„Digitale Verteidigung“ ist nicht nur eine Frage technischer Leistungsfähigkeit: Können politische Entscheidungsstrukturen mit der Geschwindigkeit der Systeme mithalten? Die eigentliche Herausforderung lautet: Digitale Verteidigungsfähigkeit darf nicht zur unbeabsichtigten Eskalationsmaschine werden. Und: Wer zieht im Ernstfall die Bremse? Von **Günther Burbach**.

Dieser Beitrag ist auch als Audio-Podcast verfügbar.

https://www.nachdenkseiten.de/upload/podcast/260302_Cyberabwehr_unter_Zeitdruck_ein_Szenario_das_schnell_eskalieren_koennte_NDS.mp3

Podcast: Play in new window | Download

Es ist 03:17 Uhr. In mehreren europäischen Rechenzentren schlagen nahezu zeitgleich Anomaliealarme an. Netzwerkverkehr aus unterschiedlichen Regionen wird von KI-gestützten Systemen als hochgradig verdächtig eingestuft. Die Muster ähneln bekannten Vorbereitungsphasen koordinierter Angriffe auf Energie- und Kommunikationsinfrastruktur. Die Modelle berechnen eine hohe Wahrscheinlichkeit, dass es sich nicht um isolierte Vorfälle handelt, sondern um eine orchestrierte Operation.

Innerhalb von Sekunden beginnt das automatisierte Abwehrprotokoll. Verbindungen werden isoliert, externe Server blockiert, Datenströme umgeleitet. In bestimmten Segmenten werden Systeme vorsorglich vom Netz getrennt, um eine mögliche Ausbreitung zu verhindern. Die Eingriffe bleiben zunächst intern. Doch ein Teil der Gegenmaßnahmen betrifft Infrastruktur außerhalb des eigenen Hoheitsgebiets. Routing-Tabellen werden angepasst, bestimmte Netzknoten aktiv ausgefiltert. Der Vorgang ist technisch defensiv motiviert, aber seine Wirkung bleibt nicht auf das eigene Netz beschränkt.

Gegen 03:29 Uhr registrieren Betreiber in einem Drittstaat erhebliche Störungen. Kommunikationsverbindungen brechen ab, Teile ihrer Infrastruktur verlieren die Verbindung zu europäischen Netzen. Wenige Minuten später beginnt dort eine interne Untersuchung. Auch dort schlagen Sicherheitssysteme an. Die KI-Modelle klassifizieren die Störungen als mögliches feindliches Eingreifen. Automatisierte Schutzmechanismen werden aktiviert. Gegenmaßnahmen setzen ein.

Was in Europa als präventive Verteidigung begonnen hat, wird anderswo als aktiver Eingriff interpretiert. Die Attribution der ursprünglichen Anomalien ist zu diesem Zeitpunkt nicht gesichert. Digitale Spuren deuten auf verschiedene Zwischenstationen hin. Es ist unklar, ob

es sich um staatliche Akteure, kriminelle Gruppen oder eine Fehlkonfiguration handelt. Die Modelle arbeiten mit Wahrscheinlichkeiten, nicht mit Gewissheit. Doch die Systeme reagieren, weil sie reagieren sollen.

Während technische Prozesse in Sekunden ablaufen, bewegt sich die politische Ebene in Minuten. Krisenstäbe werden informiert. Außenministerien prüfen Lagebilder. Militärische Ansprechpartner tauschen erste Informationen aus. Doch zu diesem Zeitpunkt sind bereits wechselseitige Schutzmaßnahmen aktiv. Die öffentliche Wahrnehmung beginnt sich zu formen. Erste Medienberichte sprechen von „Cyberangriff“ und „Gegenreaktion“. Der Begriff „Eskalation“ fällt, bevor die Sachlage geklärt ist.

Dieses Szenario ist keine Fantasiegeschichte. Es ist die logische Zuspitzung zweier Entwicklungen, die längst Realität sind: hochautomatisierte Abwehrsysteme und eine geopolitisch angespannte Welt. Je stärker Cyberabwehr auf KI-gestützte Echtzeitanalyse setzt, desto kürzer wird das Zeitfenster für politische Einordnung. Und je enger digitale Infrastrukturen global verflochten sind, desto größer ist die Wahrscheinlichkeit, dass defensive Maßnahmen grenzüberschreitende Auswirkungen haben.

Die politische Kernfrage lautet nicht, ob Staaten sich verteidigen dürfen. Diese Frage ist unstrittig. Die Kernfrage lautet, wie stabil eine Sicherheitsarchitektur ist, wenn Verteidigung und Gegenmaßnahme technisch ineinandergreifen.

Klassische Sicherheitslogik kennt Eskalationsstufen. Militärische Aktionen durchlaufen Entscheidungsprozesse, die, zumindest formal, politische Zustimmung erfordern. Im Cyberraum hingegen werden Reaktionen zunehmend in Softwarearchitekturen vorstrukturiert. Playbooks, Schwellenwerte und automatische Response-Ketten definieren, was bei welchem Muster geschieht.

Jeder Schritt wird vom anderen als Bedrohung interpretiert

Diese Vorstrukturierung ist nachvollziehbar. Angriffe können sich in Sekunden ausbreiten. Eine rein manuelle Reaktion wäre zu langsam. Doch Geschwindigkeit ist nicht nur ein Vorteil. Sie verändert die Eskalationsdynamik. Wenn zwei Systeme, die beide auf schnelle Reaktion ausgelegt sind, aufeinandertreffen, entsteht eine Rückkopplungsschleife. Jeder Schritt wird vom anderen als Bedrohung interpretiert. Das Problem liegt nicht in böser Absicht, sondern in der Logik automatisierter Sicherheit.

Hinzu kommt ein zweiter Faktor: infrastrukturelle Abhängigkeit. Viele der eingesetzten Systeme – von der Cloud-Infrastruktur über KI-Frameworks bis hin zu Threat-Intelligence-

Feeds, basieren auf globalen Plattformen. Ihre Wartung, Aktualisierung und teilweise auch ihre Kernfunktionen unterliegen externen Rechtsräumen. In stabilen Zeiten ist das kein unmittelbares Problem. Doch in einem geopolitischen Konfliktumfeld können regulatorische Eingriffe, Exportbeschränkungen oder politische Spannungen indirekt auf diese Systeme wirken.

Stellen wir uns vor, das oben skizzierte Szenario spielt sich in einer Phase politischer Konfrontation ab. Handelskonflikte, Sanktionsregime oder militärische Spannungen bilden den Hintergrund. Jede technische Maßnahme wird in diesem Kontext politisch gelesen. Eine automatisierte Netzisolierung wird nicht nur als Sicherheitsmaßnahme wahrgenommen, sondern als Signal. Gleichzeitig könnte die Verfügbarkeit bestimmter Updates oder Supportleistungen durch politische Entscheidungen beeinflusst werden. Die Verteidigungsarchitektur operiert damit nicht im luftleeren Raum, sondern im Spannungsfeld internationaler Machtpolitik.

Das eigentliche Risiko liegt daher nicht allein in der Möglichkeit eines Fehlalarms. Es liegt in der Kombination aus beschleunigter Automatisierung und struktureller wechselseitiger Abhängigkeit. Je enger Systeme global verflochten sind, desto stärker wirken sich Maßnahmen über Grenzen hinweg aus. Je schneller diese Maßnahmen erfolgen, desto geringer ist die Chance, sie politisch einzuhegen, bevor sie Wirkung entfalten.

Die klassische Vorstellung von Eskalation geht von klaren Handlungen aus: Angriff, Reaktion, Gegenreaktion. Im digitalen Raum ist diese Sequenz oft unscharf. Maßnahmen können gleichzeitig defensiv motiviert und offensiv wahrgenommen werden. Attribution bleibt unsicher. Die beteiligten Systeme handeln innerhalb definierter Parameter, doch diese Parameter sind selbst politische Entscheidungen in kodierter Form. Wer die Schwellenwerte festlegt, definiert implizit die Eskalationsbereitschaft.

In einem solchen Szenario wird deutlich, dass digitale Verteidigung nicht nur eine Frage technischer Leistungsfähigkeit ist. Sie ist eine Frage politischer Synchronisation. Können Entscheidungsstrukturen mit der Geschwindigkeit der Systeme mithalten? Gibt es klar definierte Eskalationsbremsen? Sind internationale Kommunikationskanäle robust genug, um Missverständnisse schnell aufzuklären? Und vor allem: Ist die Verteidigungsarchitektur so gestaltet, dass sie auch unter politischem Druck stabil bleibt?

Eine Cyberabwehr, die nur unter idealen politischen Bedingungen störungsfrei funktioniert, ist keine robuste Abwehr. Sie ist eine Abwehr im Schönwetterbetrieb. Resilienz zeigt sich im Ausnahmefall. Das bedeutet nicht, Automatisierung zurückzudrehen oder internationale Kooperation aufzugeben. Es bedeutet jedoch, die strukturellen Risiken offen zu benennen

und in die Architektur einzubauen.

Das oben skizzierte Szenario ist kein Aufruf zur Panik. Es ist eine analytische Übung. Sie verdeutlicht, dass digitale Sicherheit heute in einem dichten Geflecht aus Technologie, Politik und globaler wechselseitiger Abhängigkeiten operiert. Wer diese Ebenen getrennt betrachtet, unterschätzt das Zusammenspiel. Wer sie zusammen denkt, erkennt die eigentliche Herausforderung: Verteidigungsfähigkeit darf nicht zur unbeabsichtigten Eskalationsmaschine werden.

Wer zieht im Ernstfall die Bremse?

Das beschriebene Szenario ist nicht deshalb beunruhigend, weil es spektakulär wäre, sondern weil es strukturell plausibel ist. Hochautomatisierte Systeme reagieren in Sekunden. Politische Entscheidungsprozesse benötigen Zeit. Und digitale Infrastruktur ist global verflochten. Entscheidend ist daher nicht, ob ein solcher Vorfall möglich ist, sondern wie eine demokratische Sicherheitsarchitektur darauf vorbereitet wäre.

Die zentrale Frage lautet: Wer zieht im Ernstfall die Bremse? In klassischen militärischen Konstellationen existieren formalisierte Eskalationsstufen. Politische Freigaben sind erforderlich, Kommunikationskanäle sind etabliert, Verantwortlichkeiten klar zugeordnet. Im Cyberraum ist die Lage komplexer. Viele Maßnahmen laufen unterhalb der Schwelle eines offenen Konflikts. Sie bewegen sich in Grauzonen, in denen juristische Definitionen, etwa die Frage nach einem „bewaffneten Angriff“, nicht eindeutig greifen. Die operative Reaktion wird zunehmend in technischen Playbooks vorab festgelegt.

Diese Vorab-Festlegung ist notwendig, um Geschwindigkeit zu gewährleisten. Doch sie wirft eine heikle Frage auf: Wie flexibel sind diese Playbooks, wenn sich die politische Lage ändert? Werden Schwellenwerte dynamisch angepasst? Gibt es eine institutionalisierte Möglichkeit, automatisierte Prozesse temporär zu verlangsamen oder zu pausieren? Oder laufen Systeme weiter, weil sie auf maximale Effizienz optimiert wurden?

Eine demokratische Verteidigungsarchitektur muss zwischen Routineabwehr und strategisch sensiblen Maßnahmen unterscheiden. Das Isolieren eines kompromittierten Servers ist eine operative Frage. Das gezielte Blockieren externer Infrastruktur mit potenziell grenzüberschreitender Wirkung ist eine politische Frage. Wenn diese Unterscheidung nicht klar institutionalisiert ist, verschwimmen technische und politische Ebenen.

Hinzu kommt die internationale Dimension. In einem angespannten geopolitischen Umfeld

werden technische Vorfälle politisch gelesen. Ein automatisierter Eingriff kann als Signal gewertet werden, selbst wenn er rein defensiv motiviert war. Deshalb braucht digitale Verteidigung belastbare Kommunikationskanäle zwischen Staaten, die auch in Krisensituationen funktionieren. Transparenz über Grundprinzipien, nicht über operative Details, kann Eskalationsspiralen dämpfen.

Doch selbst bei optimaler Kommunikation bleibt ein strukturelles Problem bestehen: die Abhängigkeit von globalen Plattformen. Wenn zentrale Sicherheitskomponenten auf Infrastruktur basieren, die außerhalb des eigenen Rechtsraums betrieben wird, entsteht ein zusätzlicher Unsicherheitsfaktor. In einer geopolitischen Krise könnten regulatorische Entscheidungen, Exportbeschränkungen oder politische Vorgaben indirekt die technische Funktionsfähigkeit beeinflussen. Eine Verteidigungsarchitektur darf nicht darauf angewiesen sein, dass externe Rahmenbedingungen dauerhaft stabil bleiben.

Das bedeutet nicht, internationale Kooperation infrage zu stellen. Es bedeutet, Kernfunktionen zu identifizieren, die im Zweifel autonom betrieben werden müssen. Dazu gehören besonders sensible Analyseprozesse, Lagebilderstellung und kritische Kommunikationswege. Redundanz ist hier kein Luxus, sondern Teil strategischer Vorsorge. Systeme sollten so gestaltet sein, dass sie auch dann weiterarbeiten können, wenn einzelne externe Komponenten temporär nicht verfügbar sind.

Ein weiterer Punkt betrifft die Nachvollziehbarkeit automatisierter Entscheidungen. KI-gestützte Systeme operieren auf Basis von Modellen, Trainingsdaten und definierten Schwellenwerten. Diese Parameter sind nicht naturgegeben, sondern politisch gerahmt. Wer legt fest, ab welcher Wahrscheinlichkeit eine Maßnahme ausgelöst wird? Wer definiert die Toleranz gegenüber Fehlalarmen? Und wer überprüft diese Festlegungen regelmäßig? Ohne institutionalisierte Audit-Mechanismen droht eine Entkopplung von politischer Verantwortung und technischer Umsetzung.

Demokratische Kontrolle im Cyberbereich kann nicht bedeuten, jede einzelne technische Entscheidung öffentlich zu diskutieren. Sie muss jedoch sicherstellen, dass Entscheidungsarchitekturen transparent und überprüfbar bleiben. Parlamente sollten zumindest die Grundlogik automatisierter Reaktionsketten kennen und evaluieren können. Wenn Cyberabwehr als Teil staatlicher Sicherheitsgewalt verstanden wird, darf sie nicht ausschließlich in technischen Expertengremien verhandelt werden.

Die eigentliche Herausforderung liegt somit nicht in der Existenz von KI oder globaler wechselseitiger Abhängigkeit. Sie liegt in der Kombination beider Faktoren unter Zeitdruck. Ein System, das schnell reagiert und gleichzeitig strukturell abhängig ist, operiert unter

doppelter Spannung. Geschwindigkeit reduziert das politische Reaktionsfenster. Abhängigkeit erhöht die Sensibilität gegenüber externen Rahmenbedingungen.

Digitale Verteidigung muss deshalb bewusst entschleunigende Elemente enthalten. Das klingt paradox, ist aber strategisch sinnvoll. Nicht jede automatisierte Reaktion muss maximal schnell sein. Für Maßnahmen mit potenziell externer Wirkung kann eine zusätzliche Prüfinstanz vorgesehen werden. Technische Effizienz darf nicht das einzige Kriterium sein. Stabilität und politische Einhegung sind gleichwertige Ziele.

Langfristig stellt sich zudem die Frage nach technologischer Schwerpunktsetzung. Wenn Europa digitale Souveränität ernst meint, muss es gezielt in Schlüsseltechnologien investieren, nicht aus protektionistischen Motiven, sondern aus Resilienzüberlegungen. Eigene Kompetenzen in sicherheitsrelevanter KI, Cloud-Infrastruktur und Halbleiterfertigung stärken die Verhandlungsmacht und reduzieren strukturelle Verwundbarkeit. Vollständige Autarkie ist unrealistisch, aber strategische Eigenständigkeit ist erreichbar.

Am Ende bleibt eine nüchterne Erkenntnis: Cyberabwehr ist kein rein technisches Upgrade staatlicher Sicherheit. Sie ist ein politisches Projekt im Spannungsfeld globaler wechselseitiger Abhängigkeiten und beschleunigter Automatisierung. Ein System, das nur im Normalbetrieb stabil ist, verdient nicht den Namen Resilienz. Ein System, das schnell reagiert, aber politisch unzureichend eingebettet ist, trägt Eskalationsrisiken in sich.

Die Frage ist daher nicht, ob Staaten ihre digitale Verteidigungsfähigkeit ausbauen sollen. Die Frage ist, wie sie diese Fähigkeit so gestalten, dass sie auch unter geopolitischem Druck und technischer Beschleunigung kontrollierbar bleibt. Wer Sicherheit verspricht, muss auch zeigen, wie er im Ernstfall die Bremse zieht.

Quellen:

- Cybersicherheitsstrategie für Deutschland 2021 – Bundesministerium des Innern
- Richtlinie (EU) 2022/2555 – NIS-2-Richtlinie zur Netz- und Informationssicherheit
- Verordnung (EU) 2024/1689 – EU Artificial Intelligence Act
- NATO Cyber Defence Policy – Offizielle NATO-Doktrin zur Cyberverteidigung
- Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations – NATO

CCDCOE

- U.S. CLOUD Act (Clarifying Lawful Overseas Use of Data Act) – US-Kongress

Titelbild: Marko Aliaksandr / Shutterstock.com