Kritische Infrastruktur: Wie wir resilient werden

Es häufen sich Angriffe auf und Vorfälle bei kritischen Infrastrukturen. Die Politik reagiert vor allem mit der Forderung nach mehr Überwachung und Befugniserweiterungen. Für mehr Sicherheit sind aber vor allem Investitionen in resiliente Systeme und mehr Sorgfalt bei der Prävention nötig.

Von MANUEL ATUG

Wiederholte Angriffe auf die Stromversorgung, der fehlgeschlagene Drohnenangriff auf ein ukrainisches Frachtflugzeug auf dem Flughafen Leipzig/Halle im August, Sturzfluten wie im Ahrtal, der Cyberangriff auf die Berliner Verwaltung oder die Manipulation der Kühlsysteme in französischen Supermärkten – all das zeigt uns, wie verwundbar unsere kritischen Infrastrukturen sind, also jene Bereiche, deren Beeinträchtigung oder Ausfall zu Versorgungsengpässen, Störungen der öffentlichen Sicherheit und weiteren dramatischen Folgen führen können.[1]

Die Häufung solcher Vorfälle ist Ausdruck wachsender geopolitischer Spannungen, des weltweiten Aufstiegs von Autokratien und des voranschreitenden Klimawandels. An diese veränderte Bedrohungslage müssen wir uns anpassen. Doch während nach einem Vorfall regelmäßig die Forderung nach mehr Überwachung laut wird, passiert hinsichtlich der konkreten Prävention bislang viel zu wenig. Die Politik hat das Thema Resilienz zwar auf der Agenda, behandelt es aber vor allem als eine Frage der Sicherheit in Form von mehr Befugnissen für Ermittlungs- und Polizeibehörden oder Geheimdiensten. Nach einem Vorfall heißt es oft: Wir brauchen mehr Massenüberwachung und KI-Datenauswertung, um die Täter zu erwischen. Der Bundesverband der Energie- und Wasserwirtschaft etwa fordert Anpassungen der Datenschutzbestimmungen, um öffentliche Bereiche rund um die Anlagen rechtssicher überwachen zu können. Nordrhein-Westfalens Innenminister Herbert Reul, der als einer der Ersten in seinem Bundesland die offensichtlich verfassungswidrige Rasterfahndungssoftware der US-Firma Palantir eingeführt hat[2], brachte nach den Angriffen auf die Stromversorgung in Nordrhein-Westfalen und Brandenburg im September die Idee ins Spiel, die Betreiber kritischer Infrastrukturen sollten nicht nur

MANUEL »HONKHASE« ATUG, *geb. 1976 in Wipperfürth, ist Informatiker und Ingenieur. Er berät die Bundesregierung sowie mehrere Bundesländer zu IT-Sicherheit und digitalem Katastrophenschutz und ist Sprecher der AG KRITIS, eines Zusammenschlusses von Fachleuten für die Sicherheit kritischer Infrastrukturen.*

1 Dazu zählen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen, Abfallentsorgung, Staat und Verwaltung sowie Medien und Kultur.

2 Vgl. Sonja Peteranderl, Das Überwachungsimperium. Wie sich die deutsche Polizei von Peter Thiels Palantir-Software abhängig macht, in: »Blätter«, 8/2025, S. 91-96.

mehr Videoanlagen installieren, sondern auch private Sicherheitsdienstleister zum Abschuss von Drohnen einsetzen dürfen. Das aber würde an den Grundfesten unseres demokratischen Rechtsstaats rütteln. Denn das »Herbeiführen eines Absturzes einer unkooperativen Drohne« ist ausschließlich den Sicherheitsbehörden vorbehalten, die Entscheidung über aktive Abwehrmaßnahmen müssen staatliche Hoheitsträger treffen. Diese arbeiten nicht erlösmaximierend und haben immer auch den Kollateralschaden im Blick. Sonst landen wir im Extremfall bei Szenarien wie jenen, in die die von den USA beauftragte Sicherheitsfirma Blackwater (jetzt Academi) involviert war. Die Angestellten dieser Firma feuerten in der irakischen Hauptstadt Bagdad mit Maschinengewehren und Granatwerfern willkürlich in eine Menschenmenge, weil sie glaubten, »machen zu können, was sie wollen«, und sich als das Gesetz verstanden.[3]

Backup-Systeme statt Massenüberwachung

Natürlich brauchen wir Informationen, um Täter ermitteln zu können. Aber schon jetzt kann man viele öffentliche Bereiche rund um Anlagen der kritischen Infrastruktur rechtssicher überwachen, an Flughäfen beispielsweise sind hunderte bis tausende Kameras im Einsatz, um etwa die Schengengrenze und die Außengrenze zu kontrollieren. Schon jetzt gibt es in Städten vielerorts viel zu viel Videoüberwachung – inzwischen werden diese vermehrt mit KI-gesteuerter Gesichts- und Bewegungsmustererkennung ausgestattet. Überall wird man schon heute aufgezeichnet und registriert. Genau diese Maßnahmen jetzt noch zu verstärken, das verkleinert die Bedrohung keineswegs. Denn eine Kamera kann zwar ein Naturereignis, einen Unfall oder eine Vorsatzhandlung filmen. Aber egal, wie viele Kameras ich aufstelle, wie viel KI-Gesichtserkennung ich habe: Keine Kamera kommt herunter und verhindert einen Vorfall. Stattdessen normalisiert sie die Massenüberwachung noch mehr. Dagegen können andere Methoden Angriffe überwachungsarm und grundrechtsschonend detektieren oder verhindern, wie etwa Sensoren, die das Übersteigen und Durchtrennen von Zäunen melden, oder durch eine Ruhestromüberwachung.

»Die kritischen Infrastrukturen müssen so widerstandsfähig sein, dass sie uns nach einem Vorfall weiterhin versorgen können.«

Innenminister Alexander Dobrindt und Wirtschaftsverbände wie der Bundesverband der Energie- und Wasserwirtschaft fordern neben mehr Überwachung zudem, dass Daten – etwa über den Verlauf von Stromtrassen oder Wasserleitungen – aus dem Netz entfernt werden sollen, damit sie nicht so leicht als Angriffsziele auffindbar sind. Das würde allerdings nur das Sicherheitsgefühl erhöhen, nicht aber für Sicherheit und Resilienz sorgen. Es ist sogar absehbar, dass es zu mehr Stromausfällen führen würde als bisher. Denn während sich ein Saboteur sicher nicht davon abhalten lassen würde, ein Umspannwerk auszusuchen und anzugreifen, wird es deutlich mehr »Baggerbisse« an Stromleitungen geben, weil die Bauunternehmen online nicht mehr nachschauen können, wo eine Trasse entlangführt – 2019 verursachte beispielsweise ein Bagger einen 31-stündigen Stromausfall in Berlin.

3 Vgl. Blackwater-Söldner muss lebenslang in Haft, spiegel.de, 15.8.2019.

Was wir also brauchen, ist nicht ein größeres Sicherheitsgefühl durch Überwachung oder Pseudogeheimhaltung, sondern echte und funktionale Resilienz. Beim Schutz der kritischen Infrastrukturen geht es erst einmal darum, dass die Bevölkerung weiterhin mit Strom, Wasser und Lebensmitteln versorgt wird. Das heißt, die kritischen Infrastrukturen müssen so resilient, sprich: widerstandsfähig sein, dass sie den Betrieb im Falle eines Angriffs oder sonstigen Vorfalls aufrechterhalten und uns weiterhin versorgen können. Im Idealfall verpuffen die Auswirkungen eines Vorfalls dann völlig wirkungslos oder man hat eine kleine Störung, aber keine Krise oder Katastrophe. Bei den zwei Sabotageaktionen auf die Umspannwerke in Brandenburg und Nordrhein-Westfalen im September dieses Jahres konnte man umschwenken auf andere Erzeuger und Trassen. Die Bevölkerung und die Unternehmen wurden störungsfrei weiter versorgt. Das ist echte Resilienz. Beim Brandanschlag auf das Berliner Stromnetz im Januar, bei dem 45000 Haushalte und über 2000 Betriebe im Südwesten der Stadt bei Minustemperaturen tagelang vom Strom abgeschnitten waren, hat das hingegen nicht funktioniert.

Um einen Stromausfall wie den in Berlin zu verhindern, benötigt man ein funktionales Notfallmanagement, Backup-Systeme und Redundanzen. Also beispielsweise Stromgeneratoren und den dazugehörigen Diesel. Systeme und Trassen müssen »georedundant«, also an unterschiedlichen Stellen vorhanden sein, um auch solche Engpässe verhindern zu können. Denn wenn verschiedene Leitungen über dieselbe Trasse führen, so wie das in Berlin auf der Kabelbrücke der Fall war, dann können alle gleichzeitig angegriffen oder anderweitig gestört werden. Insgesamt muss Sicherheit immer als Prozess gedacht und gelebt werden, denn welche Schutzmaßnahmen wie wirken, das verändert sich, weil etwa der Klimawandel zu extremeren Ereignissen führt oder die Autokraten und Diktatoren in den USA, in China und Russland immer extremer handeln.

»Es ist einfacher, den Leuten ein Sicherheitsgefühl zu verkaufen, als echte Sicherheit herzustellen.«

Bislang allerdings hat der Staat Betreibern kritischer Infrastrukturen nicht gesetzlich vorgeschrieben, physische Sicherheitsmaßnahmen zu ergreifen, um sich gegen Naturereignisse, Unfälle und Angriffe passend aufzustellen. Es ist daher dringend notwendig, das KRITIS-Dachgesetz zum Schutz der kritischen Infrastruktur, das seit März in Kraft ist, endlich anwendbar zu machen.

Bislang ist das Gesetz nur eine leere Hülle, da zwei zugehörige Verordnungen fehlen, die regeln sollen, wer als Betreiber darunterfällt und was diese genau an physischen Sicherheitsmaßnahmen umsetzen müssen. Die Verordnungen sollen konkrete Präventivmaßnahmen wie Schutzzäune, Mauern oder den Bau von Zugangskontrollen definieren. Zur Drohnenabwehr kann man Käfige, wie sie auch in der Ukraine eingesetzt werden, um ein Umspannwerk herum errichten oder sie zumindest vorrätig haben, um sie im Angriffsfall schnell aufbauen zu können. Zur Erkennung kann man mehr Wachposten und Wachstreifen einsetzen, aber auch Bewegungsdetektoren, Vibrationsmelder oder Übersteigschutz- und -erkennungssysteme, die effektiver sein können als Videoüberwachung und keine Datenschutzprobleme aufwerfen. Zudem ist es unabdingbar, Evakuierungspläne vorzuhalten

oder zu wissen, wie man methodisch vorgeht, um alternative Energieleitungen zu nutzen, wenn eine Leitung beschädigt ist.

Doch der politische Wille, die Verordnungen schnell zu verabschieden, ist zurzeit offenbar nicht vorhanden. Laut Bundesinnenministerium soll ihre Ausarbeitung noch ein oder zwei Jahre dauern. Wir bräuchten sie aber eher in Wochen. Allerdings hätten wir auch bei einer Umsetzung des Gesetzes noch das Problem, dass dessen Nichteinhaltung mit maximal einer Mio. Euro sanktioniert wird. Wenn ein Konzern mehrere Dutzend Mio. Euro investieren muss, um physische Sicherheit herzustellen, dann ist das kaum ein Anreiz für Wirtschaftsunternehmen, das Gesetz umzusetzen.

Der Grund, warum bislang zu wenig in Prävention investiert wird, ist einfach: Vorsorge ist nicht attraktiv, damit lässt sich keine Wahl gewinnen. Und mal ganz ehrlich: Niemand möchte für Resilienz bezahlen. Aber um dauerhaft Ausfälle kompensieren zu können, muss man in Präventionsmaßnahmen investieren. Doch wenn dies geschieht, heißt es schnell: »Warum habt ihr 50 Mio. Euro für Energienetze ausgegeben, obwohl nichts passiert ist? Wir brauchen doch Kita-Plätze.« Es ist einfacher, den Leuten ein Sicherheitsgefühl zu verkaufen, als echte Sicherheit herzustellen.

Marode Brücken, marode Cybersicherheit

Das zeigt sich auch beim Datenschutz. Dabei ist Datenschutz Menschenschutz, denn wir schützen damit ja die Menschen hinter den Daten. Beim jüngsten Datenabfluss in Berlin etwa haben die Erpresser 5,8 Terabyte mit mehr als 1,4 Mio. teils hochsensiblen Daten im Darknet veröffentlicht, darunter staatlich-hoheitliche Geheimschutzinformationen wie Daten über Objekte, die man im Verteidigungsfall besonders schützen muss - Heizkraftwerke für Krankenhäuser, Tanklager, Notstromanlagen, Umspannwerke, oder eine Liste der Rüstungsunternehmen, die das Land als besonders wichtig einschätzt. Diese Informationen sind nun offen zugänglich für Terroristen, Geheimdienste und Kriegstreiber. Wer Geschäftsführer in einem solchen Rüstungsunternehmen ist und noch keinen Personenschutz hatte, sollte jetzt sehr aktiv darüber nachdenken. Auch sehr vertrauliche personenbezogene Daten von Mitarbeitenden, wie Informationen zu Disziplinarverfahren, Schwerbehindertenausweise oder Ausweiskopien befinden sich unter den veröffentlichten Informationen. Wenn alle meine persönlichen Daten veröffentlicht wurden, dann kann ich davon, wenn überhaupt, die Telefonnummer, das Konto und den Wohnort ändern. Aber ein neues Gesicht, ein anderes Geburtsdatum oder einen neuen Fingerabdruck kann ich mir schlecht zulegen.

Sind diese Dinge erst einmal in der Welt, ist das nicht revidierbar, schließlich weiß man nicht, wer alles Kopien hat. Wenn diese Daten in fünf oder 20 Jahren veröffentlicht werden, habe ich als betroffene Person das Problem immer noch. Und falls Daten meiner Kinder dabei waren, kann dies sie auch in 50 Jahren noch einholen. Einen solchen weitsichtigen Blick zur Technologiefolgenabschätzung hat fast keiner.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt schon lange vor einer erhöhten Cyber-Bedrohungslage. Doch die Sicherheitslage und der Datenschutz sind im Laufe dieser Zeit nicht besser, sondern schlechter geworden. Im Juli 2021 rief der Landkreis Anhalt-Bitterfeld als erste Kommune in Deutschland den Katastrophenfall wegen eines Cyberangriffs aus. Seitdem gab es solche Angriffe auf über 250 weitere Kommunen. Meistens gibt die Behördenleitung das Thema an einen Informationssicherheitsbeauftragten ab, der es im IT-Keller mit zu wenig

Geld und zu wenig Personal lösen soll, aber die Verantwortung für die Steuerung der Sicherheitsmaßnahmen liegt bei den Behörden- und Geschäftsleitungen und kann nicht delegiert werden. Hinzu kommt, dass die IT-Architektur und die Software stark veraltet sind. Man kann sich das wie bei Brücken vorstellen: Rund 8000 Brücken in Deutschland sind sanierungsbedürftig. Mehrere tausend Brücken sind inzwischen so baufällig, dass man sie abreißen und neu bauen muss. Diesen Zustand gibt es auch im Digitalen. Nach Anhalt-Bitterfeld gab es viele Diskussionen, aber passiert ist wenig. Dann kam 2023 der Cyberangriff auf das kommunale Dienstleistungsunternehmen Südwestfalen-IT, von der 70 Kommunen mit insgesamt rund 1,7 Millionen Einwohnern betroffen waren, jetzt Berlin.

»Ein Cyber-Hilfswerk könnte in einem digitalen Katastrophenfall schnelle Ersthilfe leisten.«

Aktuelle Vorfälle, die zunächst nach raffinierten Cyberangriffen aussehen, wie beispielsweise der in Frankreich und den Niederlanden, wo bei einem Angriff Mitte Oktober die Tiefkühlanlagen von Supermärkten aufgetaut wurden, zeigen aber auch, dass oftmals schwerwiegende Verantwortungslosigkeit in den Geschäftsleitungen der eigentliche Grund für solche Vorfälle sind – so auch in diesem Fall. Der Hersteller für die Steuerungsmodule, mit denen sich die Temperatur von Tiefkühlgeräten einstellen lässt, hat die absoluten Basismaßnahmen in der sicheren Softwareentwicklung nicht berücksichtigt. Das Management des Dienstleisters und der Supermärkte haben ihre Verantwortung zur Herstellung von sicheren Systemen schlicht nicht wahrgenommen, indem sie den Betrieb dieser Systeme ungeschützt aus dem Internet zuließen. Sie stellten, bildlich gesprochen, den Regelungsknopf der Temperatur aller Tiefkühlgeräte öffentlich vor den Eingang des Supermarktes und haben gehofft, dass keiner auf »warm« drehen würde. Die Probleme waren seit Monaten bekannt, aber Updates, die Verbesserungen gebracht hätten, wurden nicht eingespielt. Auch hierzulande werden ähnliche Geräte betrieben, die aus dem Internet erreichbar sind. Das BSI sollte als Aufsichtsbehörde die Geschäftsleitungen von solchen Unternehmen anschreiben und Stellungnahmen einfordern, ob ihre Systeme den geltenden NIS2-Cybersicherheitsvorgaben entsprechen, und wenn ein Gesetzesverstoß vorliegt, dann muss eine Strafe verhängt werden. Sofern wir die bestehenden Gesetze – allen voran den Datenschutz, das KRITIS-Dachgesetz und das BSI-Gesetz – wirklich durchsetzen würden, wären wir schon deutlich resilienter und souveräner.

Unabdingbar: Digitale Backups

Um digital resilient zu werden, braucht man als Basissicherheitsmaßnahme ein Backup, um die Daten wiederherzustellen. Dieses muss regelmäßig erstellt und offline aufbewahrt werden. Die Betriebe und Behörden müssen auch wissen und üben, wie man es schnell wieder einspielen kann – wenn das zehn Monate dauert, ist nichts gewonnen. Darüber hinaus brauchen wir ein Cyber-Hilfswerk nach dem Vorbild des Technischen Hilfswerks.[4] Nach der Ahrtal-Katastrophe 2021 ist das THW schnell ausgerückt und hat Behelfsbrücken gebaut, damit die Menschen notversorgt werden konnten.

4 AG KRITIS, Das Cyber-Hilfswerk, Konzept zur Steigerung der Bewältigungskapazitäten in Cyber-Großschadenslagen, ag.kritis.info, 23.3.2025.

Das haben wir im Digitalen nicht. Die Behörden in Anhalt-Bitterfeld konnten kein Sozialgeld auszahlen, keine Personalausweise und Reisepässe neu ausstellen und auch monatelang keine Autos zulassen. Ein kleines Beispiel macht das Grundproblem nachvollziehbar: Ein Autohaus kann so etwas eine Woche überbrücken, aber nicht Monate. Wenn es infolgedessen insolvent geht, werden die Mitarbeitenden arbeitslos, ihre Familien sind die Leidtragenden. In einem solchen Fall hat nicht das Autohaus etwas falsch gemacht, der Staat hat seine Kernfunktion nicht aufrechterhalten - aber dafür haftet niemand. Um bei bis zu 2000 kritischen Infrastrukturen solche Folgen zu verhindern, reicht das mobile Einsatzteam (MIRT) des BSI mit etwa 30 Leuten nicht aus. Ein Cyber-Hilfswerk könnte in einem digitalen Katastrophenfall unterstützende schnelle Ersthilfe leisten, damit die Bevölkerung weiter versorgt werden kann.

Regeln für KI als Katastrophenvorsorge

Auch bei der Verwendung von KI sollten im Bereich der kritischen Infrastrukturen klare Regeln gelten, um digital souverän bleiben zu können. Denn Unternehmen und Behörden haben erst die Hardware in Rechenzentren ausgelagert, dann die Daten und die Verarbeitungslogik in die Cloud überführt und jetzt geben sie die vollständige Geschäftslogik in den KI-Prompts ab. Jeder Prompt liefert den KI-Konzernen kostenlos Geschäftsgeheimnisse, Strukturdaten oder strategische Überlegungen. Es sollte beispielsweise auch verpflichtend sein, dass die Betreiber kritischer Infrastrukturen einen Quellcode verstehen und ihn dokumentieren und ihn nicht einfach als *vibe code* von einer KI generieren lassen und ihn dann nur noch nutzen. Nur so kann ich sichere Systeme betreiben. Was sonst droht, hat Constanze Kurz vom Chaos Computer Club »Inkompetenz zweiter Ordnung« genannt: Inkompetenz bedeutet, man weiß nicht, wie es geht. Inkompetenz zweiter Ordnung heißt, ich weiß nicht einmal, woran ich erkennen könnte, ob es funktioniert, oder welche Frage ich stellen müsste, um kompetente Beratende zu finden.

»Wir alle gemeinsam können ein Stück mehr Resilienz schaffen, ohne den Staat und die Unternehmen aus ihrer Verantwortung zu entlassen.«

Neben den beschriebenen staatlichen Maßnahmen und Vorgaben kann jede und jeder persönliche Vorsorgemaßnahmen ergreifen und sich als souveräne EU-Bürgerin und -Bürger selbstbestimmt ausstatten, um einen kurzen Ausfall von kritischen Infrastrukturen zu überbrücken. Aufgeladene Powerbanks helfen, das Mobiltelefon länger nutzbar zu halten. Wasser und Dosenvorräte helfen nicht nur mir selbst, sondern auch Nachbarinnen und Nachbarn, Hygieneartikel und Desinfektionsmittel und -tücher helfen, Keime zu entfernen und Infektionen zu verhindern. Und wenn man im sozialen Miteinander auch mal nach den Nachbarn schaut und prüft, wer zu den vulnerablen Gruppen gehört, wie etwa eine alleinerziehende Mutter mit einem Kleinkind oder ein 90-Jähriger mit Beatmungsgerät, der kann diesen im Notfall helfen und so die Rettungsdienste deutlich entlasten. Diese können dann den betroffenen vulnerablen Gruppen ohne Nachbarschaftshilfe zur Rettung eilen. So können wir alle gemeinsam ein Stück mehr Resilienz schaffen, ohne den Staat und die Unternehmen aus ihrer Verantwortung zu entlassen. ⬡