ELKRAFT 2017

POWERBOX – From Power Plant to POL – Cyber-Criminals are on You!

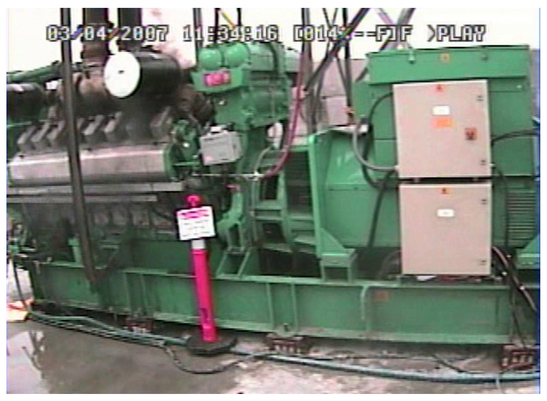
The Threats

→ Hackers & Crackers
→ Computer Criminals
→ Terrorism
→ Cyberwar
→ Industrial Espionage
→ Insiders

The Consequences

→ Population
→ Reputational
→ Infrastructures
→ Regulatory
→ Equipment
→ Data protection and privacy
→ Safety
→ Economic

At start was the Aurora

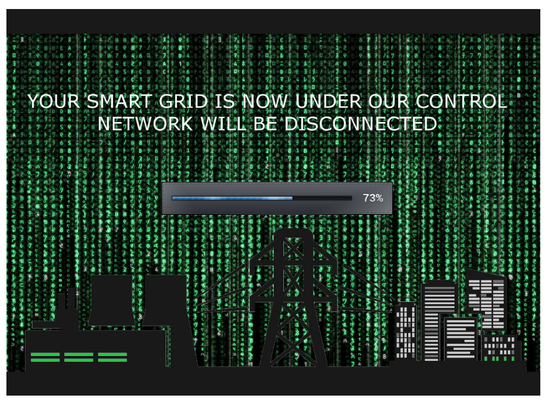


→ 2006 / 2007 The Aurora project
  – Idaho National Lab. accessed a generator
  – Supervisory Control & Data Acquisition (SCADA) used to access and send commands
  – Generator destroyed through simulated “cyber attack”
→ Lessons learned
  – Physical damage can result from a cyber attack
  – Public / Private partnership complicated
  – Lack or regulatory and guidance
  – Discovering a new word of threats
→ Aurora opened the Pandora Box

From simple to complex attacks

→ April 2007
  – Exploit of Microsoft zero-day vulnerability to access energy company SCADA
  – Origin of the attach through simple phishing
  – Taking advantage of windows DNS vulnerability
→ August 2010
  – Mutant of the “Stuxnet” worm propagated through SCADA into Smart Grid
  – Suspected to be the first attack from another government not involving military action

Dark Christmas for Ukraine



→ Direct attacks toward regional distribution system (Ivano-Frankivsk region)
→ 225 000 customers impacted
→ Multiple modus operandi
  – Phishing e-mails - BlackEnergy 3 malware
  – KillDisk attacking Master Boot record
  – Control of Human Machin Interface (HMI)
  – Control of UPSs operation
  – Physical sabotage
→ February 25, 2016 US Dept. of Homeland Security (DHS) issued a formal alert

Ransomware shutdown BWL

→ Michigan - Board of Water & Light (BWL attacked through Ransomware
→ BWL forced to shutdown all IT systems
→ FBI involved in the investigations
→ Several months for BWL to restore
→ Attack suspected to come from another country from cyber-criminal organization
→ This case is considered as part of a mechanism to attack Energy Suppliers

Connecting SG to DDoS

→ September 2016 – OVH (France)
  – Massive Distributed Denial-of-Service DDoS attack through 150 000 IoT devices (CCTV cameras and smart-meters) 1Tbps
→ October 2016 – Dyn (USA)
  – Dyn getting “tens of millions” of messages from Internet-connected devices, including smart-meters
→ November 2016 – Deutsche Telekom
  – More than 900 000 customers knocked offline - Routers infected by a new variant of a computer worm known as Mirai

Securing the Smart Grid

→ The US Department Of Energy (DOE) released a number of projects and initiatives, as well other governmental agencies
→ December 2016 – White House published the “National Electric Grid Security And Resilience Plan”
→ The European Network and Information Security Agency (ENISA), the EU-funded SPARKS (Smart Grid Protection Against Cyber Attacks – project) and many others building safer SG
→ International projects aiming to bridge US and EU into a common protection alliance in discussion

What about at board level?

→ Power community is not used to deal with security
→ Hacker could access a system through industrial SCADA without any problem
→ How much is PMBus secured?
→ Is the power industry too confident?
→ Insider threats are real (Dolphin case)
→ Cyber criminality is increasing faster than we could imagine
→ Power industry must deploy strategies to include highest level of security in any layer of software

Conclusions

→ Smart Grid is a very complex architecture requiring high level of cooperation to protect
→ Learning by mistake is not an option!
→ Governmental initiatives are accelerating though political instability increasing threats at high pace
→ Creating awareness and educating power designers and systems architects business critical
→ In front of Cyber Criminality, nothing is for granted
→ Cyber security starts at board level
→ Sounds dramatic though a lot of fun ahead!

P R
B X
POWERBOX
Mastering Power

For more information
Visit www.prbx.com
Please contact Patrick Le Fèvre, CMCO
+46 (0)158 703 00
marcom@prbx.com