swissgrid

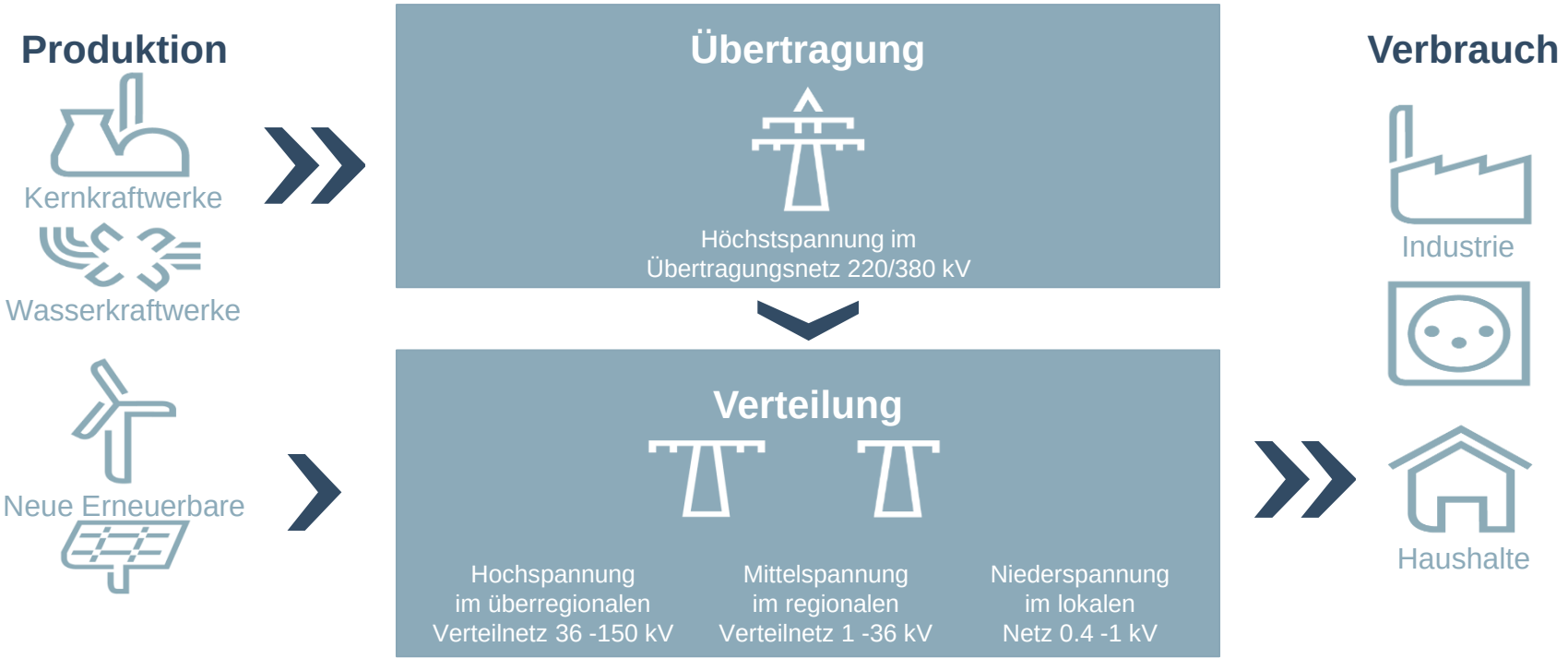
Cyberrisiken bei kritischen Infrastrukturen

Herausforderungen für einen Netzbetreiber

Rainer Mühlberger, CIO
Mitglied der Geschäftsleitung

Swissgrid - Bindeglied zwischen Produktion und Verbrauch

swissgrid



Netzeigentümerin mit umfassender Verantwortung

swissgrid

12000

Strommasten in der ganzen Schweiz

6700

km Netzlänge des Schweizer Übertragungsnetzes

12000

Inspektionen pro Jahr

650

km notwendige Netzmodernisierung und Netzausbau

2.5 CHF

Mrd. CHF Investitionskosten für Erweiterung und Erhalt des Übertragungsnetzes bis ins Jahr 2025

141

Schaltanlagen

41

Grenzleitungen

7

Standorte und Stützpunkte in allen Regionen der Schweiz

365

Tage im Einsatz rund um die Uhr

BBC | Sign in | News | Sport | Weather | Shop | Earth | Travel

NEWS

Home | Video | World | UK | Business | Tech | Science | Stories | Entertainment & Arts

Technology

Ukraine power cut 'was cyber-attack'

11 January 2017 Share

CBS News / CBS Evening News / CBS This Morning / 48 Hours / 60 Minutes / Sunday Morning / Face The

CBS THIS MORNING Today's Rundown | Politics & Power

CBS NEWS | June 23, 2017, 12:48 PM

Was Russian hacking of Ukraine's power grid a test run for U.S. attack?

Share / Tweet / Reddit / Flipboard / Email

In its July cover story, Wired magazine takes an in-depth look at a years-long

Die Bedrohung ist real: Stromausfall durch Cyberangriff in der Ukraine 2015

swissgrid

Am 23. Dezember 2015 legte ein Hackerangriff sieben Unterwerke in der Ukraine lahm:

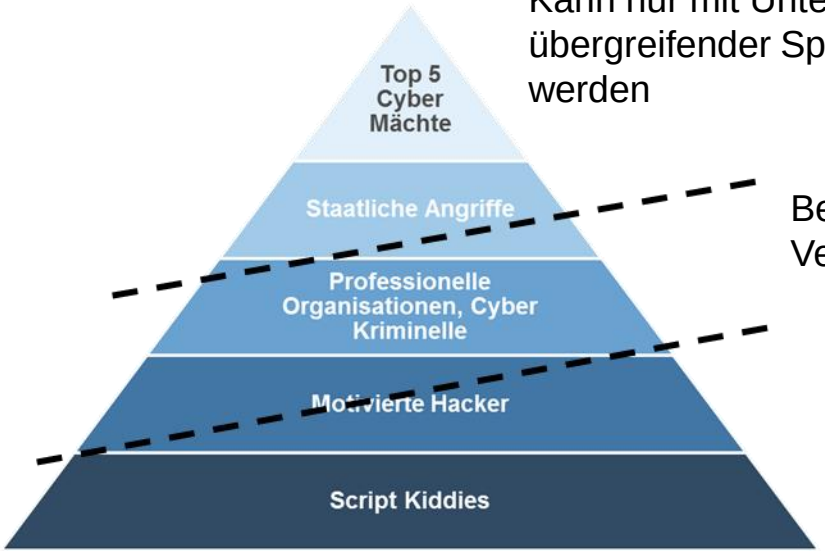
- Rund 225’000 Kunden waren während 3 Stunden ohne Stromversorgung
- Die Angreifer übernahmen die Kontrolle über das Netzleitsystem (SCADA) und schalteten damit einzelne Unterwerke aus
- Die Angreifer verübten gleichzeitig eine DDOS Attacke auf das Call Center, so dass Kunden nicht mehr durchgestellt wurden

Quelle: SANS-ICS / E-ISAC: Analysis of the cyber attack on the ukrainian power grid, March 18, 2016

Ein komplexer Angriff, von langer Hand vorbereitet

1. **Spearphishing** - gezieltes e-mail mit Schadsoftware an Mitarbeiter mit Zugriffsrechten
2. **Credential Theft**: Diebstahl von Benutzername und Passwort
3. **VPN Access:** Zugriff von aussen ins Netzwerk (Remote Access)
4. **Workstation Remote:** Benutzung von Fernzugriffs-Werkzeugen
5. **Control & Operate:** Benutzung des Leitsystems (via HMI)
6. **Tools & Tech:** Veränderung der Firmware auf Operational Technology Systemen und dadurch Abschaltung, Löschung von Disks, Löschung von Log-Files, Denial-of-Service Attacke auf Telefonsystem

Ein vollständiger Schutz ist nicht möglich



Kann nur mit Unterstützung staatlicher Stellen und übergreifender Spezialistenteams (CERT) abgedeckt werden

Bereich, in dem viele Unternehmen Verbesserungsbedarf haben

Wird durch Unternehmen heute zu einem grossen Teil gut beherrscht

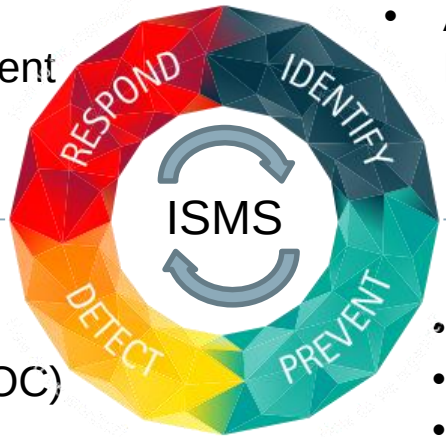
Die Antwort: Sicherheit als integraler Ansatz

- **Identify**: Risikobasierte Erkennung des Handlungsbedarfs
- **Prevent:** Grundschutz, risikobasierte Erweiterung
- **Detect:** Erkennen von Angriffen
- **Respond:** Reagieren, überbrücken und wiederherstellen

Detect und Respond rücken in den Vordergrund

- Computer Emergency Response Team (CERT)
- Business Continuity Management (BCM)
- Krisenübungen

- Risikomanagement Prozesse
- Ausbildung und Zertifizierung der Mitarbeiter



- Security Operations Center (SOC)
- Protocol Analyzer im Netzwerk
- Log-File Analysen

- Benutzerzugang mit 2-Faktoren
- Netzwerksegementierung
- Firewalls und andere Schutzssysteme
- Patch -/ und Vulnerability Management Systeme

Handlungsbedarf bei den Rahmenbedingungen

Handlungsfelder

- Verpflichtung zu minimalem Grundschutz
- Meldepflicht bei Sicherheitsvorfällen
- Klare gesetzliche Grundlage für Personen-sicherheitsprüfungen
- Ausreichendes staatliches Dispositiv zur Unterstützung bei Erkennung und Abwehr von Angriffen
- Verstärkte Zusammenarbeit der Stakeholder national und international