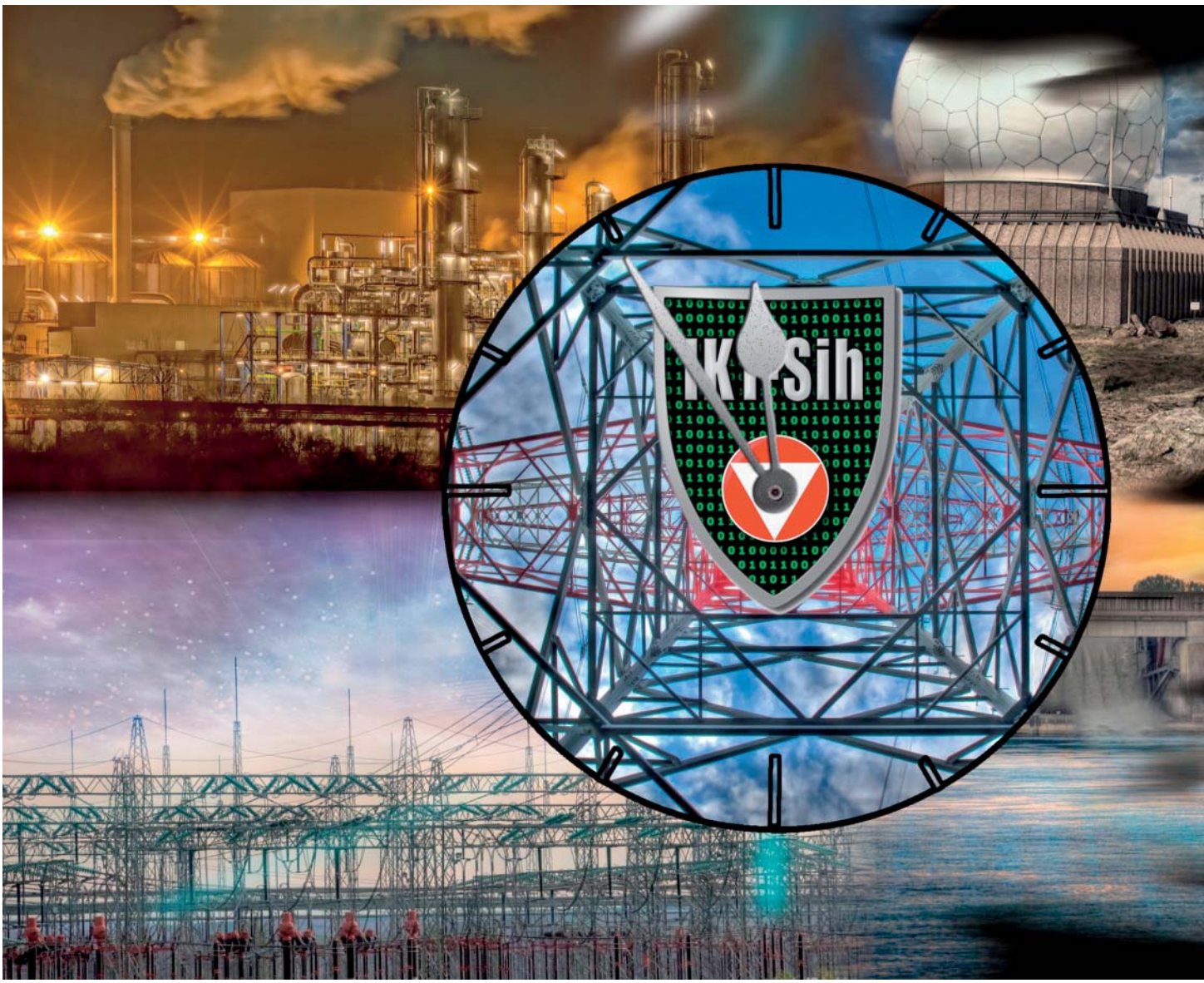


Die Gesellschaft hat in den vergangenen Jahrzehnten fast ihren gesamten Wohlstand auf den Energieträger Strom aufgebaut. Weite Teile der lebenswichtigen, strategischen Infrastruktur aber auch das gesamte Gemeinwesen funktionieren nur durch eine verlässliche Energieversorgung. Viel Wert wurde auf die Verfügbarkeit von elektrischer Energie gelegt. Künftig muss noch mehr darauf Bedacht genommen werden, einen totalen Stromausfall (Blackout) und dessen kurz-, mittel- und langfristig katastrophale Schäden zu verhindern bzw. nach dessen Eintritt rasch zu bewältigen.

Bisher gab es kaum schwerwiegende, großräumige Stromausfälle. Durch die umfassende Vernetzung und Computerisierung haben sich in den vergangenen Jahren völlig neue Abhängigkeiten ergeben, die nur sehr schwer zu durchschauen sind. Damit steigt die Fehleranfälligkeit und es sinkt die Widerstandsfähigkeit („Resilience“) der hochkomplexen Systeme, auf denen das Gemeinwesen basiert. Jede Gesellschaft ist daher gut beraten, sich intensiver mit diesen Risiken auseinanderzusetzen, denn eines der folgenschwersten Ereignisse für unsere hochtechnisierte Zivilisation ist ein großräumiger, länger andauernder Stromausfall - ein Blackout.

Europa ist bisher weitgehend von lang andauernden Blackouts verschont geblieben. Die Ereignisse von 2003 oder 2006 sind bereits wieder in Vergessenheit geraten. Schwerwiegende Zwischenfälle sind vor allem aus den USA bekannt, wo es immer wieder infolge von Naturereignissen oder aufgrund technischer Mängel, die etwa auf die Privatisierung der Strominfrastruktur zurückzuführen sind, zu Blackouts kommt.

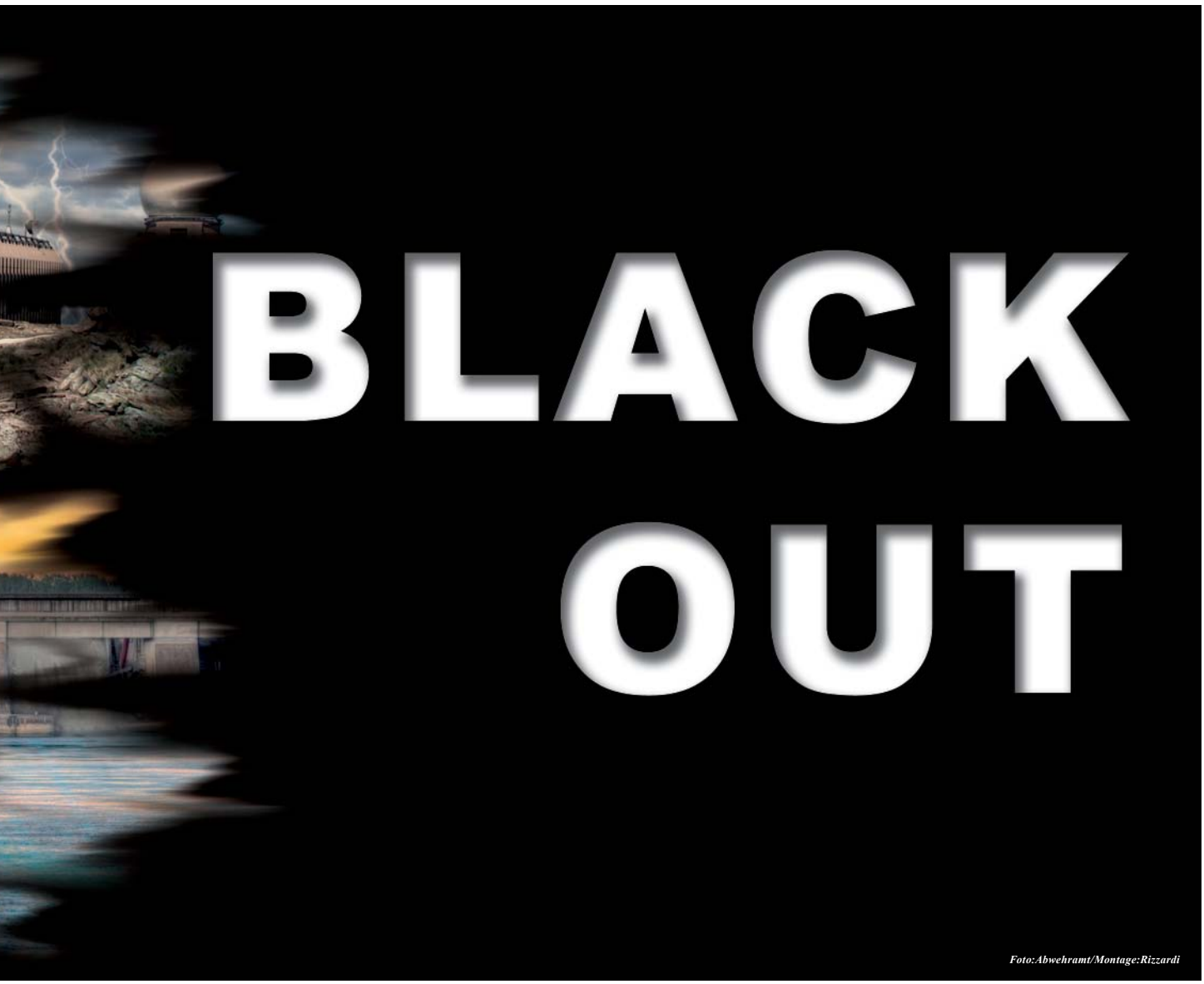


Foto:Abwehramt/Montage:Rizzardi

Die Ursachen für ein Blackout können vielfältig sein, manchmal auch sehr banal, wie die folgenden zwei Beispiele zeigen.

Blackout 2003

Italien kann seinen Strombedarf selbst nicht decken und muss einen wesentlichen Teil des Bedarfes aus der Schweiz bzw. aus Frankreich beziehen.

Am 28. August 2003 begann in Graubünden/Schweiz eine Verkettung von Ereignissen, die binnen einer halben Stunde in ganz Italien zu einem Blackout führten. In den frühen Morgenstunden schloss eine wichtige Strom-

Blackout

Hinter dem englischen Begriff verbirgt sich die etwas sperrige Beschreibung für einen plötzlichen, großräumigen und länger andauernden Stromausfall, wobei es keine klare quantitative Eingrenzung gibt.
In dieser Beitragsserie wird mit dem Begriff Blackout ein Stromausfall in einem großflächigen Gebiet assoziert, wobei unmittelbar keine externe Hilfe zugeführt werden kann, und dieses Blackout länger als eine Stunde dauert.
Die Auswertungen von bisherigen Blackouts haben ergeben, dass diese in der Regel von ein bis zwei nicht verbundenen Ereignissen ausgelöst wurden, die dominoartig zu Abschaltungen von Kraftwerken, Übertragungsleitungen und Schaltanlagen führten. Vor allem extreme Wetterbedingungen, menschliches Versagen und technische Mängel, oder eine Kombination dieser Faktoren, waren bis dato die häufigsten Ursachen.

Foto: Internet

Blackout: Notbeleuchtung in der finsteren Stadt.

transitleitung über einen Baum kurz. Diese wurde daraufhin automatisch abgeschaltet. Mehrfache Versuche, die unterbrochene Verbindung wieder in Betrieb zu nehmen, scheiterten. Daher musste eine benachbarte Leitung eine höhere Leistung aufnehmen. Kurz darauf führte die Mehrbelastung dieser Leitung zur erhöhten Erwärmung und zum starken Durchhängen der Leitungsseile, was wiederum zu einem Kurzschluss durch Berührung mit einem Baum führte.

Nach dem Ausfall der beiden wichtigen Leitungen folgte innerhalb von zwölf Sekunden kaskadenartig die Abschaltung der anderen grenzüberschreitenden Stromtransportleitungen nach Italien. In dieser Phase der Instabilität kam es in Norditalien zu einem starken Spannungsabfall, der die Abschaltung etlicher Kraftwerke bewirkte. Das italienische Stromversorgungssystem war nicht mehr in der Lage, die nunmehr vom Ausland abgeschnittene Stromversorgung aufrechtzuerhalten oder kontrollierte Abschaltungen durchzuführen. Zweieinhalb Minuten nach der Trennung vom übrigen Netz kollabierte in ganz Italien die Stromversorgung.

Mehr als 110 Züge mit rund 30 000 Passagieren waren während der Nacht stundenlang blockiert. Tausende saßen in Bahnhöfen und Flughäfen fest. In dem Chaos, das rund 56 Millionen Bürger betraf und in einzelnen Regionen bis zu 18 Stunden dauerte, kamen zumindest fünf Menschen durch Unfälle ums Leben.

Blackout 2006

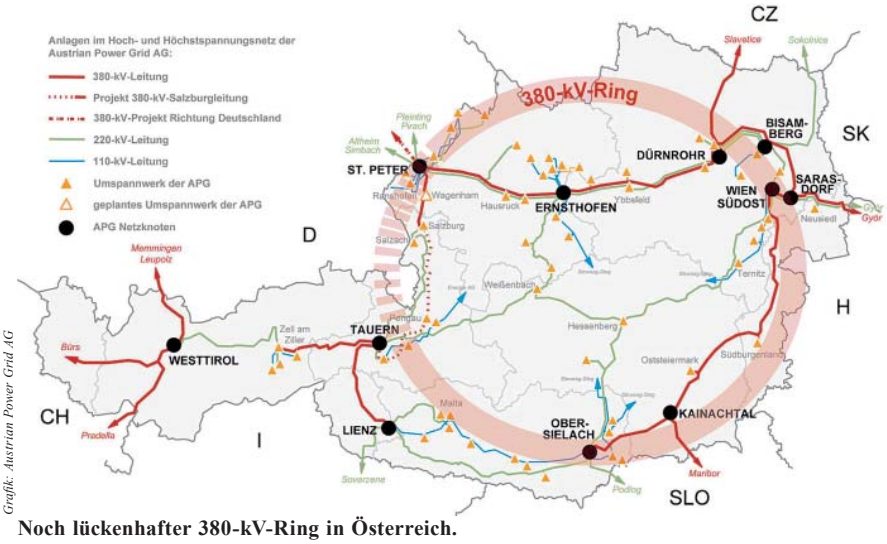
Menschliches Versagen führte am 4. November 2006, kurz nach 2200 Uhr, zu einem Blackout, das einen noch größeren geografischen Raum umfasste. Durch mangelhafte Planung, kurzfristige Änderungen und Kommunikationsfehler beim Bedienungspersonal kam es bei der geplanten Abschaltung einer Hochspannungsleitung im Raum Hamburg zu einer Kettenreaktion. Teile von Deutschland, Frankreich, Belgien, Italien, Österreich und Spanien waren bis zu 120 Minuten ohne Strom. Betroffen waren mehr als 15 Millionen Haushalte.

Durch das rasche Handeln des im Netzverbund operativ tätigen Personals, unter Einberufung des Krisenstabes, konnte ein österreichweites Blackout gerade noch verhindert werden. Aufgrund der Nachtzeit blieb das Blackout wohl weitgehend unbemerkt bzw. ohne schwerwiegende Folgen.

Wegen des noch nicht fertig gestellten 380-kV-Ringes läuft die europaweite Trennungslinie der Stromnetze quer durch Österreich. Durch diesen fehlenden Lückenschluss stellt das österreichische Hochspannungsnetz nach wie vor eine Schwachstelle im europäischen Netzverbund dar. Diese Beispiele zeigen sehr beeindruckend, wie ein relativ unbedeutendes Ereignis binnen weniger Minuten von einer friedlichen Lage zum Ausnahmezustand für Millionen von Menschen führen kann. In beiden Fällen war es wohl Glück, dass das Blackout in den Nachtstunden eintrat und daher nur beschränkt Folgen zu verzeichnen waren.

Strom - Lebensader moderner Gesellschaften

Strom ist die wichtigste Lebensader, da so gut wie alle anderen Lebensadern und damit die strategischen Infrastrukturen von der Verfügbarkeit



Grafik: Austrian Power Grid AG

Noch lückenhafter 380-kV-Ring in Österreich.

des elektrischen Stromes abhängen. Bei großflächigen und längerfristigen Stromausfällen sind erhebliche, wenn nicht sogar katastrophale Folgen für das gesamte Gemeinwesen zu erwarten. An zweitwichtigster Stelle folgen die Informations- und Kommunikationstechnikinfrastrukturen. Ohne technische Kommunikation sind viele Lebensbereiche nur sehr eingeschränkt funktionsfähig. Diese sind aber wiederum ganz wesentlich von der Verfügbarkeit von Strom abhängig. Die europäischen Stromnetze zählen bisher weltweit zu den stabilsten. Das kann nicht unbedingt linear in die Zukunft projiziert werden.

Es ist wichtig mögliche künftige Stromversorgungsprobleme aufzuzeigen, die Gesellschaft zu sensibilisieren und zur Übernahme von Eigenverantwortung zu animieren. Diese betrifft vor allem die Vorsorge im eigenen Umfeld, welche mit der Auseinandersetzung mit den möglichen Krisenszenarien beginnt und bis hin zu einer Eigenbevorratung und persönlichen Notfallplanung führt. Wer sich persönlich, emotional betroffen fühlt, wird auch darauf achten, wie Verantwortungs- und Entscheidungsträger mit der Thematik umgehen. Nur so kann es gelingen, diesem Thema Gehör zu verschaffen.

Die wahrscheinlichen Konsequenzen einer nicht verfügbaren Stromversorgung sind zu schwerwiegend, als dass bis zu einem möglichen Eintritt eines Blackouts zugewartet werden kann. Bei der bisherigen Bearbeitung dieses Themas wurde immer wieder Unverständnis festgestellt. In den seltensten Fällen ist den Verantwortungsträgern in Politik und Verwaltung sowie der Bevölkerung die volle Tragweite der Folgen eines langen Blackouts bewusst.

In diesem Zusammenhang ist ein Zitat von Professor Walter Seledec (Die „Lehren aus London“ TD Heft 5/2011, Seite 430) angebracht *„Anfang August erreichten uns Alarmmeldungen von den Britischen Inseln, die man kaum glauben konnte oder besser, deren Inhalt unserer bisherigen Vorstellung widersprach.“* Nur weil derzeit etwas nicht unseren Vorstellungen entspricht, bedeutet das nicht, dass es nicht dennoch eintreten kann. Es werden hier daher einige Aspekte beleuchtet, welche die Eintrittswahrscheinlichkeit eines solchen Ereignisses in einem anderen Licht erscheinen lassen. Bagatellisierungen wie *„Das wird schon nicht so schlimm werden!“* oder Anmaßungen wie *„Das haben wir alles im Griff!“* sind im höchsten Maße unverantwortlich.

Eine Aufzählung aller Probleme, die durch einen langzeitigen Stromverlust entstehen, würde den Rahmen dieses Beitrages sprengen. Es muss sich nur jeder überlegen, was alles nicht mehr funktioniert, wenn es keinen Strom gäbe und damit auch keine sonstigen Energieträger. Bereits nach etwa 24 Stunden Stromausfall muss mit einer besonders kritischen Lageentwicklung gerechnet werden. Durch eine fehlende Notstromversorgung der Zapfsäulenpumpen von Tankstellen und Tanklagern ist ein völliges Zusammenbrechen der Mobilität und der Kommunikationsmöglichkeiten auch für die Einsatzorganisationen zu erwarten.

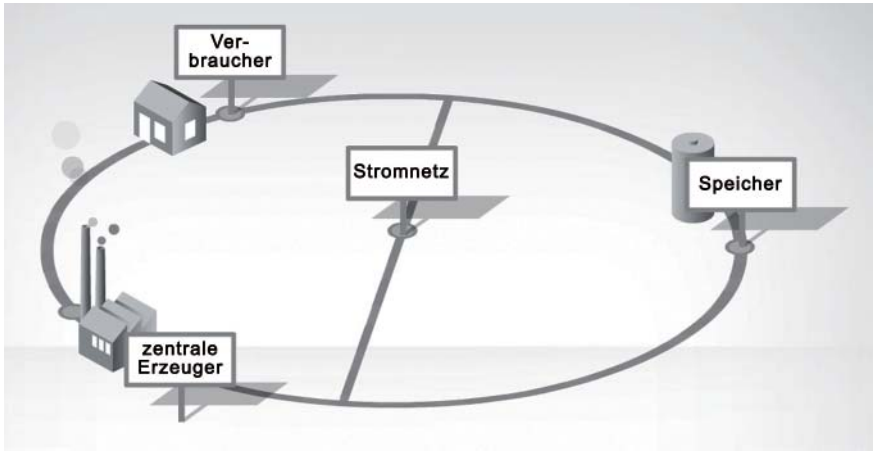
Es muss bereits jetzt festgelegt werden, welche zusätzlichen organisatorischen Maßnahmen zu den bisher getroffenen Krisen- und Katastrophenschutzvorkehrungen notwendig sind, um solchen Zusammenbruchsszenarien gesamtgesellschaftlich bestmöglich entgegnen zu können. Es sollen Denkanstöße und keine fertigen Lösungen geliefert werden. Durch die Komplexität der Thematik kann diese Blackoutsituation nicht von Einzelpersonen, losgelöst von verschiedenen vorhandenen Strukturen und Organisationen, betrachtet werden. Um dieses Krisenszenario zu erfassen, ist es notwendig, auch mögliche Folgen von Cyber-Konflikten auf die Stromversorgung zu betrachten. Einen ersten Vorgeschmack auf diese Problematik hat die technisierte Welt mit der 2010 bekannt gewordenen Schadsoftware

Foto: Abwehramt

Strategische Infrastruktur.

Strategische Infrastruktur

Darunter versteht man Versorgungs- und Basisinfrastrukturen, deren Ausfall gravierend negative Auswirkungen auf das öffentliche Leben und die Gesellschaft nach sich zieht und in weiterer Folge die nationale Sicherheit erheblich beeinträchtigt.
Dazu zählen die Bereiche Energieversorgung, Telekommunikation, Finanzwesen, Gesundheitsbereich, Ver- und Entsorgungs- und das Transportwesen sowie die öffentliche Sicherheit.
Anderer Begriff dafür ist:
Kritische Infrastruktur bzw. Critical Infrastructure.



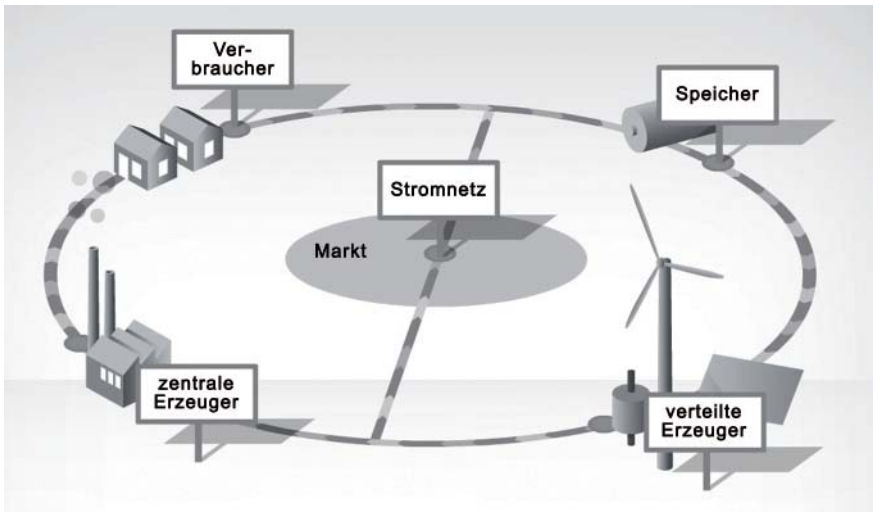
Grafik: www.smatgrids.at

Stromnetz gestern.

STUXNET („STUXNET - Ein Cyber War Angriffsprogramm“ TD Heft 2/2011, Seite 148) bekommen. Nach kaum verifizierbaren Informationen dürfte diese Schadsoftware gegen ein ganz spezielles und gut geschütztes Ziel, nämlich das iranischen Atomprogramm bzw. die dafür erforderliche Urananreicherung, gerichtet gewesen sein. Diverse Quellen sprechen von einem erfolgreichen Angriff. Um wie viel einfacher könnte ein solcher Angriff auf die weit weniger geschützte und aufgrund der vielen Schnittstellen auch nicht wirklich vollständig zu sichernde Strominfrastruktur sein?

Das Österreichische Bundesheer wird bei einem großen Blackout eine sehr wichtige Rolle einnehmen müssen. Daher sind bereits jetzt entsprechende Ableitungen und Vorbereitungsmaßnahmen in enger Kooperation mit den Blaulichtorganisationen zu treffen. Im Anlassfall muss davon ausgegangen werden, dass die technischen Kommunikationsmöglichkeiten weitgehend nicht zur Verfügung stehen werden. Entsprechende Planspiele und Übungen dazu sind essenziell. Nur so können die entsprechenden Lehren gezogen, Verbesserungsmaßnahmen umgesetzt und bei einem Blackout vorbereitete und automatisierte Abläufe mit geringem Kommunikationsaufwand aktiviert werden.

Durch eine Forschungseinrichtung wurde, aufbauend auf bereits vorhandene Grundlagen und Erkenntnisse, ein umfangreiches Berechnungsmodell über den wahrscheinlichen volkswirtschaftlichen Schaden durch ein Blackout erstellt. Je nach Jahres- und Tageszeit sind enorme Verluste zu erwarten. Als Berechnungsbeispiel diente dazu ein Novembertag, 0900 Uhr Vormittag. Ein österreichweites, einstündiges Blackout wurde an so einem Tag mit einem Gesamtschaden von rund 180 Millionen Euro berechnet. Dauert das gleiche Blackout 24 Stunden, so sind das bereits 890 Millionen Euro Schaden!



Grafik: www.smatgrids.at

Stromnetz heute.

Verletzlichkeitsparadoxon

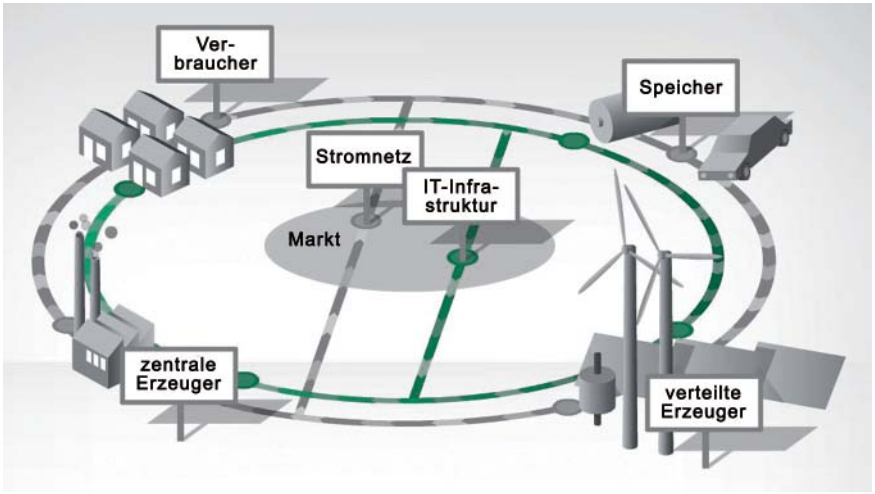
In diesem Zusammenhang beschreibt das „Verletzlichkeitsparadoxon“ den Widerspruch zwischen Risikowahrnehmung und Realität. Die meisten technisch entwickelten Staaten weisen eine relativ zuverlässige, über lange Zeiträume funktionierende Stromversorgung auf. Darüber hinaus bauen nahezu alle technischen Systeme und sozialen Handlungen auf dieser relativen Verlässlichkeit auf. Nicht oder nur unzureichend wird die damit einhergehende massive Verletzbarkeit bei einer längeren Unterbrechung der Stromversorgung berücksichtigt. Darüber hinaus führt dies dazu, dass oft aus Kostendruck die Versorgungsleistungen zunehmend weniger störsicher organisiert werden.

(n-1)-Kriterium

Überregionale Stromnetze werden nach dem (n-1)-Kriterium betrieben. Das bedeutet, dass die automatischen Regel- und Sicherheitseinrichtungen so konfiguriert sind, dass zu jeder Zeit ein elektrisches Betriebsmittel, etwa ein Umspannwerk, eine Hochspannungsleitung oder ein Kraftwerk ausfallen darf, ohne dass es zu einer Überlastung eines anderen Betriebsmittels oder gar zu einer Unterbrechung der Energieversorgung kommen darf. Wenn beispielsweise eine Überlandleitung aus irgendeinem Grund ausfällt, wird der Strom auf andere Leitungen verteilt und die schadhafte Stelle wird im Netzprinzip umgangen. Tritt aber zeitgleich ein weiterer Fehler im benachbarten Segment auf, kommt es zu einer Überbelastung des regionalen Netzes und die betroffenen Betriebsmittel werden zum Eigenschutz automatisch abgeschaltet. Im korrekt betriebenen System müssen also mindestens zwei Ereignisse zusammentreffen, damit überhaupt eine Versorgungsunterbrechung entstehen kann. Dies kann dann zu einem Dominoeffekt und zu großräumigen Abschaltungen führen, die in einem Blackout enden.

70 Prozent-Regel

Eine wichtige Voraussetzung für den sicheren Netzbetrieb nach dem (n-1)-Kriterium ist die „70 Prozent-Regel“. Dies bedeutet, dass Hochspannungsleitungen nur mit 70 Prozent der vorgesehenen Gesamtbelastbarkeit auf Dauer betrieben werden sollen, um bei Bedarf entsprechende Reserve- bzw. Überkapazitäten aufnehmen zu können. Wenn diese Reserve nicht ausreicht, oder durch eine bereits erhöhte Permanentlast ausgeschöpft ist, kann dies zu einer folgenschweren Sicherheitsabschaltung, wie im Jahr 2003 in der Schweiz, führen.



Grafik: www.smartgrids.at

Stromnetz morgen.

Folgen eines Blackouts

Ein Zusammenbruch der Stromversorgung wirkt sich ohne Vorwarnung und übergangslos zu 100 Prozent auf alle elektrischen Geräte und Einrichtungen aus, die nicht von Batterien oder Akkus gespeist werden bzw. für diesen Notfall nicht an eine Netzersatzanlage in Form eines Notstromaggregates etc. angeschlossen sind.

Je nach Jahres- und Tageszeit werden sich die Folgen entsprechend rasch auswirken. Die großen Blackouts von 2003 und 2006 passierten in der Nacht und wurden meist in dieser Zeit noch behoben. Daher waren die Folgen beschränkt bzw. wurde der Zwischenfall von der Masse der Bevölkerung verschlafen. Passiert ein solcher Zwischenfall während des Tages oder dauert dieser länger an, dann ist mit völlig anderen Konsequenzen zu rechnen.

Ursachen für ein Blackout

Die Ursachen für einen lang andauernden und überregionalen Stromausfall können vielfältig sein:

- Menschliches Versagen (Schaltfehler, Unaufmerksamkeit etc.);
- Systemische, organisatorische Mängel (Netzaufsplitterung, übertriebenes Gewinnstreben etc.);
- Technisches Versagen (Wartungsmängel, Überalterung von Anlagen, Fehldimensionierungen von Betriebsmitteln, mangelhafte Planung und Umsetzung, Materialfehler, Produktionsfehler, Ausfall von zentralen Betriebsmitteln etc.);
- Kriminalität/Terrorismus (Betrug, Erpressung, Sabotage, Anschläge, Kabeldiebstahl, Cyber Angriff auf Steuersysteme etc.);
- Ressourcenausfall der Primärenergie (Mangel an Wasser, Wind, Öl, Gas, Kohle oder Brennstäben etc.);
- Pandemie (krankheitsbedingter Ausfall von Betriebspersonal);
- Klima/Klimawandel/Naturereignisse (Blitzschlag, Stürme, Hochwasser, Schnee/Eis, Erdbeben, Sonneneruptionen etc.);
- Kriegerische Auseinandersetzungen (Zerstörung von elektronischen Bauteilen durch einen Elektromagnetischen Puls/EMP, Einsatz von Cyber Waffen).

Hier werden noch einige mögliche Ursachen näher beschrieben, die jederzeit unter Berücksichtigung des (n-1)-Kriteriums zu einem Blackout führen können bzw. die Basis dazu liefern. Dabei werden nur Ursachen berücksichtigt, die derzeit permanent anzutreffen sind. Menschliche Ursachen, wie Sabotage oder gezielte Angriffe werden in einem nachfolgenden Beitrag behandelt.

Das europäische Verbundnetz

Das europäische Verbundsystem ist ein europaweites, engmaschiges Stromnetz aus Hoch- und Höchstspannungs-Leitungen zur Verteilung von elektrischer Energie und besteht aus mehreren physisch voneinander getrennten Netzen (z. B. Zentraleuropa, Skandinavien, Großbritannien). Die Vernetzung im jeweiligen Teilbereich war bisher für die Stabilität des Gesamtnetzes sehr wichtig, da dadurch Reserven großräumiger eingesetzt werden konnten.

Das österreichische Stromnetz

In Österreich treten ungefähr 10 000 kleine bis mittelgroße Stromausfälle pro Jahr auf. Die meisten davon sind für die Endkunden, aufgrund der sehr kurzen Dauer, in der Regel nicht wahrnehmbar. Diese Unterbrechungen sind meist lokal begrenzt und werden durchschnittlich in etwa 70 Minuten behoben. Für alle Stromkunden ergab sich z. B. 2009 damit im Durchschnitt (bei nicht angekündigten Unterbrechungen) eine Stromunterbrechung von 36,7 Minuten. In Deutschland betrug die Ausfallszeit sogar nur 16,5 Minuten. Diese Zuverlässigkeit der Stromversorgung macht auch nachvollziehbar, dass es kein entsprechendes Problembewusstsein hinsichtlich möglicher Blackoutszenarien gibt.

Das derzeit bestehende österreichische Übertragungsnetz ist großteils 60 Jahre alt. Der Stromverbrauch hat sich seit dieser Zeit nahezu verfünffacht. Daher arbeitet das Übertragungsnetz an seiner Leistungsgrenze. Insbesondere die Nord-Süd-Verbin-

dungen sind massiv überlastet. Eine nachhaltige Entspannung kann erst durch den Lückenschluss des 380-kV-Ringes entstehen. Ähnliche Szenarien gibt es auch in anderen Ländern. Durch diese permanente Überlastung bestehen kaum Reserven, um bei Ausfall eines Teilstückes die Lastverteilung ohne Probleme durchführen zu können.

Strommarktliberalisierung

Mit der von der EU forcierten Strommarktliberalisierung ab Ende der 1990er Jahre sollte ein reibungsloser Elektrizitätshandel zwischen den Mitgliedstaaten umgesetzt werden. Die Energieversorgung gehörte bis dahin zu den Kernaufgaben des Staates und daher waren große Teile der Stromproduktion und des Energienetzes fest in staatlicher Hand. Die ursprüngliche Intention, die Monopolstellung aufzubrechen und durch den freien Markt auch eine Preissenkung für die Verbraucher zu ermöglichen, ist mittlerweile weitgehend hinfällig. Einerseits wird die Möglichkeit eines Stromlieferantenwechsels kaum in Anspruch genommen und andererseits bleiben immer weniger große Stromanbieter übrig, so dass die Preisunterschiede zunehmend geringer werden.

Nachdem der Strommarkt nun marktwirtschaftlich ausgerichtet ist, müssen die Unternehmen auch Gewinne erwirtschaften. Dies bedeutet, dass erforderliche Investitionen nicht in jedem Fall umgesetzt oder hinausgeschoben werden. Das ist zwar längerfristig teurer, beschert aber kurzfristig Gewinne. Diese Entwicklung konnte in einigen europäischen Ländern beobachtet werden. In diesem Zusammenhang spielt vor allem das Alter eines Bereiches der europäischen Stromnetzinfrastruktur eine Rolle. Teile davon sind 50 Jahre alt oder noch älter und erfordern daher eine Wartung. Trotz Erfüllung der entsprechenden Vorschriften, hat der rund 60 Jahre alte Stahl der Strommasten, beim Blackout im Münsterland 2005, eine Rolle gespielt. *„Als Ursache für das Versagen des Mastens 65 in BL1503 konnte die Kombination aus wetterbedingt hohen einseitigen Zusatzlasten und Bauteilen aus versprödetem Thomasstahl widerspruchsfrei identifiziert werden.“* (Bundesamt für Materialforschung und -prüfung: Schadensanalyse an im Münsterland umgebrochenen Strommasten. Internet, 2006, URL: http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Energie/Sonderthemen/VersorgungsstoerungMuensterland05/BAMGutachtenId6409pdf.pdf?_blob=publicationFile [12.12.11], S. 2.)

Foto: Internet

Mastbruch im Münsterland 2005.

Die wesentliche Rolle spielten jedoch mehrere Extremwetterereignisse, wie starke Schnee- und Eislasten auf den Stromleitungen, starke Winde und zusätzlicher Regen. In Folge wurden fünf Fernleitungen schwer beschädigt und rund 50 Strommasten sind reihenweise zusammengebrochen.

Ein Untersuchungsbericht hält dazu fest *„Zu der Schadenssituation im Münsterland ist es nur gekommen, weil mehrere Schadensauslöser gleichzeitig aufgetreten sind. ... Eine Erkenntnis aus den Ursachen der Versorgungsstörung im November 2005 ist, dass ein solcher Störfall sich überall erneut ereignen kann.“*

Der mehrtägige Stromausfall im dünn besiedelten Münsterland im Jahr 2005 löste Schäden von schätzungsweise 130 Millionen Euro aus. Die Vernachlässigung von Betriebsmitteln hinsichtlich Wartung und Erneuerung aus Gewinnstreben ist ein ständig wiederkehrender Vorwurf an die Elektrizitätsgesellschaften. Bisher werden vor allem in den USA immer wieder größere Zwischenfälle damit in Zusammenhang gebracht.

Ein anderer Vorwurf richtet sich seitens der Elektrizitätswirtschaft an die Politik. Durch den marktregulierenden Eingriff und die Aufsplittung des hochkomplexen Systems der Stromversorgung in möglichst viele Teile der Lieferkette haben sich nicht zu vernachlässigende Risiken ergeben. So kann es nun vorkommen, dass jene Funktionsträger, die früher räumlich in einer Leitstelle zusammengefasst waren und ein eingespieltes Team bildeten, nun viele Kilometer voneinander getrennt sind. Darüber hinaus kann es aus rechtlichen Gründen, z. B. bei Haftungsfragen, zu Verzögerungen oder gar Unterlassungen von Informationsübermittlungen kommen, weil die beteiligten Stellen nicht derselben Organisation angehören.

Bisherige Beispiele haben gezeigt, dass besonders in Notfällen ein rasches und entschiedenes Handeln erforderlich ist, um folgenschwere Zwischenfälle zu verhindern. Es bleiben nur wenige Minuten, um zu reagieren, bevor das Versorgungssystem kollabiert.

Der finanzmarktorientierte Eingriff in das komplexe System der Stromver-

sorgung könnte langfristig negative Folgen für die Versorgungssicherheit nach sich ziehen. Die überhastete Implementierung von intelligenten Stromzählern („Smart Meter“) in das hoch komplexe System verstärkt diese Befürchtung.

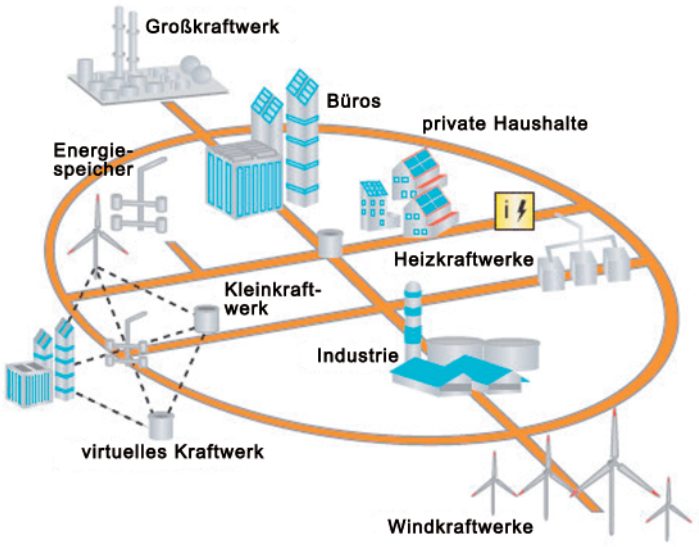
Erneuerbare Energieträger

Erneuerbare Energieträger, wie etwa Wind- oder Sonnenenergie, spielen in Europa bereits heute eine nicht mehr vernachlässigbare Rolle in der Stromerzeugung. Großflächige Ausfälle, z. B. durch schneebedeckte Photovoltaik-Anlagen oder fehlenden Wind für Windkraftanlagen, können rasch die vorgehaltenen Primärregelleistungen (Reserven) ausreizen, insbesondere nach der mittelfristig absehbaren Abschaltung zahlreicher Atomkraftwerke. Auch die verstärkte Einspeisung von Strom aus Photovoltaikanlagen und Windkraftwerken kann zur Destabilisierung des Stromnetzes führen (das 50,2 Hertz-Problem). Erneuerbare Energiequellen haben den Nachteil, dass sie nicht permanent zur Verfügung stehen. Daher müssen die Speicherkapazitäten erheblich ausgebaut und zusätzlich völlig neue technische Wege beschritten werden. Dieses Erfordernis kann aber nicht zeitlich mit den sonstigen Entwicklungen mithalten. Der Ausstieg aus der Atomenergie ist zwar zu begrüßen, durch die kurzfristige Umsetzung muss jedoch mit einer Destabilisierung der europäischen Stromversorgungssicherheit gerechnet werden.

Dass eine Dringlichkeit zum raschen Ausbau von stärkeren Verteilungsnetzen („Stromautobahnen“) besteht, lässt sich auch aus einer in Bearbeitung befindlichen EU-Verordnung ableiten. Diese sieht für die Planung und Genehmigung wichtiger europäischer Gas- und Stromleitungen eine Verkürzung auf drei Jahre vor. Bisher dauerten diese Verfahren in vielen Ländern häufig länger als zehn Jahre.

Intelligente Stromnetze

Unsere bisherige Stromversorgung ist auf relativ einfache Strukturen ausgelegt. Es gab große, zentrale Erzeuger bzw. Großkraftwerke, ein Verteilungsnetz, Speicher (z. B. Pumpspeicherkraftwerke) und die Verbraucher. Der Vorteil einer zentralen Struktur ist ein verringerter Koordinierungsaufwand, der aber zu Lasten der Flexibilität der Netzwerke geht.



Grafik: Greenpeace

Smart Grid.

Durch den verstärkten Einsatz von erneuerbaren Energien (insbesondere Sonnen- und Windenergie) und der damit einhergehenden dezentralen Stromerzeugung, sowie durch das Verbraucherverhalten entstehen deutlich mehr Anforderungen an die Stromnetze und erfordern eine komplexe Netzwerksteuerung. Es laufen derzeit die Vorbereitungen zur Implementierung von intelligenten Stromnetzen („Smart Grids“), wodurch die Komplexität aber erheblich steigen wird, da es zu einer verstärkten, direkten Vernetzung und damit auch Abhängigkeit zwischen Strom- und (IKT-) Steuerungsnetzen kommt. In der Fachwelt spricht man bereits von den größten IKT-Projekten, die in diesen Bereichen jemals durchgeführt wurden. Betrachtet man die sicherheitskritischen Entwicklungen im Bereich der IKT der vergangenen Monate, dann bedeutet das wohl eine erhebliche Herausforderung für die Zukunft, da die Stromversorgungssicherheit weiterhin gewährleistet werden muss.

Intelligente Stromzähler

Obwohl die genauen Anforderungen an die intelligenten Stromnetze noch nicht beschrieben sind, wird eifrig an der Umsetzung eines möglichen Teilaspektes gearbeitet. Die Vorbereitung bzw. Einführung von intelligenten Stromzählern („digitale Stromzähler - Strommesscomputer“), statt der bisherigen mechanischen Ferariszähler, läuft auf Hochtouren.

In der Forschungsarbeit *„Smart Metering und mögliche Auswirkungen auf die nationale Sicherheit“* wurden erhebliche Bedenken zur derzeit geplanten Einführung von intelligenten Stromzählern festgestellt. Größtes Manko sind die fehlenden Risikoanalysen und Technikfolgen-Abschätzungen.

Durch die bisherige Trennung des Stromnetzes von sonstigen öffentlichen Netzen ist ein relativ hohes Sicherheitsniveau gegeben. Durch die Absicht, IKT-Netze mehr oder weniger direkt mit dem Stromnetz zu verbinden, zumindest aber bisher im IKT-Bereich als unsicher geltende Systeme im Bereich der Stromnetze einzusetzen, ergibt sich

Foto: Cyber Security Austria

Digitaler Stromzähler - Strommesscomputer links, mechanischer Ferariszähler rechts.

CYBER SECURITY AUSTRIA

„Cyber Security Austria - Verein zur Förderung der Sicherheit Österreichs strategischer Infrastruktur“ ist eine gemeinnützige, unabhängige, überparteiliche Organisation auf Vereinsbasis. Die Zusammenarbeit erfolgt auf ehrenamtlicher Basis. Ziel ist die Steigerung des Sicherheitsbewusstseins in Österreich, insbesondere mit Fokus auf die Erhöhung der Widerstandsfähigkeit Österreichs strategischer Infrastruktur. Zweck ist die Sicherstellung der Wohlfahrt für Österreichs Bürger und Bürgerinnen.
www.cybersecurityaustria.at
Die Sensibilisierung steht im Vordergrund: res publica (zum Volk gehörig/öffentlich).
Die Schaffung von öffentlichem Bewusstsein ist erforderlich, da mit dem Einsatz moderner Technik auch erhebliche Risiken eingegangen werden, die bis hin zur Gefährdung des gesellschaftlichen Lebens gehen können.
Strategische Ziele:
- Schaffung von Bewusstsein und Lösungen für organisatorische und nicht technische Probleme.
- Schaffung von Grundlagen für das staatliche Krisenmanagement.
- Identifizierung der IKT-Einflussgrößen auf die Verwundbarkeit Österreichs und der gesellschaftlichen Lebensfähigkeit.
- Bewusstseinsschaffung bei Entscheidungsträgern für die Etablierung eines adäquaten Krisenmanagements und entsprechender Präventivmaßnahmen.

Zielgruppen:
Sicherheit ist längst eine Querschnittsmaterie geworden. IKT-Sicherheit muss daher in möglichst viele Bereiche der Ausbildung einfließen - z. B. im Management- oder Marketingbereich und nicht nur in einschlägigen technischen Fachgebieten. Interessensvertretungen in Wirtschaft und Politik, die Gesellschaft, NGOs wie Blaulichtorganisationen oder die öffentliche Hand, sind Zielgruppen von Cyber Security Austria.

eine völlig neue Situation. Diese wird mit dem Wissen, dass es auch in den bestehenden Stromnetzen ausreichend Schwachstellen gibt, welche jedoch so gut wie nicht ausgenutzt werden können, noch erheblich erschwert. Als Höhepunkt wird mit dem Smart Meter eine neue, in der derzeitigen Form wahrscheinlich als unsicher einzustufende Technologie in eine vor unbefugtem Zugriff ungesicherte Umgebung beim Endkunden als Netzeintrittspunkt eingebaut. Bisherige Untersuchungen zeigen, dass es zahlreiche Möglichkeiten gibt, diese Endgeräte (Smart Meter) zu manipulieren.

Im schlimmsten Fall ist damit zu rechnen, dass es gelingt, über das Endgerät direkt in das restliche Steuernetz einzudringen. Die Folgen sind unabsehbar, die Folgekosten dieser manipulativ verursachten Schäden wären enorm. Daher wird mit der, in der derzeitigen Form, geplanten Implementierung von Smart Meter eine sehr gefährliche Angriffsschnittstelle geschaffen. Die Betriebssicherheit („safety“) von intelligenten Stromnetzen und -zählern hängt wesentlich von der Angriffssicherheit („security“) ab. In der bisherigen Diskussion kommt die Angriffssicherheit und Risikobewertung weitgehend zu kurz. Ein Gegenargument dazu könnte sein, dass es schon zahlreiche Länder mit flächendeckenden Implementierungen von intelligenten Stromzählern und längerer Betriebserfahrung gibt, bis dato aber kaum größere Zwischenfälle bekannt wurden. Diesem Argument ist mit den Erfahrungen aus dem IKT-Bereich zu entgegnen.

Die Angriffe auf Computersysteme haben sich im Laufe der Jahre entwickelt und mittlerweile ein bedenkliches Ausmaß erreicht. Eine ähnliche Entwicklung muss auch im Bereich von intelligenten Stromzählern erwartet werden. Die Verwundbarkeit wird mit dem Umfang der Implementierung steigen. Einerseits, weil damit die Komplexität des Gesamtsystems steigt und andererseits, weil sich damit für mögliche Angreifer lohnendere Ziele ergeben. Im Unterschied zum IKT-Bereich sind aber bei einem Angriff auf die Strominfrastruktur die Folgen wesentlich verheerender und weitreichender. Bei der etablierten Strominfrastruktur gibt es keine Möglichkeit von „Testphasen“ und kein ständiges Nachbessern, wie im IKT-Bereich.

50,2 Hertz-Problem

Um die Verbraucher mit elektrischer Energie zu versorgen, benötigt man Leitungen von den Stromerzeugern (Kraftwerken und Windkraftanlagen) zu den Verbrauchern. Dazu verwendet man Stromnetze mit verschiedenen, festgelegten Spannungen; bei Wechselstrom sind auch Frequenzen festgelegt.

In Europa wird die elektrische Energie mittels Dreiphasenwechselstrom mit einer Netzfrequenz von 50 Hz und einer Netzspannung von im Regelfall bis zu 400 kV im Verbundnetz übertragen. Bisher mussten sich Wechselrichter (ein elektrisches Gerät, das Gleichspannung in Wechselspannung bzw. Gleichstrom in Wechselstrom

umwandelt) von Photovoltaik-Anlagen bei einer Überschreitung der Netzfrequenz bei 50,2 Hertz unverzüglich vom Netz trennen.

Im Extremfall schalten sich dann mehrere Gigawatt an Leistung gleichzeitig ab. Dieser Leistungsabfall kann dann möglicherweise nicht mehr stabilisiert werden. Der Ausgleich dieser Spannungsschwankung bei einer Frequenzerholung kann durch ein zeitgleiches Wiederzuschalten von zusätzlichen Kraftwerken zu einem erneuten Überschreiten der Frequenz von 50,2 Hertz und damit zu einem neuerlichen Abschalten der Erzeugungsanlagen am Niederspannungsnetz führen („Jo-Jo"-Effekt). Die Folgen wären wahrscheinlich katastrophal. Daher müssen in Deutschland die Wechselrichter der Photovoltaik-Anlagen ab 2012 durch „fehlertolerantere Systeme" nachgerüstet bzw. ausgetauscht werden.

Elektromobilität

Derzeit gibt es umfangreiche Diskussionen zur Zukunft der Elektromobilität, worin eine große ökonomische und ökologische Chance gesehen wird. Damit wird auch die Komplexität der Stromnetze und -versorgung sowie deren Abhängigkeit weiter massiv ansteigen.

Der möglicherweise zukünftige verstärkte Einsatz von Elektroautos und der damit verbundene Anstieg im Strombedarf ist an sich noch keine Ursache für ein Blackout. In Kombination mit den bisher aufgezählten Problembereichen, wie teil- bzw. zeitweise unzureichende Produktionskapazitäten, aber vor allem mit den bereits jetzt überlasteten Stromleitungen, wird das Risiko deutlich erhöht werden. Ob dieses, durch den möglichen Ansatz Elektroautos in der Stehzeit als Stromspeicher bzw. als Puffer zu verwenden, kompensiert werden kann, muss erst verifiziert werden.

Daher muss auch in diesem Bereich eine gesamtheitliche Betrachtung bereits in der frühen Planungsphase erfolgen. Der Fokus darf dabei nicht am Einzelsystem hängen bleiben. Umfassende Risikoanalysen dazu sind unverzichtbar.

Koronaler Massenauswurf (KMA)

Bei einem KMA (Coronal Mass Ejection/CME) handelt es sich um eine Sonneneruption, bei der riesige Mengen elektrisch geladener Gase (Plasmawolken) in den Weltraum hinausgeschleudert werden. Wenn diese Gase Richtung Erde geschleudert werden, wird das Erdmagnetfeld stark deformiert und die von der Sonne kommenden Teilchen fließen als elektrischer Strom in Spiralbahnen zu den Polen der Erde, wo sie Polarlichter auslösen. Diese Teilchen benötigen etwa 24 bis 36 Stunden, bis sie auf die Erde treffen. Die Wirkung dauert etwa 24 bis 48 Stunden an. Je nach Stärke des Sonnensturmes und der auftreffenden Teilchen können durch induzierte Überspannungen Schäden an Satelliten, Störungen im Funkverkehr (inkl. GPS-Navigation) oder im schlimmsten Fall Blackouts verursacht werden. Im März 1989 wurde dadurch in Kanada ein mehrstündiges Blackout verursacht, von dem sechs Millionen Menschen betroffen waren. Dabei wurden zum Teil Stromnetze und elektrische Geräte zerstört. Die Masse der heutigen Informations- und Kommunikationstechnikinfrastrukturen wurde aber erst in den vergangenen 25 Jahren

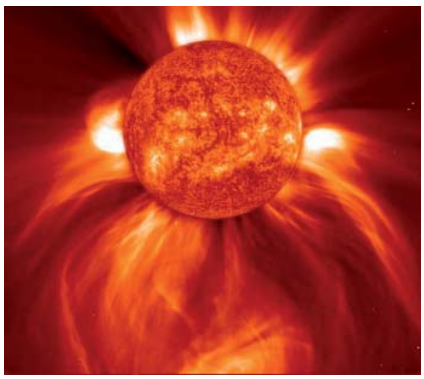


Foto: ESA

Sonnensturm.

entwickelt. Daher können wir die möglichen Folgen eines solchen Zwischenfalles heute wahrscheinlich gar nicht richtig erfassen oder beurteilen. Sicher ist jedoch, dass nach einer langen Phase an relativer Inaktivität, die Aktivität der Sonne in den vergangenen Monaten deutlich gestiegen ist. Die NASA erwartet in den nächsten Jahren erhöhte Sonnenaktivitäten.

Mangelndes Risikobewusstsein

Das Deutsche Rote Kreuz gab 2008 eine Umfrage in Auftrag: *„Stellen Sie sich bitte vor, es gäbe 14 Tage Stromausfall. Das bedeutet unter anderem, kein Geld aus dem Bankomat, kein*

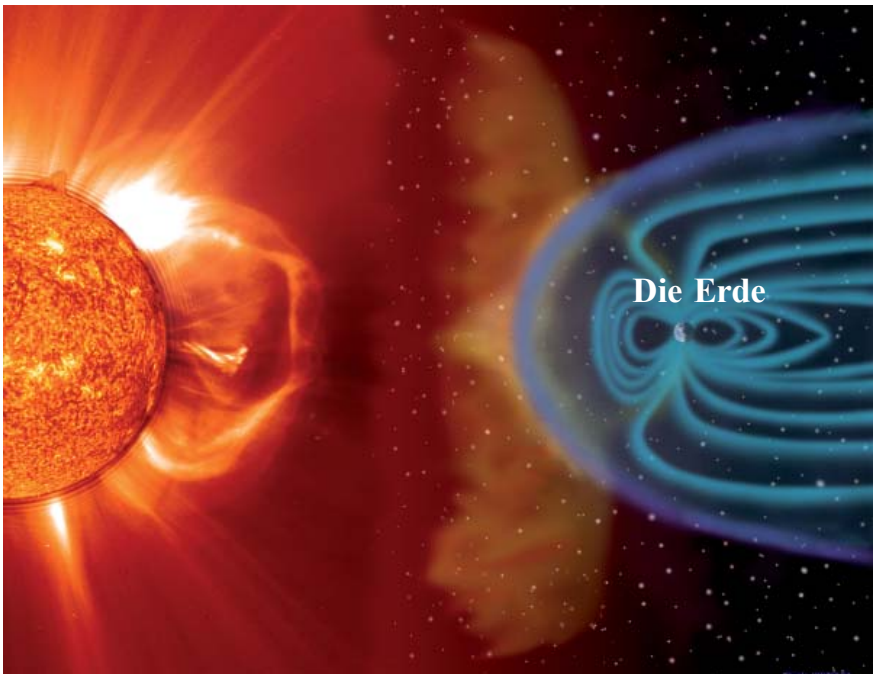


Foto: ESA/NASA - SOHO LASCO EIT

Koronaler Massenauswurf und Plasmawolken treffen auf das Magnetfeld der Erde.

Komplexe Systeme

Komplexe Systeme zeichnen sich dadurch aus, dass sie viele relevante Variable besitzen und diese in unübersichtlichen, meist nicht-linearen Beziehungen zusammenhängen. Sie verhalten sich anders als die reine Summe ihrer Einzelteile.

Komplexität hat sehr viel mit Vernetzung zu tun, sie kommt eigentlich erst durch diese zustande. Die Wirkung eines Eingriffes in ein komplexes System tritt üblicherweise nicht sofort ein bzw. kann oft auch nur indirekt festgestellt werden. Daher wird durch Entscheidungsträger häufig kein unmittelbarer Handlungsbedarf gesehen.

Durch den Drang, alles exakt zu planen, entsteht die Notwendigkeit, Fehler auszuschließen, was eigentlich genau den gegenteiligen Effekt auslöst, da es keine Fehlerfreiheit gibt. Zielführender wäre die Steigerung der Fehlertoleranz, um damit die Erhöhung und Sicherung der Überlebensfähigkeit eines Systems zu fördern. Bestes Beispiel dafür ist die Natur oder der Mensch selbst. Nur durch eine Fehlerfreundlichkeit und Symbiose mit seiner Umwelt konnte die Überlebensfähigkeit langfristig gesichert werden.

Zwei wichtige Erkenntnisse aus der Kybernetik lauten, dass Störungen und Fehler an einer Stelle sich möglichst nicht automatisch auf alle anderen übertragen sollen. Unter Kybernetik ist die Erkennung, Steuerung und selbsttätige Regelung ineinander übergreifender, vernetzter Abläufe bei minimalem Energieaufwand zu verstehen. Sie ist der Natur abgeschaut, wo bisher nur Systeme überlebt haben, die ihren Energieaufwand bestmöglich minimieren und optimieren konnten.

Ein unvernetztes System ist nicht stabil. Mit wachsender Vernetzung steigt die Stabilität zunächst an, bis sie ab einem bestimmten Vernetzungsgrad wieder absinkt. Es sei denn, es bilden sich Unterstrukturen. Dann bleibt das System auch bei hoher Vernetzung lebensfähig. Ein Negativbeispiel aus der Biologie ist der Tumor, wo der anfänglich großartige Erfolg im Wachstum letztendlich zur Selbstzerstörung führt. Zur Optimierung der Überlebensfähigkeit muss ein System laufend hinsichtlich Selbstregulation, Flexibilität und Steuerbarkeit analysiert und angepasst werden.

Sprit an der Tankstelle, keine Kühlung im Supermarkt. Glauben Sie, Sie wären in der Lage, sich selbst zu versorgen?“. Auf diese Frage antworteten von 1 000 Personen 76 Prozent mit „ja“.

Dieses Ergebnis wurde auf „eine trügerische Annahme“ und Selbstüberschätzung zurückgeführt, die auf einem völligen Mangel an Information und daher auf mangelndem Risikobewusstsein begründet ist. Das Deutsche Rote Kreuz sieht die Lage realistischer und geht davon aus, dass das öffentliche Leben in kürzester Zeit zusammenbricht und chaotische Zustände ausbrechen werden. Die Handlungsfähigkeit der Einsatzorganisation wird sich dabei auf wenige Stunden beschränken.

In einer Studie zum Blackout im Münsterland im Herbst wird u. a. die Wichtigkeit aufgezeigt, dass seitens der staatlichen Stellen Konzepte zur Notfallversorgung im öffentlichen wie auch im privaten Bereich zu aktualisieren und weiterzuentwickeln sind. Die während des Kalten Krieges vorhandenen Eigenvorsorgemaßnahmen, wie etwa die Eigenbevorratung, werden heute von vielen Menschen mit den Attributen „veraltet“ und „nicht mehr zeitgemäß“ verknüpft, was jedoch im Anlassfall fatal sein könnte.

Eine weitere Erkenntnis war, dass die Erwartungshaltungen auf beiden Seiten - Behörden und Bevölkerung - auf Dauer nicht miteinander zu vereinbaren sind. Vor allem wurden erhebliche Defizite in der Kommunikation zwischen Staat und Bevölkerung festgestellt. Die an den Erwartungen der Katastrophenschutzbehörden gemessene lückenhafte Selbsthilfefähigkeit der privaten Haushalte und das im Krisenfall nicht ausreichende Bevorratungsverhalten sind jedoch keine neuen Themen. Deshalb muss eine Verbesserung in der Information der Bevölkerung stattfinden. Im Rahmen einer Erhebung wurde festgestellt, dass die Bereitschaft und ein Interesse an Themen zur Selbsthilfe und zur Notfallvorsorge auf Seiten der Bevölkerung durchaus vorhanden sind.

Die Studie kommt daher zum Schluss, dass Politik, Verwaltung und die mit Aufgaben des Katastrophenschutzes beauftragten Organisationen in der Bevölkerung das Bewusstsein für die Notwendigkeit privater Notfallvorsorge fördern müssen. Derzeit verlassen sich zu viele Menschen ausschließlich auf die öffentliche Hilfe von Hilfsorganisationen oder staatlichen Stellen, anstatt entsprechende Eigenverantwortung und Eigenvorsorge zu übernehmen.

Die Menschen sind heute an ihre komfortablen Lebensumstände so gewöhnt, dass sie nicht darüber nachdenken bzw. sich einen anderen Zustand gar nicht vorstellen können oder wollen. Ständig vorhandene Gefahren wie ein teilweiser bis gänzlicher Ausfall unserer gewohnten Infrastruktur im tiefsten Frieden, werden nicht wahrgenommen, oder aus dem Denken ausgeblendet.

Zusammenfassung

Ziel ist die Sensibilisierung der Bevölkerung hinsichtlich der Bedeutung eines möglichen zeitlichen Verlustes der für die Gesellschaft selbstverständlichen, da bisher weitgehend ständig

vorhandenen, lebenswichtigen Ressource Strom. Dabei sollen auch die großen Abhängigkeiten vom Strom, die steigende Komplexität und die damit einhergehende Verwundbarkeit, vor Augen geführt werden.

In den vergangenen Monaten konnte eine stetig steigende Anzahl von Meldungen zu möglichen, bevorstehenden Blackouts in Europa beobachtet werden. Es besteht durchaus die Möglichkeit, dass dieses Thema auch dazu genutzt wird, um mehr Ressourcen zu lukrieren, etwa für den Netzausbau. Nichtsdestotrotz sind die derzeit stattfindenden, kritischen Veränderungen in der bestehenden Strominfrastruktur nicht wegzuleugnen. Die Folgen sind gegenwärtig noch nicht absehbar, jedoch bergen diese konkrete Risiken für größere Netzausfälle in sich. Es ist daher eine steigende Anzahl von (Teil)Blackouts zu erwarten. Dies inkludiert, dass die Netzbetreiber in kritischen Situationen Teilbereiche des Netzes abschalten können, um das Gesamtnetz wieder zu stabilisieren.

Die Vorbereitungen auf ein Blackout sind in Österreich, wie auch in vielen anderen europäischen Ländern, nicht zentral organisiert. Nach wie vor gehen viele Verantwortungsträger der Politik, der Behörden und der Wirtschaft davon aus, dass es zu keinem lang andauernden und überregionalen Stromausfall kommen wird. Dabei sind ihnen weitgehend weder die Komplexität eines solchen Stromausfalles noch die wechselwirksamen Abhängigkeiten der Infrastrukturen bekannt oder tatsächlich bewusst. Vor allem die Bevölkerung in urbanen Gebieten ist auf ein solches Szenario nicht vorbereitet: Weder Selbstschutz- noch Selbsthilfepotenziale sind in nennenswertem Umfang vorhanden.

Grundsätzlich bedarf es eines nachhaltigen Risiko- und Krisenmanagements, das die Prävention in den Vordergrund stellt. Sowohl die Risikosteuerung als auch das Krisenmanagement müssen von einer sektoralen Betrachtung zu einer prozessualen und ganzheitlichen Betrachtung führen. Der Fokus auf Einzelsysteme führt in die Sackgasse.

Zu beobachten ist auch, dass Verantwortliche von unrealistischen Annahmen ausgehen, was häufig auf die mangelnde Kommunikation zwischen diesen zurückzuführen ist. Risiko- und Krisenmanagement müssen nach standardisierten Regeln ablaufen und regelmäßig geübt werden. Nur so kann das Zusammenspiel aller erforderlichen Akteure gefestigt und können die erforderlichen Lehren daraus rechtzeitig gezogen werden.

Das Blackout ist ein Schlüsselszenario. Es besitzt Wechselwirksamkeiten mit anderen lebenswichtigen Infrastrukturen und hat Auswirkungen auf nahezu alle Lebens- und Geschäftsbereiche. Sollte es zu einem solchen überregionalen und lang anhaltenden Stromausfall kommen, wird dies erhebliche Beeinträchtigungen für die Bevölkerung und enorme volkswirtschaftliche Schäden nach sich ziehen. Die Sicherheit und die Grundversorgung der Bevölkerung könnten von staatlichen Einrichtungen und privaten Hilfsorganisationen nicht mehr aufrechterhalten werden. Ein Stromausfall dieser Größenordnung wäre eine nationale Katastrophe mit kurz-, mittel- und langfristigen Schäden für alle Bereiche der Gesellschaft.

Daher ist jeder Einzelne gut beraten, Eigenverantwortung zu übernehmen und Eigenvorsorgemaßnahmen zu treffen. Für die staatlich organisierte Hilfe sind weitere Analysen zu erarbeiten und daraus Konsequenzen zu ziehen. Diese werden auch in einem weiteren Folgebeitrag näher beleuchtet.

Die westlichen Gesellschaften wenden für Maßnahmen zur Erhöhung der allgemeinen Sicherheit viel Geld auf wie z. B. zum Schutz vor Terrorismus. Vergleicht man diese Szenarien, dann steht der Aufwand für den Terrorschutz in keinem Verhältnis zum Schutz vor einem Blackout. Jeder einzelne Betroffene eines möglichen Terroranschlages ist zu viel, aber im Vergleich zur Anzahl der Betroffenen und den Schäden eines Blackouts, wird dieser Bereich

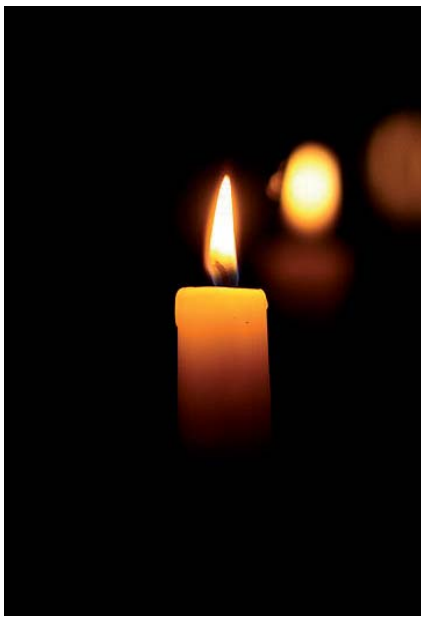


Foto: Fotolia.com

Vorsorge mit Kerzen allein wird nicht reichen.

derzeit noch sträflich vernachlässigt. Es sollte nicht erst zu einer Katastrophe kommen müssen, um Änderungen herbeizuführen. Daher sind alle Verantwortungsträger auf allen Ebenen aufgefordert, sich mit diesem Katastrophenszenario auseinanderzusetzen. Das Eintreten eines Blackouts nach mangelhafter Vorbereitung auf dessen Bewältigung würde einen massiven Vertrauensverlust in die verantwortlichen Stellen nach sich ziehen.

Im nächsten TD-Heft wird eine Lageentwicklung nach einem über 24 Stunden hinaus anhaltenden Blackout detailliert analysiert. Eine Betrachtung von möglichen Cyber Angriffen auf die Strominfrastruktur und mögliche Lösungsansätze für das Krisen- und Katastrophenschutzmanagement werden die Beitragsserie abschließen.

(wird fortgesetzt)

Mag. Udo Ladinig, Herbert Saurugg,
Cyber Security Austria

Selbsthilfe

Wichtige Informationen rund um das Thema Eigenvorsorge stellen der Österreichische Zivilschutzverband (ÖZSV) www.zivilschutzverband.at bzw. die Sicherheitsinformationszentren http://www.siz.cc/ zur Verfügung. Weiterführende Informationen bietet das deutsche Bundesamt für Bevölkerungsschutz und Katastrophenhilfe www.bbk.bund.de an.