WWW.OEAW.AC.AT

ÖAW ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN

MAI 2017 | STELLUNGNAHME

DIGITALER STILLSTAND

DIE VERLETZLICHKEIT DER DIGITAL VERNETZTEN GESELLSCHAFT

DIGITALER STILLSTAND

DIE VERLETZLICHKEIT DER DIGITAL VERNETZTEN GESELLSCHAFT

STELLUNGNAHME DER ÖAW ZUR SITUATION IN ÖSTERREICH

INHALT

IN ALLER KÜRZE

Wir sind in unserem täglichen Leben vom Funktionieren vernetzter Technologien abhängig. Dieses Gerüst, das uns das Leben in der gewohnten Weise möglich macht, basiert auf sogenannten kritischen Infrastrukturen, die in den meisten Fällen auch von digitalen Technologien abhängen. Diese Infrastrukturen sind in mannigfacher Weise bedroht, nicht zuletzt auch durch den Prozess der Digitalisierung selbst, der Ausfallrisiken wesentlich erhöht. Fallen Teile einer Infrastruktur aus, kann das schwerwiegende Kettenreaktionen und weitere Ausfälle auslösen:

- Es gibt externe Bedrohungen, wie Weltraumwetterphänomene, die die Funktion von Satelliten und das Erdmagnetfeld beeinflussen können, aber auch Waffensysteme, die durch elektromagnetische Impulse die kritischen Infrastrukturen bzw. deren Versorgung beeinflussen können.
- Ein geringes Risikobewusstsein, auch was die Vernetzung von Steuereinheiten über das Internet betrifft, trägt erheblich zum Gefährdungspotential bei.
- Daneben gibt es systemimmanente Bedrohungen, insbesondere zum Teil versteckte Systemabhängigkeiten, wie die Einbindung von GPS in viele Anwendungen, das bei Sonnenstürmen ausfallen kann.
- Schließlich sind kritische Infrastrukturen hochgradig vernetzt, was bei einzelnen Ausfällen zu Kaskadeneffekten führen kann.

Die vorliegende Stellungnahme der ÖAW empfiehlt folgende Gegenmaßnahmen um, einen „Digitalen Stillstand" zu vermeiden:

- Eine umfassende Systemanalyse sollte durchgeführt werden und die Basis für eine bessere Abstimmung der Akteure bilden.
- Für Anbieter und Betreiber kritischer Infrastrukturen und für die Bevölkerung sollten bewusstseinsbildende Maßnahmen gesetzt werden.
- Die Akteure im Bereich der kritischen Infrastrukturen sollten verstärkt zusammenarbeiten und sich österreichweit besser vernetzen.
- Das Systemdesign muss den aufgezeigten Bedrohungen angepasst werden (konsequente Verfolgung eines Security-by-Design-Ansatzes).
- Entkoppelte, d.h. nicht auf anderen kritischen Infrastrukturen aufbauende Notfallsysteme sollten bereitgehalten werden.
- Der Schutz der (digitalen) kritischen Infrastrukturen sollte intensiv mit technischer aber auch gesellschaftswissenschaftlicher Forschung begleitet werden.

ÜBERSICHT

Wir sind in unserem täglichen Leben vom Funktionieren vernetzter Technologien abhängig. Viele Menschen leben auf teilweise sehr engem Raum zusammen und werden mit allem Nötigen versorgt – mit Nahrung, Energie, Information, Gesundheitsdiensten, Finanzdienstleistungen und vielem mehr. Die Menschen unserer Gesellschaft sind mobil und in der Lage, mit der ganzen Welt zu kommunizieren.

Möglich wird das durch ein engmaschiges Netz an technischen Infrastrukturen, deren Wechselwirkungen oft nicht auf den ersten Blick zu sehen sind. Dabei sind nicht nur Kommunikationsnetze und Informationsangebote weitgehend digitalisiert, auch in allen anderen Bereichen des Lebens hat die Digitalisierung Einzug gehalten.

Kritische Infrastrukturen

Dieses Gerüst, das uns das Leben in der gewohnten Weise möglich macht, basiert auf sogenannten kritischen Infrastrukturen. Das sind Einrichtungen, deren Ausfall gravierende Konsequenzen für die gesellschaftlichen und wirtschaftlichen Prozesse in unserer Gesellschaft hätte, beispielsweise Flughäfen, Kraftwerke, Krankenhäuser oder Mobilfunknetze. Diese kritischen Infrastrukturen müssen nicht nur für sich funktionieren, sondern in zunehmendem Maße auch reibungslos zusammenarbeiten, um die Versorgung mit den lebensnotwendigen Gütern und Dienstleistungen sicherzustellen. Der Schutz kritischer Infrastrukturen und die Aufrechterhaltung ihrer Funktionsfähigkeit sind zentrale Herausforderungen für deren Betreiber und den Staat. Gefahren drohen hier von ganz unterschiedlichen Seiten. So können Naturkatastrophen, mutwillige Angriffe und Sabotage den Betrieb beeinträchtigen.

Zentrale Faktoren der Krisenanfälligkeit von Infrastrukturen liegen jedoch auch in den Infrastrukturen und deren Entwicklung selbst begründet. Neben Materialversagen und menschlichen Fehlern können sich aus wechselseitigen Systemabhängigkeiten, fehleranfälligen Schnittstellen oder der Integration von per se nicht kritischen Komponenten in kritische Infrastrukturen gravierende Probleme ergeben. Diese Fehlerquellen sind teilweise noch zu wenig erforscht und werden deshalb vielfach noch nicht ausreichend berücksichtigt.

Fokus auf Strom und IKT

Der Fokus dieser Stellungnahme liegt auf zwei Technologien, die sich durch alle Bereiche des modernen Lebens ziehen: Die Versorgung mit elektrischem Strom und die Informations- und Kommunikationstechnologien (IKT). Das Funktionieren dieser Bereiche muss vor allen anderen sichergestellt werden, wenn es darum geht, den Betrieb kritischer Infrastrukturen zu schützen.

ZENTRALE BEGRIFFE: REDUNDANZ, RESILIENZ UND SELBSTORGANISATIONS-FÄHIGKEIT

Redundanz: Ersatzsystem vorhalten

Beim Schutz der Infrastruktureinrichtungen vor Bedrohungen ist absolute Sicherheit unerreichbar. Daher muss es stets Überlegungen geben, wie mit Ausfällen umzugehen ist. Eine Möglichkeit ist, ein zweites System vorzuhalten, das die gleiche oder zumindest eine ausreichend gute Ersatzleistung erbringen kann. In so einem Fall spricht man von Redundanz.

Resilienz: rasch wieder den Normalzustand erreichen

Ziel vorsorgender Systemplanung und vergleichbarer Maßnahmen ist, die Resilienz eines Systems zu erhöhen. Das ist in diesem Zusammenhang die Fähigkeit, mit Beeinträchtigungen umzugehen und rasch wieder den Normalzustand zu erreichen.

Selbstorganisationsfähigkeit aller Akteure fördern

Unabhängig von den technischen Maßnahmen zur Erhöhung der Resilienz der Systeme spielt die Information aller Akteure einschließlich der Bevölkerung eine wesentliche Rolle: Betroffene müssen darüber informiert sein, was im Falle eines großflächigen Ausfalls kritischer Infrastrukturen zu tun ist, und wie sie möglichst viele Bereiche ihres Alltags autonom aufrechterhalten können. Diese Selbstorganisationsfähigkeit muss vorbeugend vermittelt und im Krisenfall mit Koordination und zeitnaher Bereitstellung von Ressourcen gefördert werden, da die staatliche Sicherstellung einer umfassenden Versorgung – etwa über das Bundesheer – im Fall weitreichender Krisen nicht gewährleistet werden kann.

STRATEGIEN UND ZUSTÄNDIGKEITEN IN ÖSTERREICH

In Österreich ist eine Vielzahl an Akteuren damit beschäftigt, den Schutz kritischer Infrastrukturen sicherzustellen. Auf der einen Seite sorgt die Politik für die notwendigen Rahmenbedingungen und gibt in Strategiepapieren die Richtung vor, auf der anderen Seite stehen die Betreiber kritischer Infrastrukturen, die für ihre eigenen Systeme verantwortlich sind.

Austrian Programme for Critical Infrastructure Protection

Um die Herausforderungen zu bewältigen, die sich im Zusammenhang mit dem Schutz kritischer Infrastrukturen ergeben, gibt es eine in den letzten Jahren wachsende Anzahl an politischen Programmen und Strategien. So setzt Österreich beispielsweise mit dem Programm zum Schutz kritischer Infrastrukturen (Austrian Programme for Critical Infrastructure Protection – APCIP) auf einen funktionsorientiert-kooperativen Ansatz, der die gemeinsamen Anstrengungen der Betreiber und der Verwaltung koordiniert, um die Resilienz Österreichs zu erhöhen. Dieses Programm orientiert sich auch an der EU-Richtlinie zum Schutz kritischer Infrastrukturen. Die Eigenverantwortung der Betreiber ist hier ein wichtiger Punkt. Im Rahmen des APCIP legen das Innenministerium (BMI) und das Bundeskanzleramt (BKA) gemeinsam die Liste kritischer Infrastrukturen in Österreich fest und sind in Form von Public-Private-Partnerships in Kontakt mit Betreibern strategischer Unternehmen und Organisationen. Die einzelnen Ministerien sowie die Bundesländer sind in Form eines Beirats in das APCIP eingebunden, der sich thematisch einbringt und bei Bedarf eigene Arbeitsgruppen einrichten kann. Neben nationalen Kooperationen ist auch die Zusammenarbeit auf europäischer und internationaler Ebene vorgesehen.

Staatliches Krisen- und Katastrophenschutz-management

Das staatliche Krisen- und Katastrophenschutzmanagement (SKKM) wird in einer eigenen Strategie beschrieben. Eine zentrale Einrichtung des SKKM in Österreich ist das Einsatz- und Krisenkoordinationscenter (EKC) des BMI.

Österreichische Sicherheits-strategie

APCIP und SKKM wiederum sind Mosaiksteine der Österreichischen Sicherheitsstrategie (ÖSS), die den übergeordneten Rahmen für diese Maßnahmen bildet. Die ÖSS definiert die Bereiche, die (mittels weiterführender Strategien oder Programme) geschützt werden sollen. Unter anderem sind das: der umfassende Schutz der Bevölkerung, die Gewährleistung der territorialen Integrität und der Selbstbestimmung Österreichs, der Schutz der Verfassung und der Grundrechte, Stärkung des Gemeinwohls, Aufrechterhaltung des sozialen Friedens, Sicherstellung der Verfügbarkeit lebensnotwendiger Ressourcen, Umweltschutz, der Kampf gegen Terrorismus, organisierte Kriminalität, Cyber-Angriffe und Cyber-Kriminalität, Eindämmung illegaler Migration und Bekämpfung der Schlepperei, Krisenfrüherkennung, -bewältigung und -nachsorge, Förderung des Sicherheitsbewusstseins in der Bevölkerung, und eben der Schutz kritischer Infrastrukturen.

Österreichische Strategie für Cyber-Sicherheit

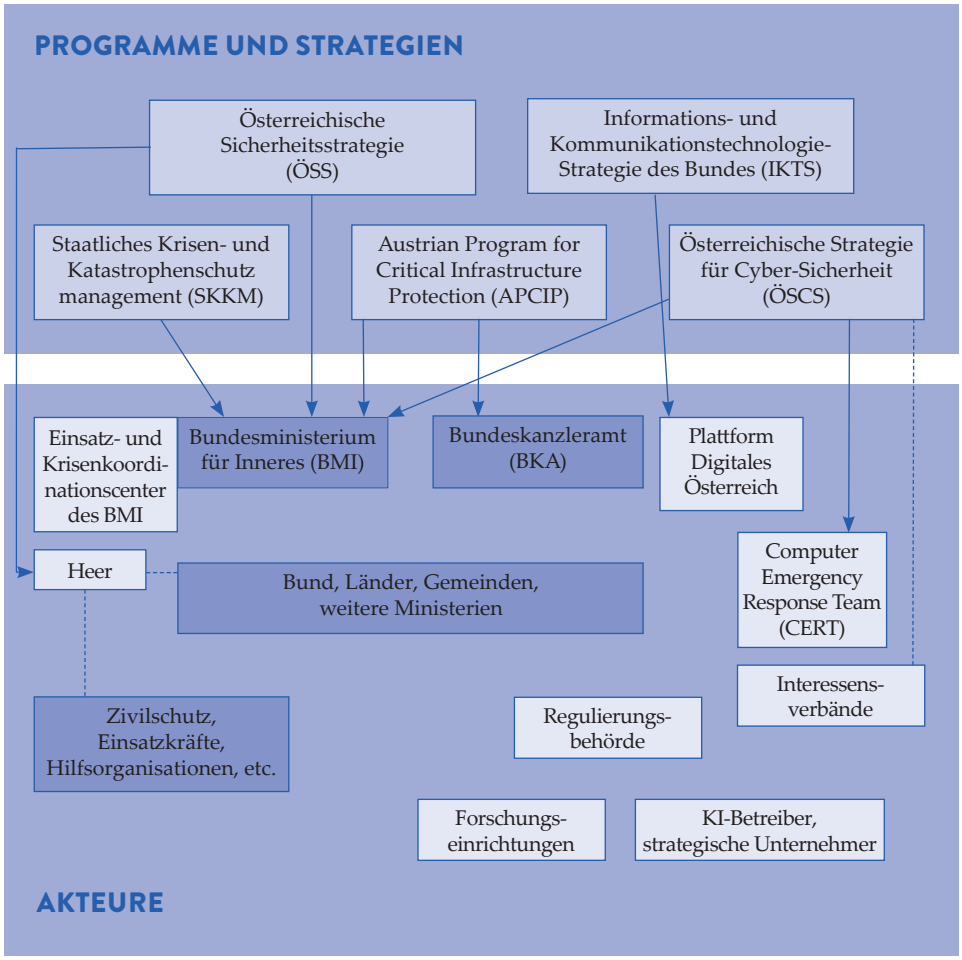
Ein weiterer essentieller Baustein zu einem sicheren Österreich ist auch die Österreichische Strategie für Cyber-Sicherheit (ÖSCS), die die Österreichische IKT-Strategie (IKTS) um das Thema Sicherheit ergänzt. Dadurch stellt sie auch eine Brücke zwischen der IKTS und dem APCIP dar. Einer der wichtigen Meilensteine in der Umsetzung der ÖSCS war

die Errichtung der Computer Emergency Response Teams (CERTs). Ein solches Team gibt es auf nationaler Ebene, die Errichtung von CERTs für alle Sektoren ist geplant. Bereits eingerichtet wurden z.B. MilCERT im militärischen Bereich und GovCERT im Bereich der staatlichen Verwaltung. Das Cyber-Lagezentrum des Verteidigungsministeriums (BMLVS) spielt ebenfalls eine wichtige Rolle bei der Koordination in Cyber-Krisen.

Österreichische IKT-Strategie

Die aufgezeigte Vielfalt der Akteure und Strategien verdeutlicht einerseits die Komplexität der Problematik, bringt aber andererseits auch Unklarheiten hinsichtlich der Zuständigkeiten mit sich, die noch analysiert und gegebenenfalls adaptiert werden sollten.

Übersicht zentraler Akteure



HERAUSFORDERUNGEN

Kritische Infrastrukturen sind vielfach bedroht

Kritische Infrastrukturen sind einer Vielzahl von Bedrohungen ausgesetzt. Einerseits bestehen Gefahren, deren Ursachen außerhalb des Systems liegen, wie zum Beispiel Naturkatastrophen, Pandemien, Unfälle in Atomreaktoren, Angriffe über Datennetze, Sabotage, Terroranschläge oder Gefahren durch elektromagnetische Impulse. Damit eine dieser Bedrohungen schlagend wird, müssen die Systeme im jeweiligen Bereich verwundbar sein, und sie müssen dieser Gefahr ausgesetzt sein. Daher setzen Maßnahmen zum Schutz kritischer Infrastrukturen sowohl dort an, wo Verwundbarkeiten verringert und Exposition vermieden werden können, als auch bei der Bewältigung von Ausfällen. Darüber hinaus bestehen Risiken, die sich aus Faktoren innerhalb der Infrastrukturen und aus deren Vernetzung ergeben. Einst physisch und logisch voneinander getrennte Systeme sind zunehmend miteinander verzahnt, und so können Abhängigkeiten entstehen, die die Anfälligkeit für Störungen und die Vulnerabilität erhöhen.

WECHSELWIRKUNGEN UND SYSTEMABHÄNGIGKEITEN

Wechselwirkung zwischen Strom und IKT

Von großer Bedeutung sind die Wechselwirkungen zwischen dem Stromnetz und den Informations- und Kommunikationstechnologien. Ein Ausfall im Bereich dieser Querschnittstechnologien würde die meisten kritischen Infrastrukturen stark beeinträchtigen. Man muss dabei von komplexen Risiken mit hohem Schadenspotenzial ausgehen. Mit eingeschleuster Schadsoftware können etwa Infrastrukturen gestört werden. Dokumentierte Fälle von versuchten Störungen bei AKWs („Stuxnet“ im Iran, „Conficker“ in Deutschland) oder im Stromnetz („Blackenergy“ in der Ukraine) verdeutlichen diese Gefahr. Auf Grund der wechselseitigen Abhängigkeiten ist zu erwarten, dass ein großflächiger Stromausfall die gesamte IKT-Infrastruktur in Mitleidenschaft ziehen und auch umgekehrt, ein großflächiger Ausfall im Bereich IKT Probleme bei der Netzsteuerung hervorrufen wird.

Zunehmende Vernetzung als Fehlerquelle

Weitere Fehlerquellen, die berücksichtigt werden müssen, entstehen durch die zunehmende Vernetzung und die damit steigende Komplexität der Systeme. Klassische Risikoanalysen, die sich mit nur einem Bedrohungsszenario und nur einem System befassen, greifen zu kurz. Wie sich in der Vergangenheit etwa bei Bahnsystemen oder der Steuerung der Wasserversorgung gezeigt hat, kann die ungenügend geplante Vernetzung zu großen Problemen führen.

In der Regel können Betreiber ihre eigene Infrastruktur kontrollieren, in verbundenen Systemen können Fehler im Netz eines Partners allerdings Auswirkungen auf die anderen Netze im Verbund haben, wenn die Schnittstellen nicht sorgfältig eingerichtet wurden. Ein extremes Beispiel sind interne Steuerungsnetze, die über das Internet erreichbar sind. Oft werden aber auch Netze unterschiedlicher Unternehmen miteinander verbunden, um Daten, etwa für die Verrechnung oder Logistik, auszutauschen. Ganz allgemein lässt sich sagen, dass eine zunehmende Vernetzung die Komplexität der Systeme erhöht, die Angriffsfläche vergrößert und den Schutz dadurch deutlich schwieriger macht.

GPS zur Zeitsynchronisierung an der Börse und im Stromnetz

Schnittstellen bestehen aber nicht nur zwischen IT-Netzen oder unterschiedlichen Systemkomponenten, sondern auch zwischen unterschiedlichen Technologien. Auch aus solchen Schnittstellen können sich Abhängigkeiten ergeben. So ist heute z.B. sehr häufig GPS (Global Positioning System) Teil von Steuerungsinfrastrukturen. Neben der Funktion als

Hilfsmittel zur Ortung bzw. Navigation wird das GPS-Signal dabei auch zur Zeitsynchronisation genutzt, u.a. bei Hochfrequenzhandelssystemen an der Börse oder bei Anlagen im Stromnetz. Gerade bei derartigen, weniger offensichtlichen Abhängigkeiten besteht die Gefahr, dass Systeme nicht redundant eingerichtet sind, und die entsprechenden Funktionen bei einem Ausfall nicht ersetzt werden könnten. Zudem wird die Zuverlässigkeit von Systemen wie GPS häufig überschätzt.

Systemabhängigkeiten werden in Zukunft noch zunehmen

Aktuelle Entwicklungen wie Industrie 4.0, autonome Fahrzeuge, Internet der Dinge etc. werden eine weiter zunehmende Digitalisierung, Vernetzung und Automatisierung mit sich bringen. Integrierte Systeme werden damit an Bedeutung gewinnen, die Systemabhängigkeiten werden sich entsprechend verschärfen. Verstärktes Problembewusstsein und mehr Analysen zur Verletzlichkeit sind notwendig, um kritische Komponenten zu erkennen und diese besser schützen zu können.

ELEKTROMAGNETISCHE IMPULSE

Unter den externen Bedrohungsszenarien sind großflächige elektromagnetische (Im)Pulse (EMP) ein Thema, das vertieft untersucht werden muss.

Nukleare und elektromagnetische Impulse können Elektronik zerstören

Ein EMP ist eine meist kurze, breitbandige elektromagnetische Strahlung, die sich auf elektrisch leitfähiges Material auswirken kann. Es kommt dabei zu einer sprunghaften Änderung einer elektrischen oder magnetischen Größe. EMP können in sehr geringem Ausmaß selbst beim Betätigen eines Lichtschalters auftreten, in größerem Maßstab etwa bei Blitzschlägen. Großflächige EMPs können künstlich – etwa durch das Zünden einer Atombombe in mehreren hundert Kilometern Höhe – ausgelöst werden oder sie entstehen durch Sonnenstürme.

Um nukleare EMPs (NEMPs) zu verursachen, sind spezielles Know-How und militärisches Equipment in einem hoch entwickelten Ausmaß erforderlich. International wird die Gefahr nuklearer EMPs aufgrund des potenziell hohen Schadensausmaßes zwar grundsätzlich als hoch eingestuft, die Wahrscheinlichkeit gilt aber als gering.

Mit HPM-Waffen können gezielt Anlagen und Anlagenteile gestört werden

Allerdings gibt es neben NEMPs auch spezielle Waffensysteme – sogenannte HPM-Waffen, die mit Mikrowellenstrahlung (High Power Microwave – HPM) arbeiten. Diese Waffen werden vor allem für das Militär entwickelt und von diesem eingesetzt (etwa von US-Truppen im Balkan- und im Irakkrieg). Dennoch ist hier durch die (verglichen mit NEMPs) einfachere Beschaffung von einem neuen Bedrohungspotenzial auszugehen, weil auch terroristische Gruppierungen derartige Waffen nutzen könnten. Diese Art vom EMPs funktioniert primär in geringer Distanz und hat wesentlich weniger Breitenwirkung als ein NEMP. Die Gefahr von HPM-Waffen bezieht sich eher auf einzelne Anlagen und nicht auf großflächige Teile kritischer Infrastruktur. Allerdings lassen sich auf diese Weise Infrastruktursysteme mitunter gezielter stören.

Für Österreich wird das Bedrohungspotenzial aufgrund seiner geopolitischen Lage und Neutralität generell als niedrig eingestuft.

Sonnenstürme bedrohen Satelliten …

Besondere Aufmerksamkeit erfahren derzeit jedoch EMPs, die durch Sonnenstürme ausgelöst werden. Sonnenstürme interagieren mit dem Magnetfeld der Erde durch die ionisierten Teilchen, die bei einer Sonneneruption oder einem koronalen Masseauswurf entstehen. Diese EMPs dauern länger an, der Impuls ist jedoch weniger stark als bei einer Nuklearbombendetonation. Satellitensysteme sind zwar relativ gut gegen Sonnenstürme abgeschirmt und können bei rechtzeitiger Warnung in einen sicheren Zustand gebracht werden, sind durch das Fehlen der schützenden Atmosphäre der Strahlung aber auch viel stärker ausgesetzt als die Infrastruktur auf der Erde. Hier kann besonders das Stromnetz

… und das Stromnetz

durch die induzierten Ströme in Mitleidenschaft gezogen werden, speziell bei hoher Leitungslänge und wenig leitfähigem Untergrund. Überspannungen im Netz können nicht nur angeschlossenes Equipment beschädigen, sondern vor allem auch Transformatoren, die nicht vor diesen Gleichstromspitzen geschützt sind.

Weltraumwetter

Sonnenstürme werden als Weltraumwetterphänomene nicht nur im Hinblick auf ihre potenziellen Auswirkungen auf die moderne Infrastruktur untersucht, sondern auch, um die Vorwarnzeiten zu verbessern. Bei rechtzeitiger Alarmierung könnten Systeme abgeschaltet oder vom Netz genommen werden, wodurch sie deutlich weniger anfällig für Ausfälle wären. Auch kommerzielle Flüge über die Polregionen, deren Zahl in den letzten Jahren stark angestiegen ist, könnten so auf andere Routen verlegt werden, um die Strahlenbelastung für Crew und Passagiere zu reduzieren. Österreich ist auch hier durch seine geografische Lage deutlich weniger gefährdet als etwa die USA oder Skandinavien.

Trotz ihrer Unwahrscheinlichkeit ist eine Berücksichtigung verschiedener EMP-Risiken sinnvoll, da bislang wenig über die potenziellen Auswirkungen auf heutige Infrastruktursysteme bekannt ist.

TERRORISTISCHE UND KRIMINELLE BEDROHUNGEN

Vorfälle wie die Sprengungen von Strommasten auf der Krim im Dezember 2015 haben gezeigt, dass es nicht nur Naturereignisse oder Hightech Angriffe mit nuklearen EMPs sind, die kritische Infrastrukturen bedrohen können.

Auch Sabotage, Terroranschläge oder Cyber-Angriffe müssen bei den Schutzmaßnahmen Berücksichtigung finden.

Zum Beispiel: Cyber-Terrorismus

Cyber-Angriffe auf IT-Systeme von kritischen Infrastrukturen werden vor allem durch mangelhafte Sicherheitskonzepte möglich. Kritische Infrastrukturen, die über öffentliche Netze direkt erreichbar sind, stellen grundsätzlich ein massives Sicherheitsrisiko dar. Angreifer können Schwachstellen gezielt ausnützen, um Schadsoftware (Trojaner, Viren etc.) einzuspeisen. Derartige Fälle sind belegt und reichen vom Virenfund in Atomkraftwerken bis zum großflächigeren Stromausfall durch gezielte Angriffe. Im Juli 2016 wurde etwa bekannt, dass die Steuerungssysteme vieler deutscher Wasserwerke und Biogasanlagen über das Internet ausgespäht werden können. In einigen Fällen wäre es möglich gewesen, sensible Ziele zu sabotieren. Es besteht daher Bedarf an verbesserten Schutzkonzepten für kritische Infrastrukturen. Das bedeutet mehr Bewusstsein für Sicherheitsstandards und deren Umsetzung.

Verbesserte Schutzkonzepte für kritische Infrastrukturen notwendig

Die steigende Zahl und der Variantenreichtum von Cyber-Angriffen zeigen jedes Jahr, dass auch die IKT-Systeme kritischer Infrastrukturen besonderen Anforderungen genügen müssen.

Die Bestrebungen der eingangs genannten EU-Richtlinien, an denen sich auch die österreichischen Strategien orientieren, konzentrieren sich auf diese terroristischen Bedrohungen. Die zu Beginn dieses Kapitels aufgezeigten Problemszenarien, die sich aus den Systemabhängigkeiten durch den steigenden Vernetzungsgrad ergeben, müssten in den entsprechenden Strategien jedoch stärker berücksichtigt werden.

UNTERSCHIEDLICHE BEDÜRFNISSE

Zielkonflikte bestehen und müssen politisch vermittelt werden

Versorgungsleistungen sind nicht das Einzige, was der Staat für seine Bürger/innen erbringt. Neben vielem anderen ist auch der Schutz der Natur Aufgabe des Staates. Oft geraten die verschiedenen Ziele in Konflikt miteinander. In einer demokratischen Gesellschaft bedarf es hier eines mit Verständnis und Augenmaß geführten Aushandlungsprozesses, der zu einer politischen Entscheidung führt, deren Konsequenzen in die Verantwortung der Politik fallen und nicht zu Lasten nur einer der betroffenen Anspruchsgruppen gehen sollten.

Lücke in der österreichischen 380kV-Ringleitung

Ein konkretes Beispiel für derartige Konflikte ist die Diskussion um die Errichtung bzw. den Ausbau des Abschnitts der österreichischen 380kV-Ringleitung zwischen dem Umspannwerk St. Peter und dem Umspannwerk Tauern. Für die Versorgung des Großraums Salzburg mit elektrischem Strom und für die notwendige Sicherheit im Hochspannungsnetzbetrieb ist der Ausbau sinnvoll. Dem stehen berechtigte Umweltschutzinteressen der betroffenen Anrainer/innen bzw. Gemeinden entgegen, die entsprechend zu berücksichtigen und zu prüfen sind.

EMPFEHLUNGEN

Die geografische und geopolitische Lage Österreichs ist bis zu einem gewissen Grad begünstigend, sodass von einigen der externen Risikofaktoren (v.a. NEMPs und Solarstürme) eher geringe Bedrohung ausgeht. Die bestehenden Strategien deuten auf ein relativ hohes Problembewusstsein hin. Allerdings gibt es insbesondere Verbesserungsbedarf bei der Berücksichtigung von Risiken durch Systemabhängigkeiten. Es gibt Bedrohungen für kritische Infrastrukturen, die bislang zu wenig beachtet wurden. Maßnahmen sind daher erforderlich, um vernachlässigte Bereiche stärker in Schutzkonzepten zu berücksichtigen. Das betrifft vor allem Ausfallrisiken durch unerkannte Abhängigkeiten, die mitunter auch die Krisenkommunikation bedrohen können.

Adressaten der folgenden Empfehlungen

Die folgenden Empfehlungen richten sich sowohl an die zentralen staatlichen Akteure zum Schutz kritischer Infrastrukturen (Austrian Program for Critical Infrastructure Protection – APCIP, Staatliches Krisen- und Katastrophenschutzmanagement – SKKM) wie Bundeskanzleramt (BKA), Bundesministerium für Inneres (BMI), Bundesministerium für Landesverteidigung und Sport (BMLVS), Bundesministerium für Wissenschaft, Forschung und Wirtschaft (BMWFW) und weitere Einrichtungen in diesem Umfeld (Computer Emergency Response Team – CERT, Hilfsorganisationen und Zivilschutzverbände) als auch die Wirtschaft und Unternehmen als Betreiber kritischer Infrastrukturen.

SYSTEMEVALUIERUNGEN

Die große Komplexität hinsichtlich der Zahl der Akteure sowie die Vielzahl an Strategien zu Teilbereichen kritischer Infrastrukturen machen eine kritische Zusammenschau der vorhandenen Aktivitäten und Planungsszenarien erforderlich.

- Evaluierung der Unterschiede, Gemeinsamkeiten, Kompetenzverteilung und Synergien von staatlichem Krisen- und Katastrophenschutzmanagement und dem Programm zum Schutz kritischer Infrastrukturen.
- Evaluierung von Ressourcen und Standards zur Krisenkommunikation.
- Im Sinne einer betrieblichen Evaluierung sind durchgehende und kombinierte Tests von Notfallplänen erforderlich. Planungsszenarien für Teilbereiche, die in sich funktionieren, müssen auch in Abstimmung auf einander lückenlos umsetzbar sein.

Evaluierung der Notstromversorgung kritischer Infrastrukturen

- Zudem ist die Evaluierung der Notstromversorgungen kritischer Infrastruktur-Betriebe notwendig: Viele kritische Infrastrukturen sind auf einen großflächigen Stromausfall nur ungenügend vorbereitet. Vorhandenen Ressourcen sind darauf hin zu überprüfen, ob alle Betreiber kritischer Infrastrukturen sowie die Betriebe, von denen diese – ev. auch nur in Teilbereichen – abhängig sind, entweder selbst in der Lage sind, eine Notstromversorgung zu betreiben, oder die Netze zumindest so eingerichtet haben, dass im Notfall die Versorgung über externe Generatoren möglich und gewährleistet ist.

VERNETZUNGSMASSNAHMEN

Vor dem Hintergrund der sektoren- und länderübergreifenden Problemstellungen müssen der Austausch von Information sowie die Vorbereitung von Kooperationen im Krisenfall weiter forciert werden.

Internationale Zusammenarbeit

- Zusammenarbeit auf europäischer Ebene im Rahmen der EKI-Richtlinie sowie bilaterale, Staatsgrenzen überschreitende Planung und Implementierung von Standards zur Sicherstellung organisatorischer und technischer Interoperabilität.

- Plattformen für mehr inter- und transdisziplinären Austausch zum Thema Verbesserung des Schutzniveaus für kritische Infrastrukturen. Auch der inter- und transdisziplinäre Austausch zwischen Betreibern und Forschungseinrichtungen wird dazu beitragen, die Resilienz zu erhöhen.
- Einrichtung eines gesamtstaatlichen Lagezentrums zur Bündelung der Ressourcen unterschiedlicher (Verwaltungs-)Ressorts.

Österreichisches Lagezentrum

BEWUSSTSEINSBILDUNG

Wissen um die Problemlagen und die Möglichkeit, erkannte Notwendigkeiten im Betrieb bzw. im Krisenfall umzusetzen, sind zentrale Erfordernisse. Dabei ist zu berücksichtigen, dass nicht alle Betreiber kritischer Infrastrukturen große Betriebe sind. Kleinere Unternehmen haben z.T. nicht die Ressourcen, um ihre Infrastruktur den Anforderungen entsprechend zu betreiben.

- Entwicklung, Bereitstellung und Förderung von Schulungsmaßnahmen für Betreiber von Kommunikationsinfrastrukturen (im Rahmen des APCIP).

Schulungsmaßnahmen

- Unterstützung der Betreiber bei ihrer Forderung an Herstellerfirmen, in deren Produkten Security-by-Design-Prinzipien umzusetzen.
- Stärkung der IT-Expertise für den Betrieb kritischer Infrastrukturen (Ausfallsicherheit, Planung, Business Continuity Management, IT-Betrieb in Hochsicherheitsumgebungen): Förderung von Ausbildungsmaßnahmen für Mitarbeiter/innen von Betreibern kritischer Infrastrukturen mit dem Ziel, die Anforderungen eines ausfallsicheren Betriebs besser erfüllen zu können.
- Bewusstsein in der Bevölkerung und bei Unternehmen für das richtige Verhalten im Krisenfall erhöhen: Informationskampagnen, gemeinsame Ernstfallübungen, Etablieren von kleinräumigen, krisensicheren Informationsstrukturen. Auch eine Aufnahme des Themas Selbstorganisation in Krisenfällen in Ausbildungscurricula wäre sinnvoll.

Kleinräumige, krisensichere Informationsstrukturen

BETRIEB

Anforderungen an die Betreiber kritischer Infrastrukturen müssen ebenso erweitert werden wie das Verständnis, wer – z.B. auch nur in Teilbereichen – zum Betrieb kritischer Infrastrukturen beiträgt.

- Systemabhängigkeiten und mögliche Kaskadeneffekte müssen bei Maßnahmen zum Betrieb und zum Schutz kritischer Infrastrukturen verstärkt berücksichtigt werden.

Mögliche Kaskadeneffekte berücksichtigen

- Security-by-Design: Entwicklung nachhaltiger Schutzkonzepte, die Systemredundanzen in kritischen Komponenten bereits im Design vorsehen.
- Netzpläne und Schnittstellendokumentationen müssen erstellt und für den Krisenfall analog vorgehalten werden: Besonders auf die Dokumentation der Schnittstellen wird derzeit zu wenig Augenmerk gelegt. Die Pläne müssen regelmäßig (zumindest bei jeder Systemänderung) evaluiert und aktualisiert werden.

Analoge und aktuell gehaltene Dokumentationen

- Erweitertes Verständnis von Redundanz umsetzen: Redundanz sollte nicht nach dem Modell „more of the same“ umgesetzt und generell nicht nur systembezogen betrachtet werden. Vor Ausfällen muss nicht primär das (IKT-)System geschützt werden, das eine Funktion erfüllt. Zielsetzung ist vielmehr, die erforderliche Funktion zumindest in einem Notbetrieb erhalten zu können.
- Ein zusätzlicher, krisensicherer Kommunikationskanal (z.B. per Funk) muss bei Betreibern kritischer Infrastrukturen jedenfalls vorhanden sein.

Krisensicherer Kommunikationskanal

FORSCHUNG

Um den Wissenstand zu verbessern und zusätzliche Möglichkeiten der Prävention zu schaffen, ist die gezielte Förderung von Forschung in mehreren Bereichen erforderlich:

- Weitere Erforschung von Weltraumwetterphänomenen und deren besserer Vorhersage; Auswirkungen unterschiedlicher Formen von EMPs auf moderne Infrastrukturen; Untersuchung der Wirksamkeit von EMP-Schutzkonzepten – elektromagnetische Verträglichkeit.
- Security-by-Design und systemorientierte Schwachstellenanalysen – Untersuchen von „eingebauten" Verwundbarkeiten und Ansätzen zu deren Reduktion: Inwieweit erhöht sich die Verwundbarkeit kritischer Infrastrukturen durch Abhängigkeiten zu technischen (Teil-)Systemen (wie z.B. GPS) oder anderen Komponenten?

Security-by-Design

Der dieser Stellungnahme zu Grunde liegende Bericht des Instituts für Technikfolgen-Abschätzung der ÖAW kann unter folgender Adresse heruntergeladen werden:
epub.oeaw.ac.at/ita/ita-projektberichte/2017-01.pdf

IMPRESSUM:

HERAUSGEBER
Präsidium der Österreichischen Akademie der Wissenschaften
Dr. Ignaz Seipel-Platz 2, 1010 Wien
www.oeaw.ac.at