

30.09.2024

NIS2-Gesetz und zukünftige Cybersecurity-Herausforderungen

Die Bedrohungslandschaft im Cyberspace (exemplarischer Auszug)



Menü **Süddeutsche Zeitung** [Jetzt abonnieren](#) [Login](#)

keine SZ | SZ Plus | Nahost | Ukraine | Oktoberfest | Politik | **Wirtschaft** | Meinung | Panorama | Sport | München | Kultur | Me: >

Home > Wirtschaft > IT-Sicherheit > 10 Jahre Stuxnet: Der Hack, den die Welt hörte

Zehn Jahre Stuxnet

Der Hack, der die Welt aufschreckte

8. Juli 2020, 9:10 Uhr | Leszeit: 5 Min.



Der damalige iranische Präsident Mahmud Ahmadinedschad besucht 2007 die Urananreicherungsanlage in Natans. 2009/2010 zerstörte der Cybersabotage-Angriff Stuxnet einen Teil der Zentrifugen der Anlage. (Foto: dpa)

Vor etwas mehr als zehn Jahren wurde eine iranische Atomanlage gehackt, mit der bis dato gefährlichsten Cyberwaffe der Welt. Der Hack gilt als geheimdienstliches Meisterwerk - und ist bis heute nicht völlig aufgeklärt.

~2010

Stuxnet: Malware, um Industriesteuerung im Iran zu manipulieren

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY [Menu](#)

America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

[Home](#) / [News & Events](#) / [Cybersecurity Advisories](#) / [ICS Alert](#) **SHARE:** [f](#) [x](#) [in](#) [e](#)

ICS ALERT

Cyber-Attack Against Ukrainian Critical Infrastructure

Last Revised: July 20, 2021 **Alert Code:** IR-ALERT-H-16-056-01

Description

On December 23, 2015, Ukrainian power companies experienced unscheduled power outages impacting a large number of customers in Ukraine. This report provides an account of the events that took place based on interviews with company personnel.

Updated July 20, 2021: The U.S. Government attributes this activity to Russian nation-state cyber actors and assess that Russian nation-state cyber actors conducted a cyber campaign against Ukrainian critical infrastructure. For more information on Russian malicious cyber activity, refer to us-cert.cisa.gov/Russia.

2015

Sandworm: weltweit erster großer Stromausfall durch Hackerangriff

CNN Politics [Watch](#) [Listen](#) [Live TV](#) [Sign In](#)

What we know about the pipeline ransomware attack: How it happened, who is responsible and more

By Zachary Cohen, Geneva Sands and Matt Egan, CNN
9 minute read · Updated 4:45 PM EDT, Mon May 10, 2021



2021

Ransomware-Angriff auf Systeme zur Rechnungslegung mit Auswirkungen auf die Gesellschaft

**Bitte was funktioniert noch
ohne Strom?**



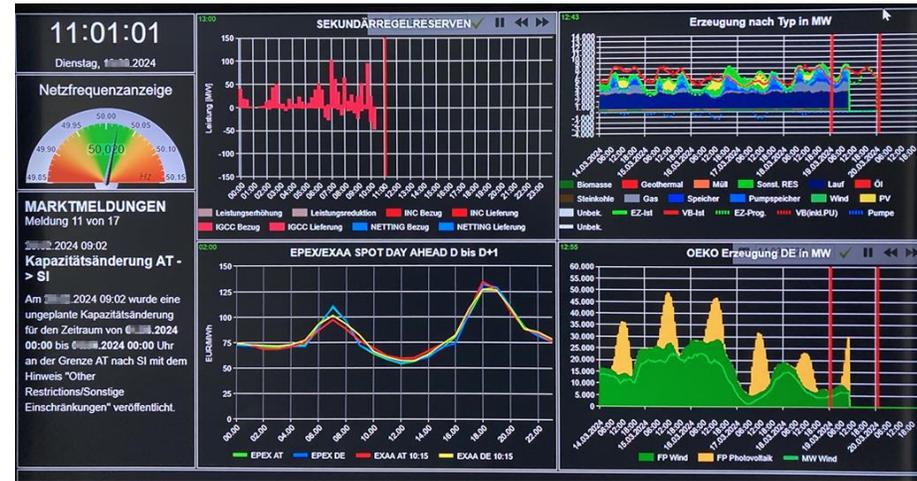
<https://www.youtube.com/watch?v=v-MYtqwxGLA>



Welche Werte müssen wir schützen?



Assets & Daten



Grundlagen der Cybersecurity?



ENISA: Cyber-Hygiene-Praktiken in ganz Europa



1. Verzeichnis aller Hardware

2. Verzeichnis aller **Software** + Sicherstellung aller Updates

3. Verwendung sicherer **Konfigurations-/Härtungsleitfäden** für alle Geräte

4. **Datenverwaltung** IN und AUS dem Netzwerk

5. Alle eingehenden **E-Mails** scannen

6. Minimierung der **administrativen** Konten

7. Regelmäßige **Datensicherungen** und **Wiederherstellungstests**

8. Erstellen Sie einen **Plan zur Reaktion auf Vorfälle**

9. Durchsetzung ähnlicher **Sicherheitsniveaus** in der gesamten **Lieferkette**

10. **Sicherheitskontrollen** in **Dienstleistungsvereinbarungen** (einschließlich Cloud-Diensten)

<https://www.enisa.europa.eu/publications/cyber-hygiene/>



Pflichten und Sicherheitsmaßnahmen eines Übertragungsnetzbetreibers



Freiwillig (seit 2007)

Gesetzlich (seit 2019)

Ab 2025?



- ▶ Jedes Jahr Überwachungsaudit
- ▶ Jedes 3. Jahr Rezertifizierungsaudit

- ▶ Netz- und Informationssystemsicherheitsgesetz (NISG)
- ▶ alle 3 Jahre Nachweis der Compliance nach NISG an Ministerium (BMI)
- ▶ <https://www.nis.gv.at/>

Cybersecurity-Ausblick für die nächsten 3-5 Jahre und deren Herausforderungen in der Umsetzung



Regulierung

- Steigende gesetzliche Anforderungen (europäisch und national)
- Strategische europäische Neuausrichtung:
 1. "EU action plan for digitalisation the energy system"
 2. Neue Legistik für Daten, AI und Cyber-Domäne (u.a. Data Act, Data Governance Act, AI Act, NIS2, NCCS)



Digitale Transformation

- Chancen & Risiken durch neue Technologien
- Herausforderungen durch ChatGPT, Deep Fakes (Faktor Mensch!)
- Rasante Geschwindigkeit auf mehreren Ebenen → Menschen mitnehmen



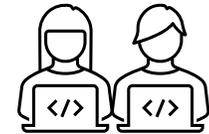
Komplexität

- Zunehmende Komplexität in der gesamten Wertschöpfungskette (stark steigende Vernetzung inkl. Dienstleister und Lieferanten)
- Viele neue gegenseitige Abhängigkeiten
- Übergreifendes Verständnis über Geschäftsprozesse und Abhängigkeiten u.a. von Dritten



Lifecycle

- Ausbau, Instandhaltung und Erneuerung von IT/OT und Betriebsanlagen (Bestand, Erweiterungen, Third/Fourth Parties)
- Organisatorische Entwicklung des Unternehmens

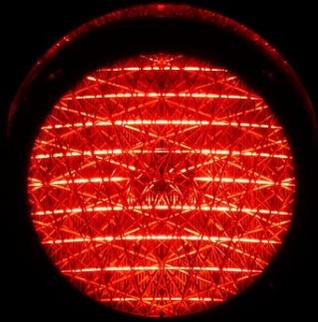


Fachkräfte

- Halten und Ausbilden von Personal (allgemein und speziell IT, OT, Cyber, Data)
- „Upskilling“: Aktive Mitarbeiter:innen-Weiterentwicklung → gesuchtes Personal, Allrounder und Spezialisten, selbst aufbauen

AI .. Artificial Intelligence
 NIS .. Netz- und Informationssystemssicherheit
 NCCS .. Network Code on Cybersecurity

Sicherer Umgang mit unsicheren Situationen



Innehalten



Genau
hinsehen



Nicht
unbedacht
handeln

Cybersecurity – take aways



Ganzheitliches, interdisziplinäres Verständnis fördern – Business-Kontext!



Risikomanagement – Was ist wie wichtig für das Unternehmen? Priorisierung!



Basismaßnahmen umsetzen → Cyber-Hygiene!



Sicherheitsmaßnahmen bei Dienstleistern und Lieferanten berücksichtigen!



Dietmar Mandl

Corporate Development and Organisation
Team Lead Compliance and Organisation
Chief Information Security Officer and Data Protection Officer

dietmar.mandl@apg.at

<https://www.apg.at>

