Die Schweiz fällt bei der Cybersicherheit zurück

Gemäss einem internationalen Ranking sind Länder wie Ghana, Tansania oder Serbien besser gegen Hackerangriffe gewappnet

GÉRALD KURTH

8,5 Billionen Franken. Auf diese unvorstellbar hohe Summe belaufen sich laut Cybersecurity Ventures die Schäden, die 2024 weltweit durch Cyberkriminalität verursacht wurden. Würde Cyberkriminalität wie das Bruttoinlandprodukt (BIP) eines Landes gemessen, entspräche sie – nach demjenigen der USA und Chinas – dem Volumen der drittgrössten Volkswirtschaft der Welt.

Die Schäden sind zehnmal so hoch wie das für 2024 prognostizierte BIP der Schweiz. Nicht mit eingerechnet sind hier die geschätzten Schäden von 15 Milliarden Dollar durch die weltweite Betriebsstörung von Rechnersystemen. Da sie keinen kriminellen Hintergrund haben, werden solche Störungen nicht mit eingerechnet. Der Grund für den hohen Störungsschaden war wohl die nicht ausgetestete Software-Aktualisierung des Cybersicherheitsanbieters Crowdstrike von vergangenem Sommer. Beim grössten IT-Zwischenfall der Geschichte blieben weltweit Flugzeuge am Boden, Spitäler standen praktisch still. 8,5 Millionen Windows-Computer, zumeist in kritischen Infrastrukturen mit hohen Sicherheitsanforderungen, waren ausser Betrieb.

Zum Vergleich: Im Gegensatz zu den Cyberschäden beliefen sich die Kosten von Naturkatastrophen im Jahr 2024 auf 350 Milliarden Franken. Im Gegensatz zu Murgängen und verschütteten Dörfern schafft es die gelähmte Infrastruktur eines Stromproduzenten allerdings seltener in die Öffentlichkeit. Dabei sind die durch aggressive Cyberakteure verursachten Kosten weltweit um den Faktor 25 höher.

Kleinwasserkraftwerke (im Bild eine Turbine) können ein Einfallstor für Cyberkriminelle sein. MANUEL LOPEZ / KEYSTONE

Erste Massnahmen ergriffen

Das gesellschaftliche und institutionelle Bewusstsein für die verheerenden Folgen von Cyberausfällen ist gering. Dazu passt, dass die Schweiz im Global Cybersecurity Index 2024 weiter abgerutscht ist. Die herausgebende International Telecommunication Union (ITU) bewertet darin die rechtlichen, technischen und organisatorischen Massnahmen sowie die Entwicklung von Cybersicherheitskapazitäten und Kooperationen eines jeweiligen Landes. Das ITU-Ranking beruht, neben dem Fokus auf Regulierung, auch auf Selbstdeklaration. In dieser Rangliste liegt die Schweiz zurzeit hinter von der ITU als vorbildlich eingestuften Ländern wie Ghana, Tansania oder Serbien.

Dabei hat Bundesbern in den letzten Jahren wegweisende Entscheide gefällt, um die Cybersicherheit der kritischen Infrastrukturen zu verbessern. Am 1. Januar 2024 wurde das Bundesamt für Cybersicherheit (Bacs) gegründet, das aus dem seit 2020 operativen Nationalen Zentrum für Cybersicherheit hervorgegangen ist. Das Bacs ist verantwortlich für die koordinierte Umsetzung der nationalen Cyberstrategie.

In der Wintersession 2024 hat das Parlament die Einführung einer Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen beschlossen. Ihre Umsetzung wird in der Cybersicherheitsverordnung festgelegt, die nächstens in Kraft tritt. Das Bundesamt für wirtschaftliche Landesversorgung hat einen IKT-(Informations-und-Kommunikationstechnik-)Minimalstandard entwickelt, der seit dem 1. Juli 2024 für die wichtigsten Stromversorger der Schweiz verbindlich ist. Dieser Standard definiert, abhängig von der Bedeutung eines Betriebs für das Gesamtsystem, unterschiedlich strenge Schutzniveaus.

Exponierte Stromversorgung

Warum aber schlagen sich all diese politischen und regulatorischen Präventionsmassnahmen nicht im ITU-Ranking nieder? Für Nick Mayencourt, Programmdirektor der diesjährigen Swiss Cyber Security Days, ist das keine Überraschung. Es sei positiv, dass an der Schnittstelle von Verwaltung und privaten Anbietern endlich ein Dialog eingesetzt habe. Der institutionelle Bewusstseinswandel hänge auch damit zusammen, dass die Warnungen aus seiner Branche zunehmend gehört würden. Die Angriffsflächen im Schweizer Cyberspace sind jedoch laut Mayencourt unverändert gross: «Wir können bei den dringenden Anstrengungen zur Härtung unserer kritischen Systeme wenig Fortschritte messen. Von digitaler Souveränität sind wir noch ein gutes Stück entfernt.»

Als Beispiel für die nach wie vor bestehenden Sicherheitslücken nennt Mayencourt die Schweizer Stromversorgung. Swissgrid sei hier «eine positive Anomalie», sagt er. Die Sicherheitskultur des nationalen Netzwerkbetreibers sei vorbildlich, aber leider nicht repräsentativ.

> Qualifizierte Experten sind rar und international begehrt. Der Schweiz fehlen gegen 10 000 Spezialisten.

Konkret bedeutet das: Sollten Cyberkriminelle in der Schweiz ein Blackout herbeiführen wollen, würden sie kaum die Festung Swissgrid angreifen. Wahrscheinlich würden sie sich Informationen über die Hardware in den noch immer etwa 1000 Kleinwasserkraftwerken der Schweiz beschaffen. Dabei könnten sie etwa herausfinden, welche Turbinen oder Generatoren in Betrieb sind. Stammen sie allenfalls von den gleichen Lieferanten? Die Angreifer dürften schnell feststellen, dass die oft veraltete Steuerungstechnik bei vielen Werken mit dem Internet und dem gesamten Stromnetz verbunden ist. An dieser Schnittstelle könnten sie eindringen und ihren Zugriff auf besser geschützte Infrastruktur ausweiten.

Der Cyber-GAU kann jederzeit passieren. Die kritischen Infrastrukturen der Schweiz sind durchdigitalisiert, das Gesamtsystem ist verletzlich. Cyberbewusste Betriebe wie Swissgrid setzen deshalb bewusst Hacker auf Schwachstellen in ihren Systemen an. Doch laut Mayencourt reicht dieses sogenannte ethische Hacking allein nicht. Es zeige nur die Verletzlichkeiten auf. Ebenso wichtig sei es, ein permanentes Monitoring einzurichten, um sofort reagieren und damit Kaskadeneffekte verhindern zu können. Mit regelmässigen Updates bekommt man laut Mayencourt viele potenzielle Gefahrenherde unter Kontrolle. Laut dem Nationalen Testinstitut für Cybersicherheit sind 60 Prozent aller Cyberangriffe auf nicht aktualisierte Software zurückzuführen und könnten billig vermieden werden.

Mit der Meldepflicht für Cyberangriffe und dem IKT-Minimalstandard für die wichtigsten Stromversorger hat der Bund einen Meilenstein erreicht. Warum aber schreibt er nicht gleich allen Betrieben Sicherheitsaudits vor? Mayencourt ist nicht der Einzige, der ausdrücklich «mehr staatliche Führung» fordert, um Sicherheitsüberprüfungen per Gesetz durchzusetzen.

Kleine Betriebe anfälliger

Dafür plädiert auch Aleksejs Okolovskis, Gründer der Swiss Cyber Security Platform: «Durch Rahmenverträge mit qualifizierten privaten Anbietern auf dem Markt könnten wir regulatorische Vorgaben mit pragmatischer Expertise verbinden», sagt er. Grundsätzlich gilt: Je kleiner der Betrieb, desto grösser die Anfälligkeit. Die Auslagerung der IT-Sicherheit kleiner Stromproduzenten mit knappen Budgets an sicherheitsüberprüfte private Dienstleister ist eine Option.

Doch wenn die Schweiz ihre kritischen Infrastrukturen messbar härten will, muss sie dafür viel mehr Personal bereitstellen. Qualifizierte Experten für Cybersicherheit sind rar und international begehrt. Okolovskis ist auch Präsident der Schweizer Filiale von ISC2, einer weltweit tätigen Trainings- und Zertifizierungsorganisation für Cybersicherheit. Er möchte diesen Mangel kurzfristig mit Weiterbildungen und der Rekrutierung internationaler Fachkräfte auffangen.

Im Kampf gegen den «Cyber Talent Gap» brauche es zudem einen unverzüglichen nationalen Schulterschluss: «Wenn alle relevanten Akteure – Bund, Kantone, Wirtschaft und Bildungsinstitutionen – an einem Strang ziehen, bringen wir schnell mehr qualifizierte Fachkräfte in den Markt», sagt er. Die USA bezifferten 2024 ihren sofortigen Bedarf an solchen Cybercracks auf mindestens eine Viertelmillion. Der Schweiz fehlen gegen 10 000 Spezialisten.

Ausbildungszertifikate sollten dabei auch aufgrund der Dringlichkeit nur eine untergeordnete Rolle spielen. Okolovskis betont zwar, dass die sogenannte CISSP-Zertifizierung des ISC2 seit 30 Jahren Industriestandard für hoch qualifizierte Fachkräfte sei. Mayencourt hingegen findet, schnelle Lösungen für zeitkritische Sicherheitsprobleme seien wichtiger als Zertifikate: «Ich gebe einen dringenden Auftrag lieber dem versierten Praktiker als jemandem mit allen formalen Qualifikationen, der das Problem nur beschreibt.»

Tatsache ist: Die Angreifer schlafen nicht, die Angriffe auf die schwächsten Glieder der kritischen Infrastrukturen nehmen zu. Will sich die Schweiz schützen, muss sie in die Ausbildung von Cyberspezialisten investieren.

Neue Kriegslogistik kostet hohen zweistelligen Millionenbetrag

Die Eidgenössische Finanzkontrolle liefert erstmals Zahlen zur dringend benötigten Neuausrichtung

SELINA BERNER, BERN

Bis zu Beginn des Angriffs auf die Ukraine schien ein Konflikt in Europa undenkbar. Nach dem Kalten Krieg rüsteten viele Länder deshalb ab und hielten lediglich eine minimale Verteidigungsfähigkeit aufrecht. Doch die Welt ist seit Februar 2022 eine andere. Und die mehr als dreissig Jahre Friedensdividende haben ihre Spuren hinterlassen. Europa rüstet nach, so auch die Schweiz. Alte Kampfsysteme sollen durch moderne ersetzt werden und die Logistik umgestellt auf Kriegstauglichkeit. Wie viel Letzteres genau kostet, war bis anhin unbekannt. Die Eidgenössische Finanzkontrolle (EFK) schreibt nun in einem Bericht von einem Betrag im «hohen zweistelligen Millionenbereich».

Die Logistik der Schweizer Armee wurde in den letzten Jahrzehnten zentralisiert auf fünf Logistikzentren. Sie erbringen die Basis-Logistikleistungen und dienen als Truppenwerkstatt. Die Zentralisierung mit Hochregallager ist effizient und kostensparend. Alle fünf Standorte sind jedoch bekannt, was im Kriegsfall ein erheblicher Nachteil wäre. Sobald beispielsweise Langstreckenraketen zum Einsatz kämen, wären die Logistikzentren als militärische Ziele gefährdet.

«Bereitschaft auf Stufe 3 von 10»

Die Armee arbeitet gegenwärtig an einem Konzept für die Dezentralisierung in unterirdische Anlagen, wie der Chef der Logistikbasis, Divisionär Rolf André Siegenthaler, kürzlich in einem Interview mit der NZZ erklärte. Es gebe genügend Platz in den Militäranlagen. Doch nur für jenes Material, welches die Armee momentan besitzt. Da bei einer Mobilmachung derzeit nur rund ein Drittel der Soldaten voll ausgerüstet werden könnte, reichen diese Anlagen im Konfliktfall kaum aus. Der Nachholbedarf im Logistikbereich sei gross, sagt Siegenthaler. Auf einer Skala von 1 bis 10 würde die Bereitschaft für einen Krieg «etwa auf Stufe 3» liegen.

Die EFK schreibt in ihrem Bericht, dass sich «bereits heute» abzeichne, dass eine kriegstaugliche Logistik Kosten im «hohen zweistelligen Millionenbereich» verursachen werde. Die Finanzierung solle im Rüstungskredit von 2027 sichergestellt werden und die Kriegslogistik dann «frühestens 2030 bereitstehen».

Im Oktober klang es noch anders. Ein Bericht von SRF sorgte damals für Aufsehen. Zitiert wurde der ehemalige Chef Armeestab. In einer parlamentarischen Aufsichtskommission soll er gesagt haben: Die Kriegslogistik werde «erst nach 2035» angegangen, die finanziellen Mittel seien derzeit zu knapp.

Planung beginnt 2027

Die EFK hat sich in ihrem jüngsten Bericht mit der Prozess-Software für die zivile Militärlogistik beschäftigt. Diese läuft mit dem Planungssystem des deutschen Softwareentwicklers SAP. Für den einsatzkritischen Bereich sucht die Armee allerdings eine andere Lösung. SAP sei zu komplex und zu teuer, um sie für den Kriegsfall sicher zu machen, so Rolf André Siegenthaler.

Für die Umstellung auf Kriegslogistik brauche es jedoch deutlich mehr als nur eine krisensichere Software, mit der die Soldaten den Nachschub an die Front koordinieren müssten, schreibt die Armee. Es gehe «um Bauten, um Infrastrukturen, um Immobilien, um Bevorratung».

Es ist nicht das erste Mal, dass sich die EFK mit der Militärlogistik auseinandersetzt. Im letzten Bericht empfahl sie der Armee, das Programm für die Kriegslogistik in einem Nachfolgeprojekt zu realisieren. Es wurde deshalb getrennt vom zivilen SAP-Projektteil. Damit fielen die Projektkosten um insgesamt 3,5 Millionen Franken tiefer aus. Wie viel eine robuste Logistik-Software kosten würde, weiss die Armee allerdings noch nicht. Eine Studie soll Klarheit bringen. «Voraussichtlich ab 2027» könne «mit der Planung und Erstellung eines solchen Logistiksystems» begonnen werden, schreibt die Armee auf Anfrage.