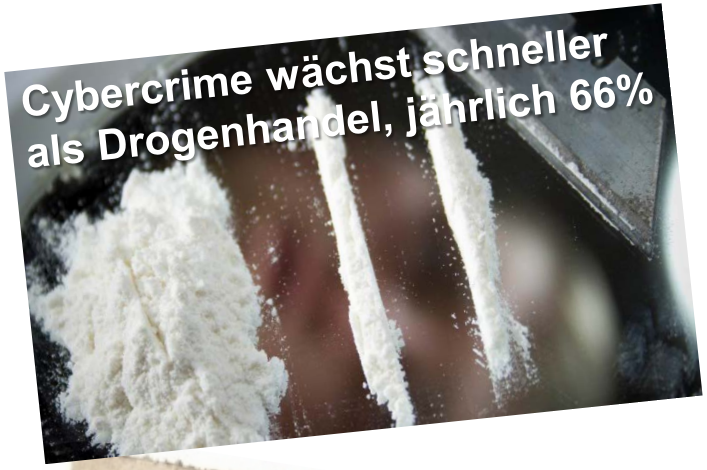
oesterreichs energie.

# Sicherheit in der E-Wirtschaft

Handlungsempfehlungen und erste Ergebnisse des Cyber-Security-Projekts

28.04.2014, Wien

# Bedrohungslage



Mobil E-Paper Apps Abo Club Immobilien Jobs & Karriere Schaufenster

Die Presse.com › Wirtschaft › National

POLITIK WIRTSCHAFT GELD PANORAMA KULTUR TECH SPORT MOTOR LEBEN BILDUNG ZEITR

Österreich International Wirtschaftsrecht Energie Kolumnen Management & Karriere Wirtschaft Unplugged

« zurück

## Stromnetz außer Kontrolle

08.05.2013 | 10:45 | MATTHIAS AUER (Die Presse)

**Hackerangriff oder Softwarefehler? Eine Computerpanne hat das Steuerungssystem der heimischen Stromnetze am Wochenende lahmgelegt – und niemand hat es bemerkt.**

Bild vergrößern

Drucken

Versenden

**Wien.** Eigentlich war der vergangene Freitag ein beschaulicher Tag für Österreichs Strombranche. Die Kraftwerke produzierten weder zu viel noch zu wenig Elektrizität, der Verbrauch war konstant. Kein Grund zur Aufregung also. Bis Freitagmittag. Dann war es mit der Ruhe nämlich vorbei. Wie aus dem Nichts prasselte eine Flut von Messdaten aus dem Süden des Landes auf die Steuerungszentralen des Übertragungsnetzbetreibers APG ein. Nun war Panik angesagt. Denn Aufgabe des Unternehmens ist es, dafür zu sorgen, dass das sensible Gleichgewicht im Stromnetz erhalten bleibt. Und das ist schwierig, wenn aus einzelnen Bundesländern so viel Datenmüll kommt, dass die APG ihren direkten Draht zu den lokalen Stromnetzbetreibern verliert.

DIE WELT

Home Politik Wirtschaft Geld Sport Wissen Panorama Feuilleton ICON Reise Motor Regional Meinung Videos Markt

## Russische Hacker attackieren Stromnetzbetreiber

50 Hertz betreibt und überwacht die Stromnetze in Berlin, Hamburg und großen Teilen Ostdeutschlands. Das Unternehmen sieht sich Angriffen aus Osteuropa und Russland ausgesetzt. Von Benedikt Fuest

Artikel empfehlen: E-Mail Twitern

Das Kontrollzentrum von 50 Hertz in Neuenhagen bei Berlin. Es ist nicht unmittelbar von den Hacker-Attacken betroffen Foto: dpa

MEISTGELESENE ARTIKEL

1. Rürup-Studie Deutschland unmittelbar vor dem Wohlstandsknick
2. Cum-ex-Geschäfte "Wie eine Goldgrube. Jeder hat mitgemacht"
3. Selbstständigkeit "Quick and dirty" – eine neue Art des Geldverdienens
4. Telefonat mit Merkel Putin sieht die Ukraine am Rande eines Bürgerkriegs
5. Globalisierung Onlineshopper verstopfen Deutschlands Zollämter

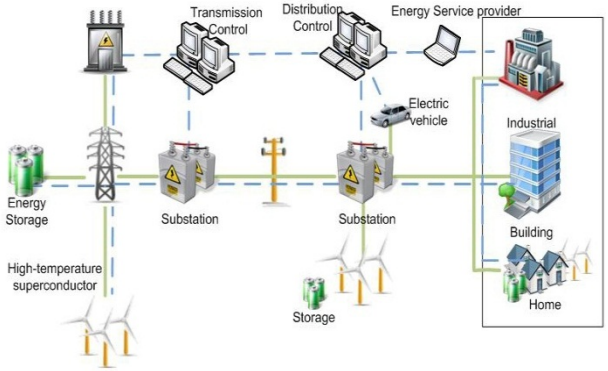
MEISTGELESEN AUF THE WALL STREET JOURNAL

1. China verliert die Lust auf Gold
2. Heartbleed: SPD will Open-Source-Sicherheit s...

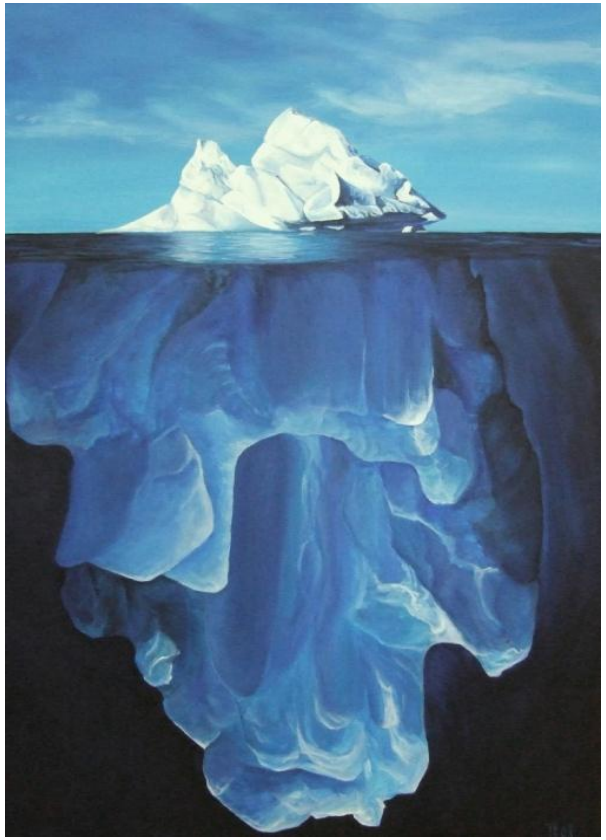
# IKT ist Schlüsseltechnologie für viele Branchen – auch für die Energiewirtschaft!

- Ein breites Umfeld an Komponenten & Systemen
- Erhöhter Integrations- und Kommunikationsbedarf im Stromnetz der Zukunft
- Massiver Anstieg der Vernetzung und der Komplexität

**In Zukunft:**



# Sicherheitsbewußtsein hoch, aber neue Risken



- Sicherheit ist und war lange vor der Liberalisierung ein Thema
  - Versorgungssicherheit
  - Arbeitssicherheit, Unfallverhütung
  - Objektschutz, Zugangsbeschränkungen
  - Kommunikationssicherheit
- IKT Energiesysteme massiv in Veränderung
- Standardisierung in Etablierung
- Permanente Veränderungen bei Risken und Sicherheitstechnologien

**→ Risikomanagement**

# Wie viel Security braucht die Energiewirtschaft

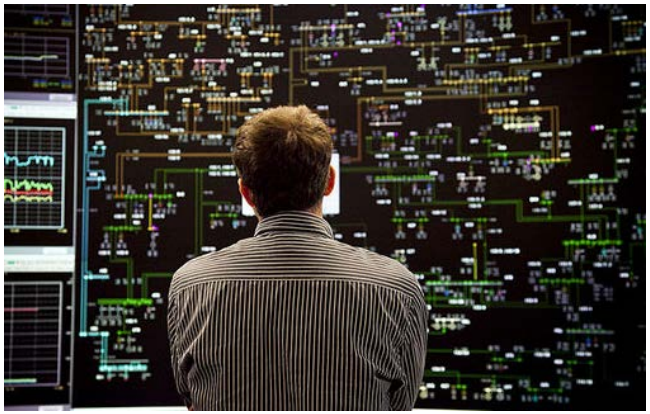
- Entscheidend dafür sind u.a.:
  - Gesetze und Regulierung
  - Technologische Entwicklungen
  - Bedrohungslage und Risikoanalyse
- Zertifizierungen führen nicht automatisch zu notwendigem Sicherheitsniveau
- Internationale Normen und Standards nur als Orientierungshilfe
- Etablierung von Branchenstandards für einheitliches Sicherheitsniveau

# Kritische Erfolgsfaktoren sichere Energie

- Awareness auf allen organisatorischen Ebenen (vom Vorstand bis zum Mitarbeiter)
- Management Commitment für Informationssicherheit
- Organisatorische Strukturen und etabliertes Risikomanagement
- Bedachtsamer Einsatz von neuen Technologien
- Wirksamer Prozess im Krisenfall
- Unternehmens- und länderübergreifende Zusammenarbeit

- Bereitstellung der Ressourcen (Budget, Mitarbeiter,…)

# Risikoanalyse



- Projekt Risikoanalyse 2013
- Inhalt: Betrachtung der relevanten IKT-Systeme und -bereiche der Energiewirtschaft zur Sicherstellung der Versorgungssicherheit
- Aktive Teilnahme von
  - Ministerien
  - ECA
  - Oesterreichs Energie (OE)

# Risikoanalyse Ergebnisse

- 73 Einzelrisiken identifiziert
  - Von Experten in Arbeitsrunden analysiert und erfasst
- Zusammengefasst in sieben Risiko-Cluster:
  - Eskalation und Kommunikation
  - Design und Architektur
  - Human Factor
  - Organisatorische Sicherheit
  - Hardware und Software
  - Normung und Recht
  - Zugriffskontrolle und Kryptographie

# Risikoanalyse Umsetzung

- Projektstruktur bleibt erhalten
  - Lenkungsgremium
  - Arbeitsgruppe
- Koordination bei Oesterreichs Energie
  - Bearbeitung der Handlungsempfehlungen
- Prozesseigner zugeordnet
- Prioritäten vergeben
- Themenbereiche sind durch Fachgremien von Oesterreichs Energie abgedeckt

# Etablierte Aktivitäten

- Eigene unabhängige IKT-Infrastruktur (im und zwischen den Unternehmen, bevorzugt leitungsgebunden):
  - Getrennt von öffentlichen Netzen (wenige Übergangspunkte)
  - Weitgehend unabhängig von anderen Kommunikationsflüssen, Bedrohungen, Ausfällen
  - Intern strikte Trennung zwischen Systemen für die Betriebsführung und denen der Bürokommunikation
- Analyse von Kommunikationstechnologien für Krisensituationen
- Best Practice-Paper zum BDEW-Whitepaper: „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ erstellt
- Unternehmensübergreifende Übung zur betrieblichen Kommunikation (IKT-Planspiel)

# Etablierte Aktivitäten

- Aktives Monitoring, dadurch frühzeitige Erkennung
- Etabliertes Risikomanagement
- Awareness und Schulung Mitarbeiter, Lieferanten, Hersteller

- Sorgfältig geplanter und risikogeprüfter Einsatz neuer Technologien
  - Security by Design Ansatz
  - Verifikation in begrenzten Pilotinstallationen

- Internationale Vernetzung in der Branche
  - Sektor
  - Sektor und Hersteller
  - Standardisierungsgremien

# Fazit

- Sicherheit ist
  - Unbequem (teilweiser Komfortverlust)
  - Benötigt Ressourcen (personell und finanziell)
  - Kein Projekt sondern ein Prozess
- ABER: Ein Unfall/Hackangriff ist noch unbequemer, verschlingt weit aus mehr Ressourcen und bedeutet einen immensen Image-Verlust
- Die Energiewirtschaft investiert daher in hohe Sicherheitsstandards um für die Anforderungen aus der Digitalisierung in der Energiewirtschaft bestmöglich gerüstet zu sein

oesterreichs energie.

# Danke für Ihre Aufmerksamkeit.

**DI Dr. Peter Layr**
Präsident Oesterreichs Energie
Brahmsplatz 3, 1040 Wien

Tel +43 1 501 98-0
info@oesterreichsenergie.at