Wie verwundbar sind kritische Infrastrukturen?

In Kürze

- Gesellschaftliche und wirtschaftliche Prozesse sind heute hochgradig von verschiedenen Technologien und deren Zusammenspiel abhängig.
- Kritische Infrastrukturen sind damit die „Hauptschlagader" der digital vernetzten Gesellschaft, deren Funktionsfähigkeit wesentlich für Daseinsvorsorge und Grundversorgung ist.
- Systemausfälle durch externe Risikofaktoren, systemimmanente Fehler oder unbekannte Schwachstellen können diese Funktionsfähigkeit gravierend beeinträchtigen.
- Die Schaffung wirksamer Sicherheitsmaßnahmen erfordert vor allem mehr Bewusstsein für die bislang unterschätzte Problematik von System-Abhängigkeiten.

Worum geht es?

Der Begriff „Kritische Infrastrukturen" (KRITIS) umfasst alle Infrastrukturen (d.h. Systeme, Anlagen, Prozesse oder Netzwerke), die wesentlich für die Funktionsfähigkeit gesellschaftlicher Abläufe sind. KRITIS lassen sich in verschiedene Sektoren untergliedern, die von Lebensmittel- und Energieversorgung, Transport und Verkehr, Telekommunikation, Medien, Finanz- und Versicherungswesen bis zu Sozial- und Gesundheitswesen reichen. Beeinträchtigungen oder Ausfälle einer oder mehrerer Infrastrukturkomponenten in diesen wesentlichen Bereichen können dementsprechend enorme Auswirkungen auf Wirtschaft, staatliche Handlungsfähigkeit und soziales Wohlergehen haben. Wie verwundbar die Gesellschaft ist, hängt aber vor allem von jenen Funktionen und Diensten ab, die KRITIS-Systeme in verschiedenen Bereichen ermöglichen. Österreich orientiert sich deshalb bewusst an Funktionen statt Sektoren von KRITIS (wie etwa Deutschland). Neben Bereichen der staatlichen Daseinsvorsorge zählen daher strategisch wichtige Unternehmen und Einrichtungen als KRITIS-relevante Funktionsträger.
Es lassen sich zwei zentrale Querschnittstechnologien identifizieren, von denen praktisch alle anderen KRITIS-Bereiche abhängig sind: Die Energie-Versorgung (insb. Stromnetz) sowie IT-Systeme. Energie und Information sind allumfassende, zentrale Grundgüter, für Staat, öffentliche Einrichtungen zur Gesundheitsversorgung, Industrie und Unternehmen ebenso wie für private Haushalte.

Sektoren kritischer Infrastrukturen

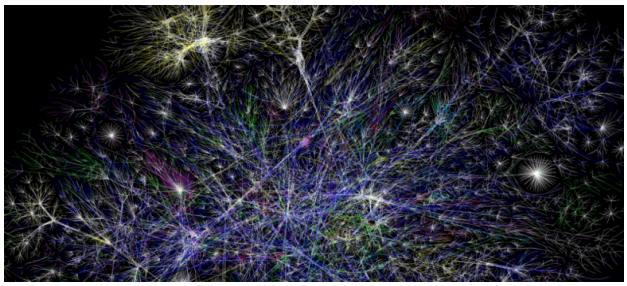
Die steigende Abhängigkeit von Kritischen Infrastrukturen wirkt sich letztlich negativ auf die Selbstorganisationsfähigkeit aller gesellschaftlichen Akteure (staatliche und private Institutionen, Unternehmen wie Zivilgesellschaft) aus. Diese ist aber zur Krisenbewältigung essentiell. Um diese Abhängigkeit zu reduzieren braucht es ein stärkeres Problembewusstsein und eine höhere Widerstandsfähigkeit (Resilienz) der Gesellschaft. Die Vielfalt potentieller Gefahren kann den Schutz von KRITIS erheblich erschweren. Das Spektrum reicht von Naturkatastrophen, technischen Unfällen und menschlichem Versagen bis zu Kriminalität und Terrorismus sowie Gefahren im Cyberspace. Spezielle Risiken sind sogenannte elektromagnetische Impulse (EMP), die technische Systeme nachhaltig stören bzw. sogar zerstören können. EMPs sind relativ aufwändig zu erzeugen und eher militärischen Akteuren vorbehalten, die über spezielle Waffensysteme verfügen. Sie treten aber auch in der Natur auf: eher harmlos als Gewitterblitze aber auch als Weltraumwetterphänomene wie Sonnen- bzw. Magnetstürme – zwar mit eher geringerem Risiko, jedoch relativ unberechenbar und daher nicht zu unterschätzen. Insbesondere, weil solche EMPs bei Eintritt folgenschwere Kettenreaktionen nach sich ziehen können.

Eckdaten

Projekttitel:	Digitaler Stillstand
Projektteam:	Strauß, S., Krieger-Lamina, J., Peissl, W.
Laufzeit:	01/2015 – 04/2017
Auftraggeber:	ÖAW-Präsidium

Vernetzung und zunehmende Systemabhängigkeiten

Unabhängig von den diversen Risiken ist die Kernproblematik die Abhängigkeit der Gesellschaft von technischen Systemen, insbesondere von Energie- und Informationssystemen – Tendenz weiter steigend (vor allem durch fortschreitende Digitalisierung). Aufgrund ihres hohen Komplexitäts- und Vernetzungsgrades bilden IT-Systeme die Achillesferse der kritischen Infrastrukturen. Mit mehr Vernetzung und Abhängigkeiten steigt auch die Gefahr von Kaskadeneffekten: Fällt eine kritische Komponente aus, können größere Systemausfälle in anderen KRITIS-Bereichen folgen.



en.wikipedia.org/wiki/File:Internet_map_1024.jpg

Mehr Vernetzung erhöht Komplexität und Systemabhängigkeiten.

Trotz zahlreicher „Cyber-Risiken" (z.B. Cyberangriffe wie „WannaCry", Botnetze aus Alltagsgeräten wie „Mirai", oder gravierende Sicherheitslücken wie zuletzt „Spectre" etc.) sollte nicht übersehen werden: Diese sind zwar ein Symptom erhöhter Verletzlichkeit (als schwerwiegende Nebenwirkung steigender Vernetzung und technischer Abhängigkeiten), Störfälle können aber dennoch analoger wie digitaler Natur sein. Steigende Komplexität und geringes Wissen über das Zusammenspiel von Systemkomponenten sind gravierende Risikofaktoren. Häufige Ursachen für Ausfälle aller Art sind wachsende Vernetzung gepaart mit mangelhaften Sicherheitskonzepten. Drastische Beispiele hierfür sind Kraftwerke (sogar AKWs), deren Steuerung direkt per Internet erreichbar ist. Aber auch scheinbar harmlose Komponenten bergen Risiken, wie etwa der Hack eines digitalen Autoradios zeigt: mangelnde Sicherheitskonzepte ermöglichten es, die Fahrzeugsteuerung zu übernehmen. Schwachstellen im System-Design sind daher ein zentrales Sicherheitsrisiko. Dabei können vor allem unterschätzte Abhängigkeiten problematisch sein: Hohe Komplexität kann zur unbeabsichtigten Vernachlässigung von kritischen Systemkomponenten führen. Ein Beispiel ist die oft implizite Abhängigkeit von IT-Systemen zu Satellitensystemen. Letztere werden nicht nur zur Navigation, sondern auch zur Zeitsynchronisation (u.a. auch im Stromnetz oder im Finanzwesen) eingesetzt. Ausfälle solcher Komponenten können die Stabilität eines Systems insgesamt gefährden. Im Kern geht es bei KRITIS um System-Schnittstellen, die besonderen Schutzbedarf haben.

Was tun?

Die Problematik von System-Abhängigkeiten ist bislang unterschätzt. Hier ist mehr Bewusstsein nötig, um Wirksamkeit von Sicherheitsmaßnahmen und damit das Schutzniveau insgesamt zu erhöhen. Zentrale Aspekte sind dabei u.a.:

- Schnittstellen verbinden verschiedene Systemelemente (z.B. Steuerungskomponenten mit Internet- oder Mobilfunkverbindung). Sie sollten daher als neuralgische Punkte begriffen und entsprechend geschützt werden. Unsichere, beeinträchtigte oder fehlerhafte Schnittstellen können kritische Infrastrukturen destabilisieren.
- Kritische Infrastrukturen sollten systematisch auf Schwachstellen analysiert werden, um auch nicht offensichtliche System-Abhängigkeiten zu erkennen und abzusichern.
- Die Redundanz und Substituierbarkeit zentraler Komponenten und Funktionen kritischer Infrastrukturen sollte erhöht werden, um die Gefahr von Kettenreaktionen einzudämmen.
- Notversorgung und krisenfeste Kommunikationssysteme sollten sichergestellt werden, um im Schadensfall kommunikations- und handlungsfähig zu bleiben; die Rolle von Computer Emergency Response Teams (CERTs) als Anlaufstelle zur Krisenbewältigung sollte gestärkt werden.
- Standards und Richtlinien des Krisen- und Katastrophenschutzes sowie zur elektromagnetischen Verträglichkeit sollten evaluiert und gegebenenfalls angepasst werden.
- Es braucht mehr Forschung zu Auswirkungen von Vernetzung und Systemabhängigkeiten, sowie Security-by-Design zum wirksamen Schutz kritischer Infrastrukturen.

Zum Weiterlesen

Strauß, S., Krieger-Lamina, J. (2017): Digitaler Stillstand: Die Verletzlichkeit der digital vernetzten Gesellschaft – Kritische Infrastrukturen und Systemperspektiven. Bericht Nr. ITA 2017-01, Wien: ITA
epub.oeaw.ac.at/ita/ita-projektberichte/2017-01.pdf

Kontakt

Stefan Strauß

E-mail: tamail@oeaw.ac.at

Telefon: +43(1)51581-6582

IMPRESSUM: Medieninhaber: Österreichische Akademie der Wissenschaften; Juristische Person öffentlichen Rechts (BGBl. 569/1921 i.d.F. BGBl. I 130/2003); Dr. Ignaz Seipel-Platz 2, A-1010 Wien; Herausgeber: Institut für Technikfolgen-Abschätzung (ITA); Strohgasse 45/5, A-1030 Wien; www.oeaw.ac.at/ita | Erscheinungsweise: Die ITA-Dossiers erscheinen unregelmäßig und dienen der Veröffentlichung der Forschungsergebnisse des ITA. Die Dossiers werden in kleiner Auflage gedruckt und open access über das Portal „epub.oeaw" zur Verfügung gestellt: epub.oeaw.ac.at/ita/ita-dossiers | ISSN: 2306-1960

ITA-Dossier Nr. 33, März 2018, epub.oeaw.ac.at/ita/ita-dossiers/ita-dossier033.pdf | Ko-Autoren: Jaro Krieger-Lamina, Walter Peissl