

Vernetzte Sicherheit

In Vorträgen, Diskussionen und Workshops wurden am 25. und 26. November 2025 bei der Fachmesse Protekt 2025 in Leipzig Themen des Schutzes der kritischen Infrastruktur erörtert.

Das Konferenzprogramm der Fachmesse *Protekt* war in sieben Vortragsstränge unterteilt, speziell zu Cyber- und Informationssicherheit sowie physischem Schutz. Weitere Vortragsstränge befassten sich mit Praxisberichten aus der *Unabhängigen Partnerschaft (UP) KRITIS*, dem Thema KRITIS und ziviler Verteidigung und mit der Vermittlung neuer gesetzlicher Grundlagen für KRITIS-Betreiber und deren Mitarbeitende.



Fraunhofer-Lernlabor zum Thema Cyber-Sicherheit

Sicherheitslage. Der Sächsische Staatsminister des Innern, Armin Schuster wies auf in letzter Zeit erfolgte Naturkatastrophen wie Waldbrände und Überschwemmungen hin sowie auf Stromausfälle und Anschläge im Zuge einer hybriden Kriegsführung, die zeigen würden, dass man sich zwar nicht im Krieg, aber auch nicht mehr im Frieden befinde – eine Lage, die das Grundgesetz nicht kenne. Neben staatlichen Maßnahmen müsste auch in der Bevölkerung ein Bewusstsein zu Eigenverantwortung und Selbstschutz geschaffen werden.

„Gefährdungen der KRITIS, nachrichtendienstliche Aktivitäten, Desinformationskampagnen, Cyber-Angriffe, stellen Bedrohungen dar, die nicht mehr in das klassische Bild der militärischen Konfrontation passen“, führte Christoph Hübner, stv. Leiter der Abteilung Krisenmanagement und Bevölkerungsschutz, Bundesministerium des Innern (BMI), aus. Bedrohungen gegen die zivile und militärische Verteidigung seien in den Blickpunkt gerückt. Zivile Verteidigung sei eine gesamtgesellschaftliche Aufgabe. Dazu gehöre auch der Schutz der Lieferketten.

In der anschließenden Podiumsdiskussion zur „Allgemeinen Sicherheitslage in Deutschland“ berichtete die Präsidentin des Technischen Hilfswerks (THW), Sabine Lackner, von Angriffen auf E-Mail-Accounts und Überflügen von Drohnen über Einrichtungen des Hilfswerks. Die Präsidentin des Bundesamts für Sicherheit in der Informati-

onstechnik (BSI), Claudia Platter, sah ihre Behörde verstärkt Spionage-Angriffen ausgesetzt. Peter Lauwe, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), wies auf das wachsende Interesse der Bürger an Vorsorgemaßnahmen hin. Betont wurde von allen aber, dass man nicht von null beginnen müsse, sondern auf Vorhandenem aufbauen könne.

Kapitän zur See Frank Fähnrich, Territoriales Führungskommando der Bundeswehr, berichtete über 2025 erfolgte Drohnensichtungen und Cyber-Angriffe, Anschläge auf Umspannwerke, Bahnstrecken und -tunnel sowie Beschädigungen von Meereskabeln. In Quantität und Qualität würden diese hybriden Aktivitäten zunehmen. Es seien Low-Level-Agents (abschätzig „Wegwerf-Agenten“) im Einsatz, die für Handgeld und ohne zu wissen, worum es geht, Päckchen verbringen oder Zäune durchschneiden. Gesellschaft und KRITIS müssten robust, redundant und agil aufgestellt werden. Man müsse im Sinn eines Lagebildes in Zusammenhängen denken und dürfe beispielsweise die durch einen Bagger zerstörten Lichtwellenleiter und den genau unter einer mit Kabeltrassen versehenen Eisenbahnbrücke brennenden Lkw nicht isoliert sehen.

Gerlinde Niehus, Expertin für NATO- und internationale Sicherheitspolitik, stellte die Situation einer im Entstehen begriffenen multipolaren Weltordnung dar. Seit 2014 gebe es in

Europa keinen Frieden mehr. Europa müsse sich neu positionieren und seine Sicherheit selbst in die Hand nehmen.

In der anschließenden Podiumsdiskussion wurde deutlich, dass sich die Spionagetätigkeit sowohl in ihren Zielen als auch bei ihren Mitteln verändert hat. Die klassische, auf Gewinnung von Know-how gerichtete Wirtschaftsspionage wird erweitert durch Spionage, die auf Zerstörung ausgerichtet ist und sich gegen Einrichtungen der KRITIS richtet, wie etwa Umspannwerke, Wasserversorgung, Talssperren. Dazu kommt die Abhängigkeit von digitalen Technologien, die von Unternehmen bezogen werden, die ihren Sitz nicht in Europa haben.

Gegenmaßnahmen. Wenn das Internet ohne terrestrische Infrastruktur nicht mehr funktioniert und, aus welchen Gründen auch immer, die üblicherweise über die *Starlink*-Satelliten erfolgende Satelliten-Kommunikation ausfallen sollte (Schwarzfall), stehen noch die Systeme *Inmarsat*, *One-Web* und *Iridium* zur Verfügung, führte Hubert Einetter, *GESAT GmbH*, aus. Diese Systeme kommunizieren allerdings nicht untereinander. Es gibt auch nicht so etwas wie ein übergreifendes Telefonbuch. Als Lösung stellte das Unternehmen das *Redcom*-Messengersystem als Kontaktverzeichnis vor, bei dem jeder Nutzer seine eigenen Kontaktdaten einpflegt, mit der Möglichkeit einer Chatfunktion auch mit mehreren Teilnehmern. Der entsprechende Server ist besonders abgesichert.

Nach in letzter Zeit aufgetauchten Meldungen wurden durch hybride Angriffe das Navigationssystem von Schiffen und Flugzeugen gestört. Betroffen davon war unter anderem das Flugzeug der EU-Kommissionspräsidentin auf einem Flug nach Bulgarien. Das üblicherweise zur Positionsbestimmung verwendete *Global Positioning System (GPS)* wurde, wie Lukas Sökefeld, Certified Ethical Hacker, ausführte, in den 1970er-Jahren vom US-Verteidigungs-

ministerium entwickelt und ist seit 1995 offiziell in Betrieb. Es sind etwa 30 Satelliten im Einsatz, die Signale mit ihrer Position und Zeit übermitteln. Das GPS-Gerät muss zur Positionsbestimmung die Signale von mindestens vier Satelliten empfangen, misst, wie lange jedes Signal gebraucht hat, um anzukommen, und ermittelt daraus die Position im zivilen Bereich mit einer Genauigkeit von etwa 7 m. Die auf 1575,42 MHz gesendeten Signale können überdeckt und dadurch falsche Positionsangaben erzeugt werden. Für ein engeres Umfeld reichen dazu Geräte aus der Hacker-Szene. Plötzliche Sprünge in der Ortsbestimmung und ungewöhnliche Signalstärke sind Anzeichen, dass ein derartiges Gerät im Einsatz ist. Als Gegenmaßnahme kann auf Galileo, die europäische Alternative zu GPS, zurückgegriffen werden, die, als Spoofing-Schutz, eine Authentifizierung erfordert.

Marcel Kühne, *Fraunhofer IOSB*, stellte unter dem Titel „Hack the Grid“, ein physisches Lernlabor zum Thema Cyber-Sicherheit für Energie- und Wasser/Abwasserversorgung vor. An diesem Modell einer Anlage können durch



Sachsens Innenminister Armin Schuster und Gerlinde Niehus, Expertin für internationale Sicherheitspolitik

Abbildung realer Prozesse Situationen realitätsnahe dargestellt und ihre Bewältigung geübt werden. Mit Elementen der Gamification, verbunden mit Wettbewerb und Belohnung, kann der Lernerfolg gesteigert werden.

Rechtsanwältin Nina Naske erläuterte an Hand der Verordnung (EU) 2019/945 über unbemannte Luftfahrtsysteme, Möglichkeiten zur Aufklärung und Abwehr von Drohnen, wobei sich zeigte, dass enge Grenzen gesetzt sind. Die von den Drohnen ausgesendeten (verschlüsselten) Signale abzufangen, fällt unter Ausspähen bzw. Abfangen von Daten (§ 202a und 202b dStGB).

Die Drohne rechtswidrig zu beschädigen oder zu zerstören, fällt unter Sachbeschädigung (§ 303 dStGB) bzw., wenn eine Datenverarbeitungsanlage oder ein Datenträger zerstört oder beschädigt wird, unter Computersabotage (§ 303b dStGB). Sich die tatsächliche Gewalt über eine (Kriegswaffen-)Drohne zu verschaffen, fällt in Deutschland unter das Kriegswaffenkontrollgesetz. Außerhalb einer genehmigten Schießstätte darf in Deutschland mit einer Schusswaffe ohne Schießerlaubnis nicht geschossen werden. Ausnahmen bestehen für Bewachungsunternehmen. Durch Notwehr oder Notwehr gesetzte Handlungen sind nicht rechtswidrig, bei Notstand allerdings nur bei wesentlichem Überwiegen der geschützten Interessen.

„Weltweit ist seit 2019 ein starker Anstieg von Überfahrtaten gegen weiche Ziele festzustellen“, führte Christian Schneider, *Initiative Breitscheidplatz GmbH*, aus. Zufahrtsschutz sei allerdings eine Maßnahme des Bauwesens mit baulichen Anlagen. Quergestellte Fahrzeuge, mobile Barrieren oder sonst das Eindringen eines Kraftfahrzeuges in einen zu schützenden Bereich lediglich



Präsentation von Neuheiten auf der Protekt-Messe: innovative Robotertechnik, automatisiertes Zutrittskontrollsystem

behindernde Maßnahmen fallen nicht unter diesen Begriff. Selbst eine Zertifizierung reicht nicht aus, wenn die Wirkweise vor Ort nicht umsetzbar ist.

Im Rahmen von Round Tables wurde die Ausfallsicherheit des deutschen Stromnetzes erörtert, von den Stadtwerken Düsseldorf durchgeführte Notfallübungen dargestellt und Erfahrungen im Sicherheitsbereich beim Zusammenwirken der verschiedensten Verkehrsträger im Hamburger Hafen ausgetauscht.

Künstliche Intelligenz ist zwar ein unverzichtbares Werkzeug in der Sicherheitsbranche, stellte Melanie Reuter-Oppermann, Technische Hochschule Würzburg-Schweinfurt sowie Integrierte Leitstelle (ILS) Mannheim (Feuerwehr, Rettungsdienst und Katastrophenschutz), fest, allerdings nur dann, wenn die jeweils passende Methode gewählt wird. Für Leitstellen, die vornehmlich Daten benötigen (Notrufe, Dokumentation, Sprachübersetzungssysteme), ist maschinelles Lernen (ML) zweckmäßig. Wenn es hingegen um Entscheidungen und Planung geht, eignen sich Modelle des Operations Research (OR) besser.

KI kann beispielsweise eine Phishing-Mail verfassen oder einen Ransomware-Angriff einleiten, führte Martin Weiss, Firma *Sophos*, aus. Es sei auch davon auszugehen, dass westliche KI-Systeme mit russischer Propaganda und Falschinformationen gefüttert und Trainingsdaten „vergiftet“ wurden. Dem eine weitere KI entgegenzusetzen, reiche nicht aus, Es bedürfe noch der Einbindung eines Expertenpools.

„Schon heute muss man sich auf die Rechenmöglichkeiten von morgen vorbereiten“, stellte Mathias Schumacher von *Q-PrEP (qprep.eu)* das Projekt Quantencomputing vor. Diese Technologie werde bestimmte komplexe Probleme in sehr kurzer Zeit lösen, was großes Potenzial für industrielle Anwendungen, aber auch in Logistik, Produktion, im Finanzsektor oder in Politik und Verwaltung biete. Nach der Europäischen Quantenstrategie soll Europa bis 2030 Spitzenreiter auf diesem Gebiet werden. Für dieses Projekt werden Mitwirkende gesucht.

Cybersecurity. Bianca Kastl, Ethische Hackerin aus dem Umfeld des *Chaos-Computer-Clubs*, berichtete über Erfahrungen mit der elektronischen Patientenakte (ePA) in Deutschland. Dieses Kernelement der Digitalisierung im Gesundheitswesen wurde am 15. Jänner 2025 gestartet. Bis Mitte Februar hatten die Krankenkassen allen Versicherten, die nicht widersprochen haben, den elektronischen Akt zur Verfügung gestellt. Seit 1. Oktober 2025 muss die ePA bundesweit von Praxen, Krankenhäuser und Apotheken genützt werden. In den rund 70 Millionen Patientenakten befinden sich mehr als 700 Millionen Datensätze. Auf sicherheitstechnische Schwachstellen aufmerksam gemacht, seien zwar Verbesserungen durchgeführt, aber noch immer nicht alle nach dem derzeitigen Stand der Technik möglichen Sicherheitsmaßnahmen implementiert worden, meinte Kastl,

Marion Blok, *Bundesamt für Sicherheit in der Informationstechnik (BSI)*,

erläuterte das am 6. Dezember 2025 in Kraft getretene NIS-2-Umsetzungsgesetz. Das österreichische Pendant hierzu ist das Netz- und Informationssicherheitsgesetz 2026 – NISG 2026, BGBl I 94/2025, das im Wesentlichen am 1. Oktober 2026 in Kraft tritt. Durch die NIS-2 RL soll das Gesamtniveau der Cyber-Sicherheit in der EU gesteigert und ein einheitliches Sicherheitsniveau in den Mitgliedsstaaten geschaffen und verbessert werden. Für die Organe der EU wurde eine eigene Cyber-Sicherheitsverordnung (EU 2023/2841) erlassen, über die Dirk Lieser vom Europäischen Gerichtshof berichtete.

In einer Expertenrunde zur Frage, ob die KI Fluch oder Segen sei, wurde die KI mit einem Spürhund verglichen, der Funde zusammenträgt. Der Segen liege in der Entlastung des Menschen bei der Entscheidungsfindung. Negative Auswirkungen würden sich durch die Generative AI ergeben, indem beispielsweise das Vertrauen in die Echtheit von Bildern verloren gehe.

Die Protekt-Messe ist, mit einem branchenübergreifenden Ansatz, auf den Schutz kritischer Infrastruktur (KRITIS) ausgerichtet und wird als Leitmesse für diesen Bereich bezeichnet. Insgesamt standen etwa 100 Referenten zur Verfügung. Rund 600 Personen haben an der Veranstaltung teilgenommen. In Nebenräumen waren 44 Aussteller einschlägiger Sicherheitsprodukte und -dienstleistungen vertreten. Die nächste *protekt* wird am 10. und 11. November 2026 wieder in Leipzig stattfinden.

Kurt Hickisch