ATTACKS AGAINST ENERGY, WATER AND OTHER CRITICAL INFRASTRUCTURE IN THE EU

ZSOLT BEDERNA

PROF DR ZOLTÁN RAJNAI

DR TAMÁS SZÁDECZKY

ENERGY SECTOR

- Includes electricity, gas, oil
- Highly automatized, centralized, even technologically specific, e.g. GOOSE
- 2010 McAfee / WEU / China
  - Remote administration, data collection from SCADA
  - Hackers attacked individuals and executives outside the EU (in Kazakhstan, Taiwan, and the United States) and in Greece to steal proprietary information.
- 2011 Night Dragon: BP, Shell cyber-espionage
- 2013-2014 Energetic Bear Advanced Persistent Threat (APT) Group: 250 energy grid operators, major electricity generation firms, petroleum pipeline operators, and Energy industry industrial control system equipment manufacturers, cyber-espionage and possible sabotage in WEU/US
- 2015 Ukrainian blackout, Advanced Persistent Threat (APT) attack

WATER SECTOR

- Drinking water supply and distribution sector
- Moderate automation, but potential development
- No EU example
- 2020 April: chlorine overdosage in an Israeli water plant

T R A N S P O R T

- Transport sectors include air, rail, water, and road transportation as subsectors.
- 2017 WannaCry: Bristol airport two days downtime of the information screens, passenger information; Deutsche Bahn passenger information display systems and ticket automats on 470 railways stations were off for several hours in the middle of the weekend traffic
- 2017 NotPetya malware: Maersk, 10 days shutting down several ports and forcing the company to handle 80 per cent of its operations manually.
- 2018 Ryuk ransomware: Port of Barcelona launched emergency procedures
- 2019 Airbus data theft
- 2019 APT10: breach of Airbus’ network via third parties

H E A L T H

- 2017 WannaCry at National Health Service (NHS): ICT unavailable for days resulting in delayed planned operations and rerouted emergency treatment to unaffected hospitals
- 2020 a patient has died after a ransomware attack, exploiting a publicly known and patchable vulnerability, hit a German hospital. She was the first-ever victim of a fatality being linked to a cyberattack

FINANCIAL AND BANKING

- 2012 Sveriges Riksbank suffered from a distributed denial of service (DDoS) attack causing five hours unavailability
- 2014 European Central Bank (ECB) data leakage with 20 000 e-mail addresses and contacts
- 2016 hackers stole $2.5 million from Tesco Bank’s 9 000 customers
- 2017 hackers hit the e-mail account of two board members at the Bank of Italy that resulted in data leakage
- September 2020 hackers, with Russian, Chinese and Vietnamese origination, tried to launch a DDoS attack against Hungarian financial institutions including OTP Bank

DIGITAL INFRASTRUCTURE

- It includes IXPs (Internet Exchange Points), DNS (Domain Name Service) service providers, and TLD (Top-level Domain) name registries
- 2016 Mirai botnet (thingbot), control of 300 000 IoTs, created 623 gigabits per second malicious traffic as peak performance
- September 2020 Magyar Telekom reported ten times higher malicious traffic in its infrastructure

G O V E R N M E N T A L

- 2015 Swedish Transport Authority outsourced IT services to IBM Sweden, which moved data to IBM Czech Republic, while some elements were managed by the Serbian NCR Corporation. Neither of the subcontractors had undergone the Swedish security clearance. The data breach exposed names, photos, and home addresses of millions of Swedish citizens
- 2017-2018 Operation Pawn Storm, aka. APT28 (active since 2004) Informationsverbund Berlin-Bonn network, so German federal chancellery, the German parliament, federal ministries, the Federal Audit Office, and other security entities in Berlin and Bonn. Hackers may have exposed EU-wide information, too.
- 2019 Bulgarian Tax Agency, 4 million citizens' personal data and financial records stolen

S O L U T I O N S

- Identification of operators of Essential Services (OESs)
- OESs shall assess risks on its operation and the cascading effects based on sector-specific requirements
- Proper incident handling and cooperation
- Reason: ineffective patch management and human errors
- Due diligence, compliance and audit
- Cooperation between Member States