

Trends, Strategien, Lösungen

Das 12. Jahresforum „D-A-CH Sicherheit“ der Simedia GmbH beleuchtete geo- und gesellschaftspolitische Entwicklungen aus Sicht der Unternehmenssicherheit.

An die 80 Sicherheitsfachleute aus der D-A-CH Region nahmen am 11. und 12. November 2025 am D-A-CH-Sicherheitsforum in Going in Tirol teil. Nach einem Überblick über die weltpolitische Situation ging der Rechtsanwalt und langjährige Vorsitzende des Innenausschusses des deutschen Bundestages, Wolfgang Bosbach, auf sicherheitspolitische Probleme in Deutschland ein. Bei der hybriden Kriegsführung stelle sich das Problem, dass die Bundeswehr zwar die technischen Mittel hätte, Drohnenangriffe abzuwehren, aber verfassungsgesetzlich Einsätze der Bundeswehr im Inland verboten seien. Die Polizei sei zwar befugt, doch fehlten ihr die technischen Mittel. Selbst in Fällen, bei denen Polizisten gepanzerte Fahrzeuge benötigen würden, um sich einem verschanzten Scharfschützen zu nähern, dürfe die Bundeswehr diese Fahrzeuge nicht zur Verfügung stellen.

Die Auflösung der bestehenden Weltordnung mit der Ausbildung von drei großen Machtblöcken und den Klimawandel bezeichnete Andreas Schlegel, stellvertretender Regierungsberater für nationale Sicherheit, staatliche Resilienz, umfassende Landesverteidigung, Krisenvorsorge und Krisenbewältigung im österreichischen Bundeskanzleramt, als Herausforderungen einer Zeitenwende, die 20 bis 30 Jahre andauern werde. Derzeitige Kriege seien Symptome, nicht aber die Ursache dieser Entwicklung. Die Hoffnung, „durchtauchen“ zu können, werde nicht reichen, es werde erforderlich sein, sich den neuen Gegebenheiten anzupassen. Wirtschaft und globale Lieferketten würden als Waffe eingesetzt. Die Gesellschaft werde hybriden Bedrohungen (Cyber-Attacken, Desinformation, Angriffe auf KRITIS) ausgesetzt sein, ohne entsprechend darauf vorbereitet zu sein, sodass Angriffe nicht oder zu spät erkannt werden. Was den D-A-CH-Raum betrifft, schützen geografische oder geopolitische Lage nicht mehr vor solchen Angriffen, auch nicht vor Wirtschafts-/Wissenschaftsspionage. Zur umfassenden Landesverteidigung müsse an eigener Abwehrfähigkeit und Resilienz gearbeitet werden.



Wirtschaft und globale Lieferketten werden als Waffen eingesetzt

Einen ähnlichen Ausblick auf eine ungewisse Zukunft gab, im Hinblick auf Deutschland, auch Peter H. Janssen. Nach dem Ende des kalten Krieges sei Sicherheit als selbstverständlich angesehen und Zivil- und Katastrophenschutz vernachlässigt worden. Die neue Gefährdungslage bestehe in nachrichtendienstlicher Ausspähung, Sabotageakten gegen Logistik und Energieversorgung sowie gegen KRITIS-Betreiber. Unsicherheit solle erzeugt werden. Hybride Angriffe („noch nicht Krieg, aber auch nicht Frieden“) seien Bestandteil moderner Konflikte. Klimawandel und Extremwetter würden klassische Sicherheitsrisiken verschärfen. Die bestehende Sicherheitsarchitektur (Feuerwehr, Rettung, Zivilschutz, Cyber-Sicherheit, Krisenvorsorge; Polizei, Militär) sei sektoral konstruiert, müsste aber übergreifend koordiniert und nicht als Verwaltung verstanden, sondern als dynamische Aufgabe gedacht und gelebt werden.

Die Kriminologin Julia Vincke, Unternehmenssicherheit *BASF*, berichtete über hybride Kriegsführung als neue Realität und bezeichnete sie als Kombination von militärischen, technologischen, ökonomischen, psychologischen und informationspolitischen Strategien, mit denen Ziele erreicht werden sollen,

ohne einen offenen Krieg zu erklären. Verunsicherung und Spaltung sollten erzeugt, eine gesellschaftliche Destabilisierung erreicht und die Informationshoheit gewonnen werden. Vincke berichtete über Drohnensichtungen über dem Werk Ludwigshafen zwischen November 2024 und Februar 2025. Die Drohnen kamen – immer in der Dunkelheit – entweder einzeln oder in Gruppen, verharren über dem Gelände oder waren schnell wieder weg. Versuche, sie im Voraus zu entdecken, etwa mit Radar, scheiterten. Die Verhaltensmuster deuteten auf nachrichtendienstliche/militärische Aktivitäten. Mittelbare Auswirkungen hatten die Drohnenflüge insofern, als ein sicherheitstechnischer Vorfall im Werk einige Wochen später über Social Media unzutreffenderweise auf diese Flüge zurückgeführt und aufgebauscht wurde. Damit wurden diese Medien zu Brandbeschleunigern von Desinformation und Propaganda.

Krisenmanagement. Über Konzernsicherheit im Spannungsfeld disruptiver Entwicklungen berichtete Florian Haake, Leiter Konzernsicherheit des *Porsche Konzerns*. Das weltweit agierende Unternehmen sei von globalen Krisen und Katastrophen, politischer Instabilität, Kriegen und Konflikten, Terroris-

mus, Industrie- und Wirtschaftsspionage ebenso bedroht wie von Erpressung und Entführung, Betrug und Wirtschaftskriminalität. Das habe zum Aufbau einer umfassenden Datenbank geführt, in die Vorfälle eingemeldet werden. Das Sicherheits-Know-how sei bei der Konzernsicherheit zentral gebündelt und werde international zur Verfügung gestellt. *Operational Technology (OT)* und *IT-Security*, physische und Informationssicherheit könnten nicht mehr für sich einzeln betrachtet werden. Assistenzsysteme seien notwendig, um diese komplexen Systeme beherrschbar zu machen. Technologien, Prozesse und Ressourcen müssten, unter Einbeziehung aller sicherheitsrelevanten Faktoren, zu einem ganzheitlichen Sicherheitsmanagement zusammengefasst werden.

Die *Trans-Austria-Gasleitung (TAG)*, ein Unternehmen kritischer Infrastruktur, betreibt in Österreich in drei Leitungssträngen ein insgesamt 1.100 km langes Gasleitungsnetz von der slowakischen Grenze bis Italien. Michael Lederer berichtete aus dem „Maschinenraum“ des Unternehmens aus dem Blickwinkel gesetzlicher Bestimmun-



Referenten beim DACH-Forum: Theresa Mayerhofer, Michael Lederer, Richard Werner, Frank Ewald

gen für den technischen Betrieb der Anlagen. Technische und organisatorische Maßnahmen müssten laufend angepasst werden. Kostenfragen würden sich stellen. Technische Überwachungsmaßnahmen könnten mitunter in Persönlich-

keitsrechte eingreifen. Manche Begriffe seien unbestimmt. Die Einhaltung des jeweiligen Standes der Technik erfordere, sich auf dem Laufenden zu halten. Anzuraten sei, sowohl mit dem Betriebsrat als auch mit den Behörden in engem Kontakt zu stehen.

Entscheidungsfindung. Richard Werner von der Schweizer *GRC-Risk-Intelligence* stellte den Krisen-Rhythmus OODA als Führungsprinzip unter bestehendem Zeitdruck vor. Ähnlich dem PDCA-Zyklus ist die erste Stufe das Beobachten (*Observe*), was wirklich passiert. Darauf folgt die Erstellung eines Lagebildes (*Orient*), in das Daten, Erfahrung, Unternehmenskultur und Ziele einfließen. Darauf aufbauend wird eine klare Handlungsoption gewählt (*Decide*) und letztlich gehandelt (*Act*). In der Krise sei die relevanteste Expertise von Bedeutung, nicht die Stellung in der Hierarchie. Die Entscheidungsfindung unter Zeitdruck müsse geübt und Business-Continuity-Management, schon aus Haftungsgründen, nachweisbar umgesetzt werden.

Auf Risiken beim Einsatz von KI machte Frank Ewald, Konzernsicherheit

der *DHL-Group*, aufmerksam. Wie KI zu Entscheidungen komme, sei nicht exakt reproduzierbar. KI könne „halluzinieren“, also vermeintliche Fakten erfinden. Daten, die zur Entscheidungsfindung herangezogen werden, könnten, je nach den verwendeten Quellen, Vorurteile (*Bias*) enthalten oder die Trainingsdaten selbst könnten mit Fälschinformationen „vergiftet“ sein. Es werde immer schwieriger, KI-generierte Inhalte zu erkennen, was individualisierten Betrug (CEO-Fraud, Spear-Phishing, Romance Scam usw.) erleichtere, bis zum vollständig automatisierten Betrug „as a Service“. Mit generativer KI würden Fake News verbreitet und Bilder, Videos, Stimm-aufzeichnungen, verfälscht oder produziert, was zu einer Vertrauenskrise bis hin zur Radikalisierung führen könne. Verträge, Rechnungen, aber auch, wie sich gezeigt habe, wissenschaftliche Arbeiten könnten durch verborgen eingebaute Anweisungen (*Prompts*) so verfälscht werden, dass die voraussichtlich zur Prüfung eingesetzte KI nur positive Ergebnisse liefere. Der Mensch, der als kontrollierendes Glied in der Entscheidungskette fungieren sollte (*Human in the Loop*), sei überfordert und könne selbst zum Opfer werden. Etwa, indem in die Systeme menschliche Eigenschaften projiziert würden (*Eliza-Effekt*) mit psychischen Bindungen zur Maschine. Chatbots könnten zu abgeschirmten „Echokammern“ werden, in denen sich Tendenzen bis zur Radikalisierung aufschaukeln.

„Unser Gehirn nimmt, um schnellere Entscheidungen zu ermöglichen, beim Denken Abkürzungen und orientiert sich an bereits Bekanntem“, erläuterte die Wirtschaftspsychologin Teresa Mayerhofer, *VASBÖ (Verband Akademischer Sicherheitsberater Österreichs)* bzw. *SCER Institut (Safety, Consulting, Education, Research)*. Diese psychologischen Prozesse seien zwar im Alltag hilfreich, könnten aber als Human Hacking schadenbringend ausgenutzt werden. Der Angreifer sei bestrebt, ein Hinterfragen nicht aufkommen zu lassen. Er versuche, Vertrauen aufzubauen, indem gemeinsame Interessen hervorgehoben werden und Sympathie entwickelt werde. Auf einer systemischen Ebene werde Autorität hervorgekehrt, etwa durch Auftreten als Berater, Aufsichtsperson, oder dass das Gefühl erzeugt werde, dem Angreifer zu einer Gegenleistung verpflichtet zu sein, etwa



D-A-CH-Sicherheitsforum in Going, Tirol: Teilnehmer waren etwa 80 Sicherheitsfachleute aus Deutschland, Österreich und der Schweiz

bei Geschenken. Um bei komplexeren Situationen aus den gedanklich eingefahrenen Geleisen herauszukommen, brauche es Motivation durch konzeptionelles, kreatives Denken, das verinnerlicht werden müsse (Kohärenz im psychologischen Sinn).

Forschungsergebnisse. Wolfgang Tomaschitz, *Hochschule Campus Wien*, berichtete über das Ergebnis einer zwischen 21. Februar bis 22. März 2024 erfolgten Untersuchung zu Wirtschafts- und Industriespionage in Österreich. Es wurden von der Wirtschaftskammer Österreich und der Industriellenvereinigung 17.688 Online-Fragebogen an 2.239 Unternehmen versendet, von denen 510 die Fragebögen vollständig ausgefüllt rückgesendet haben. 80 Prozent dieser Unternehmen hatten weniger als 50 Beschäftigte. 91 Prozent der Unternehmen gaben an, in den letzten fünf Jahren nicht von Spionage betroffen gewesen zu sein. 5,9 Prozent hatten einen diesbezüglichen Verdacht. 3,1 Prozent waren sich sicher. 25 Prozent der betroffenen Unternehmen vermuteten, dass Mitbewerber hinter den Vorfällen stecken würden. Ehemalige Mitarbeiter wurden von 18,8 Prozent als Urheber angesehen. Tathandlungen waren zur Hälfte Hackerangriffe, gefolgt vom Abhören/Abfangen von Informationen. Informationsweitergabe durch Mitarbeiter und Social Engineering wurden zu jeweils knapp 19 Prozent als Tathandlungen angeführt; Angriffe durch KI zu 10 Prozent. Im Durchschnitt wurden die Behörden/Institutionen zu 36 Prozent

verständnis, bei vier oder mehr Vorfällen immer. Der hauptsächliche Grund für die Nicht-Meldung war, dass in der Einschaltung der Behörden kein Nutzen gesehen wurde. Betroffene Unternehmen haben das Risiko neuerlicher Angriffe zu 50 Prozent als eher hoch, 12,5 Prozent als sehr hoch bezeichnet.

In der Nachfolgeforschung *Themis*, bei der der Schwerpunkt auf Prävention gelegt werden wird, werden insgesamt 174 Gerichtsakten aus den Jahren 2003 bis 2023 ausgewertet, die Verfahren nach den §§ 122 bis 124 StGB (Verletzung/Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses) sowie die §§ 11 und 12 UWG (Weitergabe von Informationen) samt Begleitdelikten zum Gegenstand haben.

„Der Terrorismus der Zukunft ist digitalisiert, individualisiert, jugendlich und männlich“, sagte Florian Hartleb, Modul-Universität Wien, zum Thema Teenagerterrorismus und Radikalisierung. Er verwies auf Forschungsergebnisse des Terrorismusforschers Peter Neumann, wonach in den letzten drei Jahren zwei Drittel aller Terrorverdächtigen in Europa unter 19 Jahre alt gewesen seien. Netzwerke, Narrative und Needs seien die drei N der Radikalisierung. Mobbingerfahrungen und Vereinsamung würden eine Rolle spielen, verstärkt durch eine Gamification des Terrors. Die Täter seien Polizei und Sicherheitsbehörden vorerst nicht einschlägig bekannt und daher nur schwer erfassbar. Auch Schulen müssten in eine neue gesellschaftliche Verantwortung einbezogen werden. *Kurt Hickisch*