Verwundbarkeit und Resilienz digitaler Energiesysteme

Oder: Warum Notstromstrategien auf Basis erneuerbarer Energien überlebenswichtig sein können

Ausschusssitzung WiEnBe
Berliner Abgeordnetenhaus, 2.3.2020

Prof. Dr. Bernd Hirschl
IÖW – Institut für ökologische Wirtschaftsforschung, Berlin
und
BTU Cottbus-Senftenberg

Kurzvorstellung
Prof. Dr. phil. Dipl-Ing-Oec. Bernd Hirschl

- **Leiter der Abteilung Nachhaltige Energiewirtschaft und Klimaschutz am Institut für ökologische Wirtschaftsforschung IÖW (GmbH, gemeinnützig), Berlin**

  i | ö | w

  - seit 1985 Forschung und Politikberatung für nachhaltiges Wirtschaften
  - Standorte Berlin und Heidelberg, über 60 Mitarbeiter/innen aus Wirtschafts- und Sozial-, Ingenieur- und Naturwissenschaften
  - Langjährige Erfahrungen in der Analyse, Entwicklung und Bewertung von Innovationen und Märkten sowie politischen Instrumenten und Klimaschutzstrategien
  - Unabhängig, 100% durch Drittmittel finanziert; überwiegend öffentliche Auftraggeber
  - www.ioew.de

- **Leiter Fachgebiet Management regionaler Energieversorgungssysteme an der Brandenburgischen Technischen Universität (BTU) Cottbus-Senftenberg (Lausitz)**

  b-tu

  - https://www.b-tu.de/fg-energieversorgungsstrukturen

- **Ausgewählte Funktionen**
  - Mitarbeit im Akademienprojekt Energiesysteme der Zukunft ESYS, u.a. AG Resilienz digitaler Energiesysteme, AG De/Zentrales Energiesystem
  - Sprecher des Berliner Klimaschutzrates

Megatrends Digitalisierung und Elektrifizierung

Oder: Das digitale Stromsystem wird zur Leit-Infrastruktur

- **Die Megatrends Digitalisierung und Elektrifizierung wachsen immer mehr zusammen**
  - Digitalisierung findet (seit Jahren) in allen Sektoren statt – auch im Stromsystem
  - Elektrifizierung findet (seit Jahrzehnten) in allen Sektoren/ Infrastrukturen statt
  - Stromwende/ Energiewende braucht verstärkt Digitalisierung (enabling technology) für effiziente Koordination einer Vielzahl von Akteuren, Anlagen und Prozessen (am besten in Echtzeit)
  - Digitalisierung braucht (zunehmend viel) Strom
- **Strom und IKT prägen ALLE anderen Infrastrukturen – auch alle kritischen Infrastrukturen (KRITIS)**

Digitalisierung bringt eine neue Qualität an Blackout-Risiken mit sich

- **„gewöhnliche“ Blackoutgefahren bzw. Ursachen**
  - Lokale Infrastrukturschäden und Hardware-Störungen (durch z.B. Extremwetter, Terroranschläge o.ä.)
    - idR durch N-1 geschützt, Schadensgebiet regional begrenzt, Reparatur möglich
- **Stressoren für die Stabilität des Stromnetzes**
  - Schwankungen durch Erneuerbare Energien (Erzeugung) …
  - … und/oder durch Marknachfrage bzw. Marktdesign (insb. Strombörse, aber auch Regelenergiemärkte, perspektivisch Gleichzeitigkeitseffekte beim Laden von E-Mobilität)
  - Beides idR durch die Marktakteure/ Netzbetreiber gut beherrschbar (verbesserte Prognosegüte, Ausbau Netzkapazität und SDL etc.)
- **Digitalisierung bringt (insbes. durch Hackerangriffe) eine neue Qualität der Verwundbarkeit mit sich, die alle anderen Stressoren deutlich übersteigt**

Quelle: Projekt „Strom-Resilienz“ von IÖW / Uni Bremen

Beispiele von Cyberattacken auf Energieinfrastrukturen (weltweit)

Year	Target	Name of the attack	Consequences	Objective	Attackers
1982	**Explosion of a gas pipeline in Siberia (Russia)**		**Malware introduced into the SCADA managing the pipeline, the explosion was equivalent to 3 tonnes of TNT.**	**Sabotage**	**External**
1992	warning system at Chevron, (USA)		discovered when an accident took place at the Chevron refinery in Richmond, during which thousands of people living nearby were exposed to toxic substances for about 10 hours.	Sabotage	Internal
1999	Gazprom, (Russia)		Takeover of the distribution panel controlling gas flows through pipelines.	Sabotage	Internal
1999	Gas pipeline in Bellingham (USA)		This accident was linked to the development of a database for the SCADA system operating the pipelines of the Olympic Pipe Line company. The accident was partly responsible for the spillage of oil causing three deaths and several injuries.	Accident/ human error	Internal
2001	Electricity operator California, (USA)		The attackers had access to one of the internal networks of the California Independent System operator. The attack only affected the PLC network of the company before being discovered.	Sabotage	External/ China?
2003	Davis-Besse Nuclear-power,	Slammer	Shutdown of the parameter display system for four hours due to a worm, with no espionage or sabotage	Not targeted	External
2010	**Natanz, (Iran)**	**Stuxnet**	**Several years of infiltrating the uranium enrichment at Natanz, damaging more than 900 uranium enrichment centrifuges.**	**Sabotage**	**External/ State-sponsored/ USA, Israel?**
2011	Energy industries	Duqu	Parts of code nearly identical to Stuxnet, designed only for industrial espionage, without any destructive function.	Espionage	External
2011	Areva, (France)		Theft of non-critical company data. Infiltration over two years.	Espionage	External
2012	Companies and institutions linked to energy	Flame	Widespread in the Middle East and North Africa, operated for at least two years. Designed for espionage and data analysis. Discovered after Iran's Ministry of Oil and the Iranian National Oil Company had reported theft and the erasure of some important data from their systems.	Espionage/ data theft	External
2012	Saudi Aramco, (Saudi Arabia)	Shamoon	30,000 hard disks destroyed and to be replaced, no impact on the operational network.	Sabotage	External
2013	Bowman Avenue Dam, (USA)		Attackers had taken remote control of a small dam near New York, with no consequences.	Reconnaissance	External/ Iran?
2015	**Electricity operators, (Ukraine)**	**Black Energy**	**30 electricity substations disconnected from the grid, eight provinces without electricity for several hours, more than 200,000 people affected, ICS physically damaged, substations manually operated for several weeks after the event.**	**Sabotage**	**External/ State-sponsored, Russia?**

„Cyber-Abwehrzentrum warnt nach Hacker-Angriffen auf das ukrainische Stromnetz vor Stromausfall in ganz Europa“ (Der Spiegel, 24.08.2018)

Geschätzte Schäden von Cyber-Crime weltweit (2017): 500-600 Mrd. Dollar

Quelle: Gabrielle Desarnaud (2017): Cyber Attacks and Energy Infrastructures: Anticipating Risks, Études de l'Ifri (Institut français des relations internationales), S. 19-20

Beispiele auf Cyber-Attacken auf öffentliche Einrichtungen in D

Hackerattacken

Bundesamt warnt vor Angriffen aufs Stromnetz

Hacker haben 2018 laut einem Bericht vermehrt kritische Infrastruktur angegriffen. Die Bundesregierung will eine Agentur zum Schutz vor Onlineattacken gründen.

17. Februar 2019, 2:16 Uhr / Quelle: ZEIT ONLINE, dpa, ces / 64 Kommentare

Hackerangriffe auf Behörden

Bloß kein Lösegeld zahlen

Stand: 27.02.2020 09:52 Uhr

Das Kammergericht Berlin ist nur per Post, Fax oder Telefon erreichbar - dahinter stecken Hacker. Mehr als 100 Einrichtungen waren im vergangenen Jahr von solchen Angriffen und Erpressungsversuchen betroffen.

Eines der größten Sicherheitsprobleme (die als nicht 100%-verhinderbar gelten):

der „human factor“

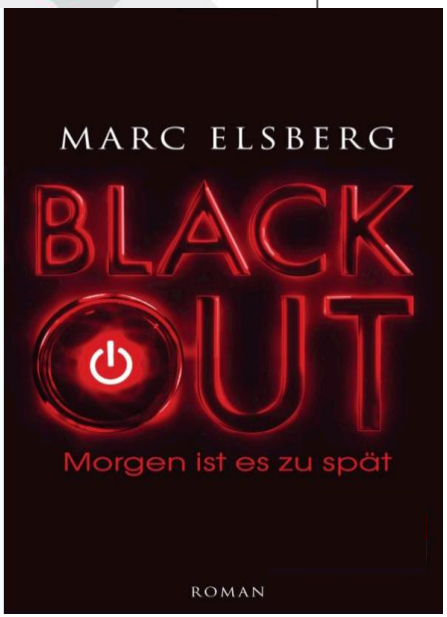
Quellen Screenshots:

Oben: Humbs und Siegmund (rbb), online unter https://www.tagesschau.de/investigativ/kontraste/hackerangriffe-oeffentliche-einrichtungen-101.html (2.3.2020)

Unten: Zeit online, online unter https://www.zeit.de/digital/2019-02/hackerangriffe-infrastruktur-stromnetz-bundesagentur (2.3.2020)

Das größte Risiko: ein langanhaltender, großflächiger Blackout

- **Ein langanhaltender großflächiger Blackout betrifft ALLE anderen Infrastrukturen & KRITIS, für die es nach heutigem Stand nur unzureichende Notversorgungslösungen gibt**
  - Z.B. Krankenhäuser, Trink- und Abwasserversorgung, Nahrungsmittelversorgung, Gewährung von Sicherheit und Schutz wichtiger Einrichtungen und der Bevölkerung etc.
- **Ein langanhaltender großflächiger blackout stellt damit eine gravierende Gefahr für den gesellschaftlichen Zusammenhalt – für die menschliche Zivilisation an sich dar - und ist daher zwingend zu vermeiden**
- **Zwischenfazit**
  - Digitale Energiesysteme sind inhärent verwundbar - und können nicht vollständig geschützt werden
  - Zentrale und dezentrale – digitale - Energiesysteme sind gleichermaßen verwundbar
    - Gründe: zentrale Elemente auch in dezentralen Systemen, human factor etc.
  - ➢ Vor diesem Hintergrund sollte die Erhöhung der Resilienz digitaler Energiesysteme höchste Priorität haben



Quelle: Projekt „Strom-Resilienz“ von IÖW / Uni Bremen

Das Konzept der Resilienz für ein digitales Energiesystem

- **Resilienz ist im allg. definierbar als**
  - „die Fähigkeit eines Systems, seine Funktionsfähigkeit unter Belastungen aufrechtzuerhalten beziehungsweise kurzfristig wiederherzustellen“ (ESYS 2017)
- **Notwendig (aber nicht hinreichend): IT-Sicherheit & Cyber-Abwehr (Prävention)**
  - Akteure: staatliche Behörden, Wirtschaft, Bürger
  - Grundbedingungen: Datenschutz und -sicherheit, Datensouveränität und –sparsamkeit
  - Erforderlich: aktuelle und wirksame Schutzsoftware - und Nutzer, die sie einsetzen (Bildung / Aufklärung), IT-OT-Trennung, …
- **Für den Fall eines großflächigen Blackouts durch Hackerangriffe ist jedoch der Fall zu befürchten, dass eine kurzfristige Wiederherstellung des (heutigen) Gesamtsystems nicht möglich ist**
- **Vorhandene Notversorgungssysteme reichen – je nach KRITIS – für wenige Stunden oder Tage (idR Dieselaggregate)**

➢ **im Krisenfall ist eine lokale/ regionale (Mindest-)Versorgung unabhängig vom übergeordneten Netz zu gewährleisten! (Inselnetzfähigkeit)**

Lösungsansätze für Resilienz eines digitalen Stromsystems

- **dezentralen Ausbau Erneuerbarer Energien in allen Regionen / Verteilnetzen konsequent vorantreiben (nicht: „günstigste“ Standorte)**
  - mehr Regionalstrommodelle, (gemeinschaftlichen) Eigenverbrauch, Zellulare Ansätze, … als Ausschreibungen
- **Eher kurz- als mittelfristig EE-Mindestversorgung in allen Städten / Kommunen / Verteilnetzen sicherstellen**
  - Insb. PV-Anlagen mit ausreichend Speicherkapazitäten, Stadt-Umland-Konzepte (Verteilnetzkopplung bzw. -Rekonfiguration)
  - Im Krisenfall vorrangig KRITIS-Versorgung
  - Lokale / Zellulare „Inselnetzfähigkeit“ im Schwarzfall (Blackout)
- **Nicht alles muss „durchdigitalisiert“ werden**
  - Weniger ist mehr, z.B. Steuerung per Netzfrequenz statt digitaler Datenimpulse
- **Resilienz als zusätzliches (ökonomisches!) Argument für massiven dezentralen EE-Ausbau**
  - Zusätzlich zu: Klimaschutz, lokaler Wertschöpfung, Akzeptanz, …

Fazit

- **Das digitale Energiesystem ist janusköpfig: Chance&Lösung sowie lebensbedrohliches Risiko&Gefahr zugleich.**
- **Die Digitalisierung führt zu größerer Blackoutgefahr als alle anderen Herausforderungen. Die Gefahr eines langanhaltenden Blackouts wird real – und ist zwingend zu vermeiden**
- **Dezentrale Energiesysteme auf Basis erneuerbarer Energien (inkl. lokaler Speicher und Flexibilität) sind zwar ähnlich verwundbar wie zentrale – bieten aber voraussichtlich deutliche Vorteile bzgl. einer inselnetzfähigen Notstromversorgung**
- **Diese muss aber technisch-konzeptionell umgesetzt werden (z.B. vorrangige KRITIS-Versorgung). Dafür braucht es einen Rahmen, genauso wie für den konsequenten dezentralen EE-Ausbau in JEDEM Verteilnetz. Die ökonomische und gesellschaftliche Bewertung/ Wertschätzung der Resilienz kann hierbei helfen**
- **Anregung: Berliner Pilotprojekte starten: „EE-basierte Notstromkonzepte für KRITIS“**

Vielen Dank.

Prof. Dr. Bernd Hirschl
IÖW – Institut für ökologische Wirtschaftsforschung, Berlin
und
BTU Cottbus-Senftenberg

2.3.2020