Fachtagung „Protekt“ für den Schutz kritischer Infrastruktur: Vorträge zu Bedrohungsszenarien und Lösungsansätzen rund um Krisenprävention und Krisenmanagement

Auch das Unmögliche denken

Bei der Fachtagung „Protekt“ für den Schutz kritischer Infrastruktur im November 2023 in Leipzig tauschten sich Experten aus KRITIS-Organisationen über mögliche Szenarien, angepasste Ansätze der Prävention und veränderte gesetzliche Rahmenbedingungen aus.

Professor Thomas Popp, Staatssekretär für digitale Verwaltung und Verwaltungsmodernisierung und Chief Information Officer des Freistaates Sachsen, hielt einen Vortrag mit dem Titel „Vorsorge ist besser als Nachsicht“. Er betonte, dass die Bezeichnung „kritische Infrastruktur“ längst vom Fachterminus in den allgemeinen Sprachgebrauch gewandert sei. „Corona-Pandemie, Diebstahl von Kupferkabeln bei der Deutschen Bahn, der unerlaubte Zutritt auf das Flughafengelände in Hamburg und nicht zuletzt die Stabilität der Energieversorgung sind Beispiele, wie wichtig das Funktionieren von kritischer Infrastruktur ist, wie bedroht sie aber auch ist“, sagte Popp. Um sich den Herausforderungen der heutigen Zeit stellen zu können, brauche es neben Regularien, die ein gemeinsames Verständnis über die Cyber-Sicherheit erzeugen, auch Resilienz. „So lange nichts passiert, sind warnende Stimmen lästig. Nur wenn etwas passiert, sind sie schuld, weil sie nicht laut genug waren“, sagte Popp, und appellierte an die Teilnehmerinnen und Teilnehmer der Konferenz: „Bleiben Sie laut, bleiben sie nervig.“ Resilienz sei etwas, das man sich hart erarbeiten müsse. Man müsse Szenarien üben und jede Organisation müsse lernen, schnell wieder auf die Beine zu kommen, falls doch etwas passiere. „Denn das ist nur eine Frage des Wann, nicht des Ob“, mahnte Popp.

Schwachstellen. Als asymmetrische Lage skizzierte Andreas Reisen, Referatsleiter Cyber-Sicherheit für Wirtschaft und Gesellschaft im Bundesministerium des Inneren und für Heimat, die gegenwärtige Situation. Ein Angreifer müsse nur eine Stelle automatisiert zum Angriff finden und bediene sich dazu häufig automatisierter Methoden – z. B. Portscans. Wenn man sich vor Angriffen schützen will, muss man aber alle potenziellen Schwachstellen im Blick haben. Der Aufwand dazu ist unverhältnismäßig höher, um alle verteidigen zu können. Daher machen hier automatisierte Methoden Sinn, etwa mittels dazu konzipierter Angriffserkennungssysteme. Für Betreiber kritischer Infrastrukturen sind diese bereits Pflicht.

Angriffserkennung. Die verschärfte Lage führt auch zu neuen europäischen und nationalen Gesetzen. Timo Hauschild, vom Bundesamt für Sicherheit in Informationstechnik (BSI) ging auf das „NIS-2-Umsetzungs- und Cyber-Sicherheitsstärkungsgesetz“ für die Cyber-Sicherheit und das KRITIS-Dachgesetz für die physische Sicherheit ein. Das BSI biete auch eine Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung. Und er lud zur Teilnahme an der „Allianz für Cyber-Sicherheit“ und am „UP KRITIS“ ein, zwei Public-Private-Partnerships im Bereich des BSI.

FOTO: LEIPZIGER MESSE GMBH / NICLAS SCHMIDT

Krisenlagen. Wolfram Geier vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) beschrieb eine zunehmend herausfordernde sicherheitspolitische Lage in der Welt. Trends zwischen Innen- und Außenpolitik würden verschwimmen und hybride Kriege häufiger werden: „Sich überlappende Langzeitlagen stellen neue Herausforderungen für Deutschland dar. Kurzzeitkrisen bewältigen wir gut.“ Sind wir sicherheitspolitisch ausreichend aufgestellt? Der Ausblick auf die Zukunft sei schwieriger, insbesondere hinsichtlich der Frage, wie wir mit multiplen Krisenlagen unterschiedlicher Ursachen umgehen: „Wir haben es immer stärker mit Desinformation und einem Vertrauensverlust in die Demokratie und in die staatliche Leistungsfähigkeit zu tun. Jeder Ausfall wird genutzt werden, um Misstrauen zu säen.“

Risiken. Gunar Korm und Peter Eitel von *PwC GmbH WPG* sprachen während der Protekt 2023 in Leipzig über die Absicherung von Energieinfrastrukturen. Sie betonten, dass die „Räume“, in denen Staaten und Unternehmen agierten, regulatorisch und operativ enger würden, denn neue gesetzliche Auflagen und geopolitische, komplexe Sicherheitsrisiken würden diese einschränken. Das geopolitische Risiko gehöre auf die Agenda aller Vertreter des Topmanagements. Risiken könnten physischer Natur sein, wie Zutrittsmöglichkeiten, Naturkatastrophen, Sabotage, Vandalismus oder ein Blackout. Sie könnten auch organisatorischer Natur sein, wie mangelnde Security-Awareness, unklare Zuständigkeiten oder fehlende Notfallplanungen. Im KRITIS-Dachgesetz werden künftig die Registrierung kritischer Anlagen, die Risiko-Analyse und -Bewertung sowie die Meldung von Störungen obligatorisch. Daher sollten Unternehmen jetzt handeln.

Ein Teilnehmer fragte, inwiefern ein privates Unternehmen für die Abwehr von Terrorismus zuständig sei. Im Ergebnis sollen Unternehmen keine aktiven oder letalen Maßnahmen einleiten, denn das obliege dem Staat. Aber die Etablierung von Frühwarnsystemen im Rahmen des Sicherheitsrisikomanagements durch Unternehmen oder öffentliche Institutionen zur Detektion von Angriffsversuchen und eine Analyse hinsichtlich der eigenen Zielattraktivität seien relevant.

André Bodemann: „Deutschland befindet sich nicht im Krieg, aber auch nicht im Frieden.“

Alarmierungen. Die „Alarmierung und Verifizierung in öffentlichen Gebäuden nach DIN VDE V 0827“, präsentierte Bernd Ammelung, Ingenieur-Büro Ammelung: Wie kann je nach Ereignis angemessen in Schulen und Gerichtsgebäuden alarmiert werden? Normale Alarmierungen führen dazu, dass Menschen Gebäude verlassen. Die Evakuierung und das Aufsuchen von Sammelplätzen ist jedoch beispielsweise bei Amoktaten oder Geiselnahmen kontraproduktiv.

Alarmierungen können in Notfällen konkurrieren und Alarme müssen von Täuschalarmen unterschieden werden. Wichtig ist es, im Notfall eine angemessene Entscheidung für die gebäudeinterne Alarmierung und die externe Alarmierung zu Polizei und Rettungsdiensten sowie eine rasche Lageinformation zu geben.

Anwendungsbereich der Richtlinie sind beispielsweise Schulen bei Brand, Amok oder Unfällen, dann Justizgebäude bei Befreiungsversuchen oder Geiselnahme und Bahnhöfe bei Bombendrohungen. Relevant seien darüber hinaus auch die Arbeitsschutzgesetze. Grundsätzlich ist wichtig: Für eine Risikobeurteilung ist der Kontext zu beachten. So könne bei einem giftigen Bodengas oder Hochwasser die Flucht in obere Etagen prioritär sein, aber bei einer Amok-Lage der Einschluss in Räume.

Stephan Boy: „Ein interdisziplinäres Lagebild in Echtzeit ist notwendig.“

Thomas Popp: „Jede Organisation muss lernen, schnell wieder auf die Beine zu kommen.“

Interdisziplinäres Lagebild. Stephan Boy vom „Zukunftsforum öffentliche Sicherheit“ sprach über Krisenmanagement. Die aktuelle Sicherheitslage sei wie ein Reallabor. Notwendig sei ein interdisziplinäres Lagebild in Echtzeit, beschrieben auch im „Grünbuch Lagebild“ des Zukunftsforums Öffentliche Sicherheit. Denken müsse man alles, auch das Unmögliche: „Wir müssen auch Szenarien überlegen, die vor einem halben Jahr noch undenkbar waren.“ Beispiele könnten die zeitgleiche Störung der Wasserwerke dreier Großstädte sein oder das Auftreten ähnlicher Krankheitsbilder in unterschiedlichen, weit voneinander entfernten Kliniken. Wer sieht da einen Zusammenhang? Notwendig für ein interdisziplinäres Lagebild sind im Idealfall Echtzeitdaten auch beispielweise aus Organisationen der Gefahrenabwehr sowie der Industrie für ein 24/7-Lagezentrum.

Incident-Response-Maßnahmen. Eine Kernbotschaft zur Cyber-Sicherheit brachte Michael Zimmer von *G Data Advanced Analytics* mit nach Leipzig: Die Schadenshöhe bei einer IT-Attacke korreliert mit der Dauer der Störung. Daher muss der Angegriffene einen Angriff möglichst früh erkennen und seine Incident-Response-Maßnahmen unmittelbar einleiten. Resilienz bedeutet, den Zeitraum zwischen Kompromittierung und Wiederherstellung kurz zu halten. Außerdem müsse ein sicherer Notfall-

Fotos: Leipziger Messe GmbH / Niclas Schmidt, Jörg Rohne/ZOES

Alarmierung und Verifizierung in öffentlichen Gebäuden: Die Evakuierung und das Aufsuchen von Sammelplätzen ist beispielsweise bei Amoktaten oder Geiselnahmen kontraproduktiv

plan im Sinne einer professionellen Incident-Response etabliert werden: Packen Sie sich die Notfallplanung auf einen Stick, drucken Sie sie aus, packen Sie es in einen Safe. Auf einem verschlüsselten Laufwerk sind diese Daten wenig hilfreich. Nur ein Offline-Backup ist ein gutes Backup. Und holen Sie sich schnell Hilfe: Professionelle Incident-Response-Teams haben Routine, weniger Stress und sind nicht in die Hierarchie der betroffenen Organisation eingebunden." Geschwindigkeit gehe in der Regel vor Gerichtsverwertbarkeit.

Bundeslagenzentrum. Christian Kunstmann, Hauptreferent Public Private Partnership vom österreichischen Innenministerium bestätigte das allgemein wahrgenommene neue Lagebild. Vor 2020 sei noch der Terror als Hauptrisiko eingestuft worden. Heute würde das neue österreichische Bundeskrisensicherheitsgesetz auf die neuen Herausforderungen antworten. In Österreich wird ein Bundeskrisensicherheitskabinett eingerichtet werden und ein baulich auf guter Sicherheitsstufe konzipiertes Lagezentrum, das den Vorteil der örtlichen Nähe zur Regierung bietet.

Besonders wichtig ist die Zusammenarbeit mit den kritischen Infrastrukturen der Wirtschaft zur Resilienz-Steigerung. Und wenn man dem ganzen schwierigen Umfeld zumindest einen positiven Aspekt abgewinnen könne, so seien „Krisen", so zitierte er JF Kennedy, „auch Chancen für Erneuerungen".

Hybride Herausforderungen. Generalleutnant André Bodemann von der deutschen Bundeswehr sprach über den „Schutz kritischer Infrastruktur im Zeichen der Zeitenwende". André Bodemann ist Befehlshaber des territorialen Führungskommandos der Bundeswehr, das als Resultat des Angriffskrieges auf die Ukraine und der Zeitenwende-Rede von Bundeskanzler Scholz im September 2022 aufgestellt wurde.

Die Herausforderungen seien hybrid: Deutschland befinde sich nicht im Krieg, aber auch nicht im Frieden. Sondern irgendwo dazwischen. Attacken finden jeden Tag hybrid statt, darunter Ausspähung, Spionage, Zunahme von Drohnensichtungen über Übungsplätzen und über Rechenzentren. Bekannt sind Sabotagehandlungen etwa an der Pipeline Nord-Stream 2, auf Bahnstrecken der Deutschen Bahn oder der Ankerwurf auf die Gaspipeline Balticconnector durch ein chinesisches Schiff. Der Generalleutnant erläuterte die Aufgaben Deutschlands für die NATO im Ereignisfall als Center of Gravity, das heißt Aufmarschgebiet für Truppenverbände. Die Gefahr für einen Logistik-Hotspot sei, dass ihn ein Gegner stören möchte. Notwendig sei ein allgemeines Lagebild aus militärischen, polizeilichen und nachrichtendienstlichen Quellen, ergänzt um Erkenntnisse aus kommunalen Gebietskörperschaften.

Falls etwas passieren würde, könnte man unterschiedliche Erkenntnisse übereinanderlegen. Dies ergebe möglicherweise ein Muster. Schwierig sei: Die NATO könne eigentlich erst ab dem Bündnisfall nach § 5 NATO-Vertrag aktiv werden und beispielsweise Reservisten einberufen. Im Ereignisfall ist eine maximale zivile Leistungserbringung notwendig. Jeder müsse dafür priorisieren: Landes- und Bundespolizei sowie zivile Betreiber. „Das ist der Sachstand dessen, was auf uns zukommt: eine Zunahme der Zahl an Sabotagefällen unter der Schwelle des §-5-Bündnisfalls wegen Unsicherheiten, um uns möglichst zu schaden", sagte Bodemann. *Benedikt Haufs*