Resilienz: Systeme sicher für Krisenfälle aufstellen

Ausgangssituation

Die Corona-Pandemie hat die Verwundbarkeit von Organisationen, Unternehmen und gesellschaftlichen Prozessen aufgezeigt. Gleichzeitig haben technische Systeme wie Internetanwendungen – bei allen Schwächen im Detail – ihre Bedeutung insbesondere im Lockdown aufgezeigt: Homeoffice und Homeschooling wären in dieser Form noch vor wenigen Jahren undenkbar gewesen, Parteitage im digitalen Raum kategorisch ausgeschlossen worden.

Problemlage

Dieses neue Bewusstsein mit all seinen digitalen Erkenntnissen muss jetzt genutzt werden, um das Thema „Resilienz technischer Systeme“ umfassend zu analysieren:

- **Kommunikation**: Leistungsstarke Internetverbindungen sind ein wichtiger Schlüssel für die Resilienz (Widerstandsfähigkeit) technischer Systeme. Unerlässlich dafür sind mehr Glasfaserverbindungen.

  Gleichwohl fehlen bei Digitalnetzen – im Gegensatz zu Installation und Betrieb der Gas- und Wassernetze – aktuell taugliche Regelwerke, die über viele Jahrzehnte gereift sind und sich bewährt haben. Gerade für den Krisenfall resultieren daraus Gefahren. Zudem nimmt bei steigender digitaler Kommunikation die Gefahr von Cyberattacken zu.

- **Energie**: Im Zuge der Energiewende wird die Stromerzeugung in Deutschland dezentralisiert. Hausbesitzer können Strom ihrer Solaranlagen in die Netze einspeisen, ebenso Betreiber von Windkraft- oder Biogasanlagen. Das steigert einerseits die Resilienz gegenüber Gefahren wie Terroranschläge auf große Kraftwerke. Andererseits steigt die Zahl digitaler Schnittstellen massiv. Mehr Vernetzungen heißt auch mehr Gefahrenpotenzial für Cyberangriffe. Die Elektrizitätsversorgung ist die entscheidende kritische Infrastruktur. Jeder andere Sektor ist davon abhängig. Ein länger anhaltender „Blackout“ hat fatale Folgen.

- **Gesundheit**: Gerade in Krisensituationen muss der Gesundheitssektor seine Leistungskraft unter Beweis stellen. Das Zusammenspiel der ärztlichen Versorgung mit digitalen Techniken bietet erhebliche Potenziale, die bislang weitgehend unausgeschöpft sind. Bestes Beispiel ist die elektronische Gesundheitskarte, die in Sachen Datenspeicherung weit hinter ihren technischen Möglichkeiten zurückbleibt.

- **Lieferketten**: Zu Beginn der Corona-Pandemie gab es massive Störungen der weltweiten Lieferketten. Deutschlands Schlüsselindustrien wie Chemie, Maschinenbau und Automobilindustrie waren erheblich betroffen. Selbst bei lebensnotwendigen Gütern wie Medikamenten und Medizinprodukten traten Versorgungsengpässe auf. Manche dieser Engpässe kamen überraschend, insbesondere dort, wo Lieferketten nicht transparent waren.

Wo sollte die Politik anpacken?

Die Politik muss Anreize und Rahmenbedingungen für die Ausgestaltung resilienter Systeme schaffen. Dazu gehört insbesondere:

- **Gefahrenszenarien durchspielen:** Wie Deutschland auf eine Pandemie reagiert, konnte in den vergangenen Monaten beobachtet werden. Wie aber steht es bei anderen Gefahrenszenarien wie extreme Hitzewellen oder Naturkatastrophen? Sie sollten häufiger durchgespielt und auch weitreichende Ereignisse politischer Art analysiert und diskutiert werden. Krisenübungen mit konkreten Szenarien sollten von einem neutralen Technologiepartner begleitet werden.
- **Cyberssicherheit stärken:** Die Cyber-Sicherheitsstrategie (CSS) von 2016 wird derzeit überarbeitet. Wesentliche Themen lauten: Schnellere Reaktionszeit bei Gefahrenlagen sicherstellen, KMU gezielt unterstützen, Standardisierung und Zertifizierung vorantreiben, Informationsaustausch zwischen Staat und Wirtschaft verbessern und bei Schlüsselprojekten wie GAIA-X sichere Hardware verbauen.
- **Breitband vorantreiben:** Der Bund sollte die Telekommunikationsbetreiber auf einen raschen und qualitativ angemessenen Glasfaser-Ausbau verpflichten. Der immer wieder diskutierte Rückfall auf kupferbasierte „Brückentechnologien“ würde Deutschland nur noch weiter ins digitale Abseits führen. Hier wurde schon zu viel Zeit verschwendet.
- **Daten nutzbar machen:** Digitalen Techniken und insbesondere Anwendungen der Künstlichen Intelligenz im Gesundheitsbereich stehen derzeit zahlreiche regulatorischen Hürden gegenüber. Sie sollten datenschutzkonform überwunden werden, um die medizinische Versorgung insbesondere in Krisensituationen dauerhaft zu verbessern.

Wie kann der VDE unterstützen?

Sicherheit ist der Kernbestandteil der DNA des VDE. Deshalb kann die Technologieorganisation in vielfältiger Form Politik und Wirtschaft unterstützen:

- **Szenarien:** Der VDE kann die vielfältigen Stakeholder aus Industrie, Politik und Gesellschaft zur Entwicklung breit getragener Zukunftsbilder und Szenarien zusammenführen. So hat der VDE beispielsweise Leitfragen zum Stellenwert der Künstlichen Intelligenz 2025 oder das Zusammenspiel von Ärztinnen und Ärzten und digitaler Technik im Jahr 2035 bearbeitet.
- **Positionspapiere:** Der VDE veröffentlicht regelmäßig Positionspapiere mit Resilienz-Bezügen. So hat VDE FNN (Forum Netztechnik/Netzbetrieb) 2020 Politik und Behörden Empfehlungen gegeben, wie sie zu einer sicheren Stromversorgung auch in Pandemiezeiten beitragen können.

  Prüfungen: Hunderte Experten der VDE Global Services überprüfen weltweit die Qualität von Hightech-Elektronik und mechanischen Produkten, bevor sie auf den deutschen und europäischen Markt kommen. Als Anfang 2020 massive Probleme bei den Lieferketten offensichtlich wurden, haben sie deutsche und europäische Unternehmen aus dem erneuerbaren Energiesektor gezielt unterstützt, um nicht Opfer mangelhafter Produkte aus Fernost zu werden.
- **Standardisierung:** KRITIS-Betreiber wie Energieversorger müssen branchenweite Mindeststandards erarbeiten und diese genehmigen lassen. Die Normungsorganisation VDE DKE unterstützt sie dabei. Beispiel: Damit deutschlandweit die Ampelanlagen jederzeit sicher funktionieren, hat VDE DKE alle interessierten Kreise zusammengebracht und gemeinsam entsprechende Standards erarbeitet.
- **Austausch:** Mit CERT@VDE bietet der VDE den kooperierenden Unternehmen aus industriellen Schlüsselbereichen wie dem Maschinenbau eine vertrauensvolle Austauschplattform auf gemeinnütziger Basis. Die Industriepartner kollaborieren hier auf Grundlage einer freiwilligen Selbstverpflichtung in einem weltweit einzigartigen Umfeld und erhalten professionelle Unterstützung bei Cyberbedrohungen.

Ihr Ansprechpartner

Markus B. Jaeger, Head of Political Affairs
VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V.

Bismarckstraße 33, 10625 Berlin
Mobil +49 171 7631986
markusb.jaeger@vde.com