und Katastrophenschutzorganisation, stellte er die Idee eines *Cyber-Hilfswerks (CHW)* zur Seite, das die bestehenden Bewältigungskapazitäten für Großschadenslagen durch Cyber-Vorfälle bei kritischen Infrastrukturen kooperativ ergänzen solle.

Es ist keine Schwäche, einen Ransomware-Angriff einzugestehen, meinte Marc Ziegler, CEO der Schweizer *Auto AG Group,* denn die Frage sei nicht, ob man angriffen wird, sondern bloß, wann das erfolgt. Viel wichtiger ist, wie auf einen Angriff reagiert wird und wie schnell das Problem behoben wird. Im Fall der *Auto AG* wurde an einem Montagmorgen festgestellt, dass die Systeme größtenteils nicht mehr funktionierten und viele Daten verschlüsselt wurden. Auf einer „txt-Datei“ fand sich eine Aufforderung der Erpresser, dass sich das Unternehmen bei ihnen melden solle. Es wurden Beweise geliefert, dass Systeme ausspioniert wurden. Auch wurden Versuche festgestellt, Backups zu kompromittieren und/oder zu löschen.

Das Unternehmen setzte sofort Polizei, Staatsanwaltschaft und das Schweizer Cyber-Security-Center in Kenntnis. Es wurde ein Krisenstab gebildet, auf manuellen Betrieb umgestellt, mit Nutzung privater Mails und von *WhatsApp*. Nach Kontaktaufnahme mit den Erpressern wurden die Möglichkeiten evaluiert und mit Polizei und Staatsanwaltschaft besprochen. Letztlich wurde eine spezialisierte Firma beigezogen, die die Daten nach 36 Stunden ohne Datenverluste wiederherstellen konnte. Nach sechs Tagen konnte das Unternehmen wieder online gehen – auch dank des engagierten Einsatzes aller Mitarbeiter, wie betont wurde. Es waren 800 Stunden Nacherfassungsaufwand erforderlich. Der finanzielle Schaden war relativ gering.

Zum Nutzen einer Cyber-Versicherung führte Ziegler aus, dass diese in der Regel nur die finanziellen Folgen eines Angriffs abdeckt und als Erweiterung einer Betriebsunterbrechungsversicherung zu verstehen sei. Allfällige Schadenersatzforderungen Dritter könnten gedeckt werden. Den Schaden durch Cyber-Kriminalität bezifferte der Referent mit 250 bis 350 Milliarden Euro

Foto: Kurt Hickisch

Referenten beim Sicherheitsforum: Kira Vinke, Frank Ewald, Walter Unger, Manuel Atug, Roman Hahslinger, Silvio Buchholz

pro Jahr, bei hoher Dunkelziffer. Dem *Nationalen CSC* der Schweiz seien im ersten Halbjahr 2023 19.048 Cyber-Vorfälle gemeldet worden. Cyber-Kriminalität überschreite territoriale Grenzen, in einem hochdynamischen Prozess mit kurzen Innovationzyklen. Die Strafverfolgung werde besser, habe aber noch einen langen Weg vor sich.

Angriffe im Cyber-Raum. Wie die Schlacht um die Ukraine auch im Cyber-Raum geführt wird und mit welchen Angriffsarten auch außerhalb kriegerischer Auseinandersetzungen gerechnet werden muss, zeigte Walter Unger, Leiter der Abteilung Cyber-Defence & IKT-Sicherheit des österreichischen Bundesheeres, auf. In sozialen Medien werden zur Manipulation der User Fake News verbreitet, Websites werden verändert *(Defacement)*. *Whiper-Gate*-Angriffe, wie sie im Jänner 2022 auf Regierungsstellen der Ukraine durchgeführt wurden, hatten rein destruktiven Charakter; Daten wurden unwiederbringlich gelöscht. DDos-Attacken legten Rechner durch gezielte Überforderung lahm. Am 24. Februar 2022 wurde das Satellitensystem *KA-Sat* und damit das *ViaSat*-Netzwerk lahmgelegt. Bereits bekannte Hacktivisten wurden zu Kriegsteilnehmern.

Grundsatz der Cyber-Verteidigung ist, die Angriffsfläche zu reduzieren und die Verteidigung zu automatisieren. Es gilt, Zugriffsmöglichkeiten zu minimieren, regelmäßig Backups anzulegen und Updates unverzüglich durchzuführen. *Intrusion Detection-Management Systeme (IDMS)* erkennen Malware und blockieren sie. Berechtigungen für Nutzer sollten auf ein Minimum reduziert und unbekannte oder nicht mehr verwendete Nutzerkonten gelöscht werden. Im Krisenreaktionsteam sollten Krisenlagen geübt und Sicherheitsverfahren getestet werden. Prinzipiell gilt, möglichst wenig persönliche Daten ins Netz zu stellen, Zwei-Faktor Authentifizierung oder einen Passwort-Manager einzusetzen und Mails von Unbekannten nur in der Text-Vorschau anzusehen. Faktenchecker-Websites wie etwa *Mimikama (mimikama.at)* oder *APA-Faktencheck* unterstützen bei der Aufdeckung von Fake News. Bilder und Videos können mit einer Rückwärtssuche überprüft werden.

Large Language Models (LLM) sind laut Frank Ewald, Leiter Konzernsicherheit *Deutsche Post DHL,* Modelle der KI, die auf künstlichen neuronalen Netzen (KNN) aufbauen und Anwendungen wie *Chat-GPT* zugrunde liegen. LLMs werden nicht auf bestimmte Fähigkeiten spezialisiert, sondern entwickeln sie mit zunehmender Komplexität. Es kann, anders als bei regelbasierten und statistischen Systemen, nicht sicher vorausgesagt werden, wann welche Fähigkeit erworben wird. Das schafft neue und verändert bekannte Bedrohungsbilder und ermöglicht die Automatisierung bekannter Bedrohungsszenarien. Es wird immer schwieriger, echten Content (Text, Bilder, Ton) von KI-generiertem Inhalt zu unterscheiden, was etwa zu hochautomatisiertem und personalisierten Betrug wie CEO-Fraud oder (Spear-)Phishing eingesetzt werden kann. Mit Hilfe generativer KI können Fake News erzeugt und zur Stimmungsmache beispielsweise in Online-Foren eingesetzt werden. Umgekehrt kann aber auch die generative KI so manipuliert werden, dass sie ihren Nutzern Schaden zufügt. Je ähnlicher die Kommunikation mit der KI der mit anderen Menschen wird, umso mehr projizieren Menschen menschliche Eigenschaften in die Systeme („Eliza-Effekt"), die zu psychischen Abhängigkeiten führen können. Chatbots mit KI können zu ultimativen Echokammern werden, was zu Radikalisierung führen kann. Es besteht die Gefahr, dass sich ohne menschliche Kontrolle bei in Endlosschleifen arbeitenden Systemen Fehler potenzieren.

Wirtschaftsspionage. „Informationsdiebe kommen auf leisen Sohlen" sagte Helmut Müller-Enbergs und meinte damit die Tätigkeit ausländischer Nachrichtendienste auf dem Gebiet der Wirtschaftsspionage. Es geht diesen darum, sich den Besitz von Know-how (Patente, Muster, Verfahren) zu verschaffen, um eigene Forschungsgelder einzusparen. Eine Methode sei, über Schwachstellen und durch Fehler von Mitarbeitern in IT-Systeme einzudringen. Derartige Angriffe würden lange unbemerkt bleiben, das Entdeckungsrisiko sei gering. Die Beseitigung der Schäden sei personal- und kostenintensiv, was eine Schwächung des angegriffenen Unternehmens zur Folge habe.

Von Wirtschaftsspionage betreibenden Staaten könnten auch eigene Unternehmen gegründet werden mit dem Ziel, durch Teilnahme am Wirtschaftsleben des angegriffenen Staates in den Besitz von relevanten Informationen zu kommen, oder, durch den Kauf von oder Einkauf in bestehende Unternehmen, sich deren Know-how zu verschaffen. Die „Hohe Schule" der Wirtschaftsspionage sei es, qualifizierte Agenten so auszubilden und mit perfekt gefälschten Identitäten und Lebensläufen auszustatten, dass sie direkt in Forschungsabteilungen eingeschleust werden können.

Holger Heyn, Konzern-Beauftragter Wirtschaftsschutz, *Volkswagen AG,* schilderte am Beispiel der *CARIAD SE (Cariad-Technology)* den Aufbau einer Security-Organisation in einem Software-Unternehmen, dessen Aufgabe die Entwicklung einer einheitlichen Elektronik und IT-Plattform für alle Marken und Standorte des Volkswagen-Konzerns ist. Was Objektschutz, Ausweise und Zutrittskontrolle betrifft, wurde das Konzept „One-ID–Everybody–Every-

FOTOS: KURT HICKISCH

where“ in Form eines standardisierten Zutrittssystems eingerichtet. Zum richtigen Verhalten beim Prototypenschutz wurde Online-Training eingesetzt. Prozesse zum Abschluss von Geheimhaltungsvereinbarungen bzw. *Non-Disclosure-Agreements (NDA)* wurden digital unterstützt aufgebaut und ein digitales Incident-Management-System aufgebaut. „Es braucht Mut, Prozesse neu zu gestalten“, meinte Heyn.

Ein allumfassendes Hightech-Sicherheitskonzept für ein stark gefährdetes Tourismus-Großprojekt im Nahen Osten stellte Christoph Eichel, CEO *Solitaire Advisory GmbH,* vor.

Krisen und Kommunikation. Am 7. Juni 2023 kam es nach der Einfahrt eines Autoreisezuges *(Nightjet)* in dem 15 km langen Terfnertunnel in Tirol zu einem Brand bei den verladenen Fahrzeugen, nachdem das geöffnete Aufstelldach eines verladenen Fahrzeugs die Oberleitung beschädigt hatte. 151 Fahrgäste wurden aus dem Zug evakuiert.

Auf diesem Vorfall aufbauend, erläuterte Roman Hahslinger, Leiter Konzernsicherheit *ÖBB,* Grundsätze der Krisenkommunikation. Es gilt, ein Risiko zu erkennen, dessen Krisenpotenzial abzuschätzen und rechtzeitig eine aktive Informationspolitik aufzusetzen. Wird eine Krise nicht frühzeitig selbst erkannt, erkennen sie andere; die Deutungshoheit geht verloren. Es kommt zu Fehleinschätzungen, Gerüchten, Vermutungen, Spekulationen, was nur schwer wieder in geordnete Bahnen zu bringen ist, schon gar nicht unter Zeitdruck. Krisenkommunikation soll informieren, eine Vertrauensbasis schaffen, Verunsicherung vermeiden, Gerüchten vorbeugen und Schaden für Image und Geschäftstätigkeit hintanhalten. Sicherzustellen ist, dass ausschließlich der Krisensprecher nach außen kommuniziert. Für die Opfer soll Verständnis aufgebracht werden; ihre Persönlichkeitsrechte sind zu schützen. Letztlich soll eine gute Ausgangssituation für die Aufbauarbeit geschaffen werden.

Als häufig vorkommende Fehler bezeichnete der Referent, den Kopf in den Sand zu stecken, nicht oder zu spät zu reagieren und zu vertuschen, zu lügen oder zu verheimlichen, Medien oder andere Kritiker anzugreifen, Gegendarstellungen zu verlangen, die Krise herunterzuspielen oder die Schuld auf andere abzuwälzen. Wichtig sei, auf das Gegenüber einzugehen („Wir sind über

Teresa Mayerhofer (VASBÖ) und Astrid Mair, Tiroler Landesrätin für Sicherheit

den Vorfall informiert“, „Derzeit können wir noch keine Informationen über Details geben“, „Wir sind gerade dabei, gesicherte Informationen einzuholen, melden uns verlässlich bei Ihnen; hinterlassen Sie bitte Ihre Kontaktdaten“). Mit jeder Zielgruppe (Öffentlichkeit, Medien, Angehörige, Mitarbeiter, Kunden, …) sollte nach ihren Bedürfnissen kommuniziert werden.

Krisenvorsorge. Am Beispiel des Tiroler Zivil- und Katastrophenschutzes stellte Astrid Mair, Landesrätin für Sicherheit der Tiroler Landesregierung, die im Bundesland Tirol für den Fall einer bis zu einem Blackout reichenden Strommangellage ergriffenen Maßnahmen vor, unter Betonung der Rolle von Public-Private-Partnership. Ein Blackout betrifft alle und alles, Flug-, Bahn- und Straßenverkehr (Ausfall von Straßenbeleuchtung, Ampeln). Kommunikationsmöglichkeiten sind massiv eingeschränkt, die Wasser-, Lebensmittel- und Treibstoffversorgung ist beeinträchtigt. Es ist vorgesorgt, dass das behördliche Digitalfunknetz mit seinen notstromversorgten Sendemasten eingesetzt wird. Es bestehen Netzwiederaufbaukonzepte; von „Strominseln“ ausgehend, erfolgt eine schrittweise Zusammenschaltung. Für die Gemeinden wurden „Blackout-Leitfäden“ entwickelt, die auf Gemeindeebene die Versorgung der Bevölkerung mit Information, Wasser, Lebensmitteln, Treibstoff sicherstellen sollen und Ratschläge für die Haushalte enthalten, krisensichere Vorräte an Lebensmittel, Medizin, Hygiene und Energie (Brennmaterial, Gaskocher …) anzulegen. Ferner werden Schulungen und Übungen angeboten

Methoden zur Sicherheitsberatung unter Einsatz von *Building-Information-Modelling (BIM)* stellte Silvio Buchholz, *Drees & Sommer,* vor. Baupläne werden digital in 3D-ähnliche Strukturen umgesetzt, die es erlauben, Gänge und Räume virtuell zu begehen und sicherheitstechnische Anforderungen einzuplanen.

Über erste Erfahrungen mit dem deutschen Hinweisgeberschutzgesetz berichtete Rechtsanwalt Rainer Bucher von Buchert-Jacob-Partner-Rechtsanwälte.

Dass der Klimawandel ein globales Sicherheitsproblem bedeutet, zeigte Kira Vinke, Leiterin des *Zentrums für Klima- und Außenpolitik* der *Deutschen Gesellschaft für auswärtige Politik,* auf.

Betroffen stimmte der Bericht des deutschen Entwicklungshelfers Jörg Lange, der im Zuge seiner Tätigkeit im April 2018 im Grenzgebiet von Mali und Niger bei einem Hinterhalt von dschihadistischen Terroristen verschleppt und 1.702 Tage in Geiselhaft gehalten wurde. Der studierte Theologe und Wasserbauingenieur schilderte die von latenter Todesangst geprägten Umstände seiner Haft und den menschenverachtenden, keinen rationalen Argumenten zugänglichen Fanatismus der Terroristen. *Kurt Hickisch*

FOTO: KURT HICKISCH