Resilienz kritischer Infrastrukturen: Keine Chance dem Blackout

Dr. Michael Littger, Geschäftsführer von Deutschland sicher im Netz e.V (DsiN)

Es war ein kalter Februartag, als der Informatiker Piero Manzano in einen Verkehrsunfall verwickelt wurde, weil alle Stromnetze in Europa ausfielen und mit ihnen die Ampelsysteme, Kommunikation, Trinkwasserversorgung. Der Beginn dieser Erzählung stammt aus dem Bestseller “Blackout” von Marc Elsberg, doch zeigen Verflechtungen und Vernetzung des Romans die Quellen einer gesellschaftlichen Verletzlichkeit, die in der Sicherheitspolitik zu einem neuen Paradigma geführt haben: Resilienz. Ursprünglich von der Psychologie verwendet, um Menschen mit hoher Krisenbelastbarkeit zu beschreiben, zielt Resilienz in der IT-Sicherheit auf bestmögliche Beherrschung von Gefährdung und Schadenswirkung, um im Krisenfall schnell zur Normalität zurückzukehren.

Heutige Forderungen nach Resilienz erfolgen meist im Zusammenhang mit Kritischen Infrastrukturen. Diese umfassen – in den Worten des früheren Bundesinnenministers – solche Systeme, bei denen es kritisch wird, wenn sie ausfallen. Sie müssen schon heute besondere Sicherheitsanforderungen erfüllen. Künftig wird es zusätzlich auf solche Akteure ankommen, die über digitale Vernetzung in sonstiger Weise mit Kritischen Infrastrukturen zu tun haben – wie die hunderttausende kleinen und mittleren Betriebe. Der Grund liegt in der steigenden Wechselseitigkeit von Gefährdung der und Abhängigkeit von der Digitalisierung, die im Begriff der Industrie 4.0 abgebildet werden, aber weit darüber hinausreichen.

Es geht um die Resilienz der Gesellschaft, in der bewährte Schablonen der IT-Sicherheit ihre Gültigkeit verlieren. So beschreibt der BSI-Lagebericht ein Bedrohungs- und Gefährdungsbild, das durch Sabotage, Spionage, Technikversagen, Naturkatastrophen sowie Sorglosigkeiten im Berufsalltag geprägt ist und nicht länger nach Innen und Außen differenziert.
Auch klassische Verantwortungszuschnitte der IT-Sicherheit büßen in dem Maße an Bedeutung ein, wie holistische Betrachtungsweisen an Bedeutung gewinnen. Und anstelle einzelner Gefährdungen wird die Vermeidung von Schadenseintritten zur zentralen Frage, die aus der allgemeinen Verwundbarkeit der digital vernetzten Gesellschaft erfolgt. Um dem Blackout Kritischer Infrastrukturen und seinen Folgen entgegenzuwirken, wird es darauf ankommen, die Resilienz der digitalen Gesellschaft zu stärken. Alle Schutzfaktoren von Wirtschaft, Staat und Gesellschaft müssen wirksam ineinander greifen. Zur Veranschaulichung hilft das Modell einer Zwiebel, deren Ringe den Einzelnen schützen und ihn zugleich einbinden. Eine erste Annäherung lässt vier Kreise erkennen:

Zwiebelmodell: Resilienz

1) Der äußere Ring steht für die internationale Verantwortung. Sie ermöglicht eine Orientierung zu grenzüberschreitenden und global abgestimmten Lösungsansätzen. Plattformen für entsprechende Verabredungen bieten Gesprächsforen der G20 und G7, das Internationale Governance Forum (IGF) sowie die Vereinten Nationen (UN).

2) Regulatorische Schutzmechanismen werden dem zweiten Ring zugeordnet. Rechtsvorgaben können Schutz und Sicherheit stärken. Die NIS-Direktive auf europäischer Ebene adressiert vorrangig Kritische Infrastrukturen. Auch Sondergesetze enthalten relevante IT-Sicherheitsanforderungen sowie auch die EU-Datenschutz-Grundverordnung (DSGVO). Die Aussicht eines zweiten IT-Sicherheitsgesetzes ist Gegenstand des Fachkongress PITS (Public-IT-Security) 2018.

3) Auf dem dritten Ring finden sich technologisch getriebene Innovationen der Wirtschaft als Schutzfaktor einer resilienten Gesellschaft. Sie wenden sich an KMU und bieten auch Kritischen Infrastrukturen Lösungsansätze. Sie stehen in gewisser Abhängigkeit zur Regulierung und können auch durch Sicherheitsstandards oder Empfehlungen wie dem BSI-Grundschutz beeinflusst werden.

4) Im Kern des Zwiebelmodells stehen Anwender und Nutzer – KMU, Behörden sowie Einzelpersonen. Sie tragen Verantwortung für eigene Betriebe sowie auch für Vorkehrungen gegen kleinere Vorfälle bis hin zum Ausfall (kritischer) Versorgungsleistungen. Über DDoS-Attacken können sie selbst zum Risiko auch für Betreiber Kritischer Infrastrukturen werden.
Mehr Abwehrfähigkeit durch digitale Aufklärung

Die Wirkungen und das Verhältnis der benannten Schutzfaktoren zueinander bedürfen weiterer Diskussionen. Augenfällig ist aber das Nachholbedürfnis von KMU bei IT-Sicherheit im Kern des Modells: Es geht um nicht geschulte Mitarbeiter bis zu fehlenden Notfallplänen. Angebote in der beruflichen Ausbildung, wie das Projekt “Bottom-Up”, fördern das Grundverständnis für Sicherheit am Arbeitsplatz. Auch der Erfahrungsaustausch untereinander, wie ihn die IT-Sicherheit@Mittelstand in Kooperation mit dem Deutschen Industrie- und Handelskammertag ermöglicht, wird wichtiger. Diese Angebote sollten von Betrieben stärker angenommen werden. Die Bundesregierung hat mit dem Beschluss im Koalitionsvertrag, die digitale Befähigung in der Gesellschaft und Wirtschaft für mehr Cyber-Sicherheit zu verstärken, das Problem der digitalen Aufklärung klar adressiert. Hier wird es darum gehen, Themenfelder, Akteure und Zielgruppen so einzubinden, dass die Abwehrfähigkeit der Gesellschaft gegen digitale Bedrohungen in der Gesamtheit wirksam verbessert wird.

Dieser Beitrag erscheint auch in der Augustausgabe im Behörden Spiegel sowie in der Sonderausgabe des Behörden Spiegel Newsletters „E-Government“, der sich ganz der PITS 2018 widmet.

Dr. Michael Littger ist Geschäftsführer von Deutschland sicher im Netz e.V (DsiN). Der Verein informiert Bürger und Unternehmen zu aktuellen Fragen der IT-Datensicherheit – mit konkreter Hilfestellung für den Alltag. Zuvor war Littger im Deutschen Industrieverband (BDI) für Digitale Wirtschaft, Telekommunikation und Medien zuständig. Schwerpunkte seiner Arbeiten liegen auf dem Gebiet des Cloud Computings und Datenschutzes.