Gezielte Angriffe auf KRITIS
Internationale Akteure und Ziele

18. März 2021
Kompetenzzentrum Digitale Wasserwirtschaft

Prof. Dr. Christian Dietrich
Institut für Internet-Sicherheit, Westfälische Hochschule
https://www.internet-sicherheit.de
dietrich@internet-sicherheit.de

https://chrisdietri.ch
@wavehackr

ENERGETIC BEAR
(DragonFly, Havex)

ELECTRUM
(Industroyer,
CrashOverride)

Kiev, transmission level
1 hour
Destructive comp
No firmware mod

2005 2010 2015 2017 2020

Stuxnet

Iran
Natanz nuclear facility
Nuclear centrifuges

VOODOO BEAR
(BlackEnergy 3,
Sandworm)

30 substations
230 k affected, 3-6 hours
Destructive (KillDisk)
Malicious firmware

ungefährer Aktionszeitpunkt

Ukraine Dezember 2015

- Initiale Infektion über Spearphishing-Email
  - Attachment, Office-Dokument, Macro-Code
  - 8 Monate vorher
  - IT vs. OT
- Zentrale Elemente des Angriffs
  - Fernsteuerung (Remote Control) via Malware und gegebene Remote Control Facilities
  - “Wiedereinschalten” erschweren
  - Lokale Steuerung nicht mehr möglich, Passwörter geändert
  - Firmware von RS232-zu-Ethernet-Adaptern überschrieben
  - Wiper-Malware gegen SCADA-Systeme
  - USV des Kontrollzentrums abgeschaltet
  - Denial-of-Service-Angriff auf Telefonsupport/Call-Center

Quelle: Ukrainian power grids cyberattack







ENERGETIC BEAR (DragonFly, Havex)

ELECTRUM (Industroyer, CrashOverride)

Kiev, transmission level
1 hour
Destructive comp
No firmware mod

TRITON

Saudi Arabia
No destructive cap
RWX implant only

2005 2010 2015 2017 2020

Stuxnet

Iran
Natanz nuclear facility
Nuclear centrifuges

VOODOO BEAR (BlackEnergy 3, Sandworm)

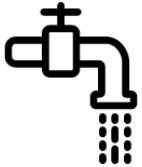
30 substations
230 k affected, 3-6 hours
Destructive (KillDisk)
Malicious firmware

Oldsmar

Oldsmar, USA
No destructive cap
Legitimate remote control








ungefährer Aktionszeitpunkt

Take-aways

Was können wir aus den Vorfällen lernen?

Initiale Infektion

- Spearphishing-Email
  - erwartete Email, mit Anhang oder Link
  - häufig Office-Dokument mit Macro-Code oder Exploit
  - Ukraine 2015, 8 Monate vorher
  - ENERGETIC BEAR

- Abgegriffene oder schwache Zugangsdaten (Credentials)
  - Phishing von Benutzernamen und Passwörtern
  - Mangelnde Segmentierung
  - Ukraine 2015, Lateral Movement
  - evtl. Oldsmar

Quelle: Ukrainian power grids cyberattack, Langner Group, The most important lesson from the Ukraine cyber attack

Angriffsvektoren in OT-ICS

- Remote Access (lesend) vs. Remote Control (lesend und schreibend)
  - Brauchen bemannte Schaltanlagen Fernsteuerungsmöglichkeiten?
  - Wenn ja, dann in abgesicherter Form
  - 2-Faktor-Authentifizierung
  - Freigabe durch lokales Personal

- Firmware-Update-Funktion
  - RS232-auf-Ethernet-Adapter
  - Unbenötigte Funktionen deaktivieren oder Zugriffe regulieren

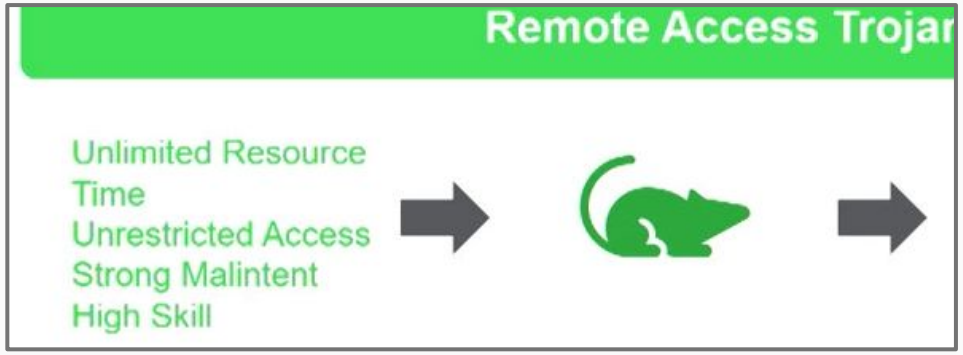
Quelle: Langner Group, The most important lesson from the Ukraine cyber attack

Einordnung

Im ersten Moment wirkt jeder Angreifer haushoch überlegen

Einordnung

- Im ersten Moment wirkt jeder Angreifer haushoch überlegen
- Faktenorientierte Einschätzung



Quelle: TRITON - Schneider Electric Analysis and Disclosure, S4 2018

- Ist jeder Angreifer so gut vorbereitet wie etwa im Ukraine-Vorfall 2015?
  - Triton-Angriff: Nein
  - Oldsmar-Angriff: Nein

Thank you. Questions?

https://armchairinvestigators.de
@wavehackr

Prof. Dr. Christian Dietrich
<dietrich@internet-sicherheit.de>
https://chrisdietri.ch

if(is) internet-sicherheit.

Westfälische Hochschule

Icons made by Freepik from www.flaticon.com