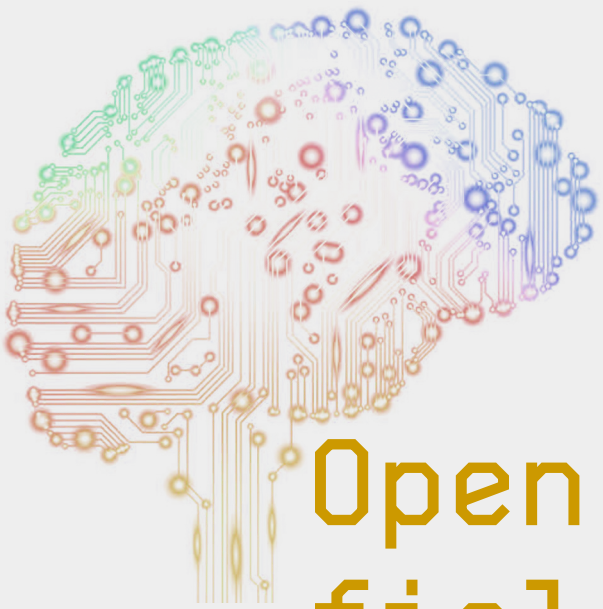


Open Education in field of Cybersecurity

OER - Security and Privacy session

Matej Kovačič

Jožef Stefan Institute

Blaž Ivanc

Elmar d.o.o.

Cybersecurity and Open Education

Cybersecurity is a typical area of expertise where permanent education is not only a need but rather a demand.

Skills and knowledge are quickly becoming obsolete, so they need to be regulary updated.

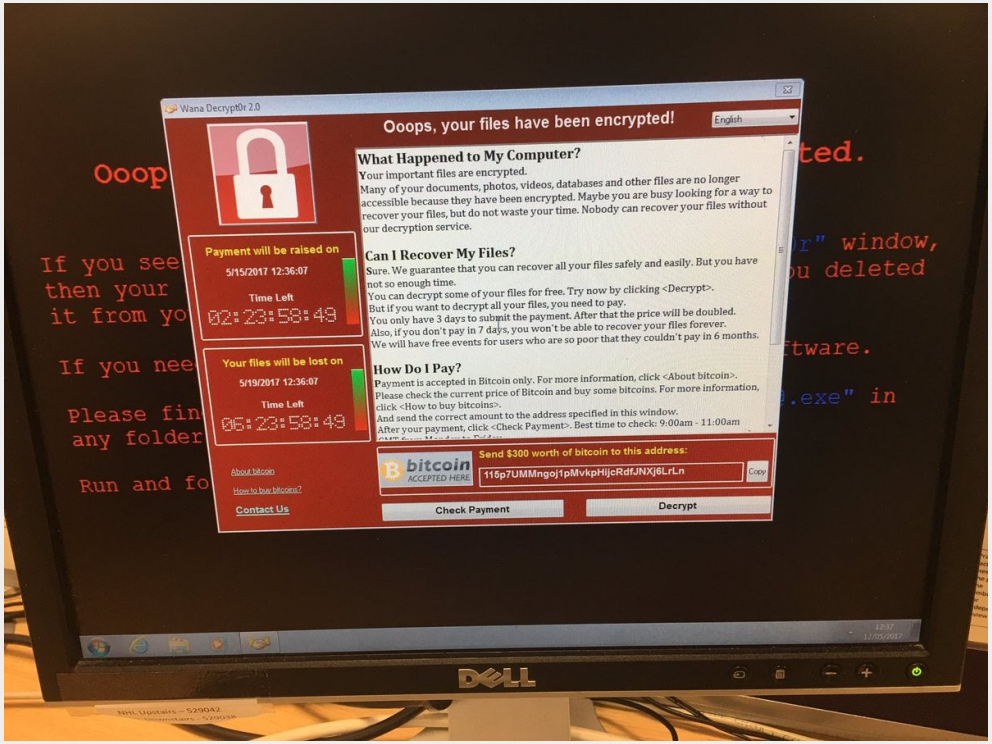
Furthermore, many security researchers in cybersecurity are self-taught, which means information security is a typical area where informal education (or training) is very important.

Cybersecurity and Open Education

Bruce Scheier, one of the leading cybersecurity experts is saying that for learning computer security someone needs to *study* (especially important are self-starter resources), *practice* and *show* his expertise (also, non-formal ways like writing a blog or making podcasts are important).

Since area of cybersecurity has many consequences on society, economy and national security, open and permanent education of experts and end-users is important.

Ransomware



Main targets of ransomware is private business, but in May 2017 a massive ransomware attack has shut down work at 16 hospitals across the United Kingdom. Ransomware authors demanded 300 USD in bitcoin to unlock computers.

Ransomware

WannaCry ransomware used leaked NSA exploits for Microsoft Windows named EternalBlue as attack vector.

NSA discovered EternalBlue vulnerability sometime before 2014, but did not notify Microsoft about it. Instead, they decided to use it by themselves, believing that nobody else would (re)discover it. It is called NOBUS ("*NObody But US*").

WannaCry has shown that hiding vulnerabilities (i. e. knowledge) could harm us all.

Redirecting communications

Due to vulnerabilities in telephone networks (SS7 protocol) it is possible to reroute outgoing and incoming calls and SMS messages.
This could be used to break two-factor authentication.

This vulnerability is in fact not a bug, but a design feature, "embedded" in core phone communication systems. It was discovered by independent security researchers.

Cyberattacks On Energy Sector

Energy sector leads in cyber attacks.

- Irish power grid compromised (EirGrid - Irish electricity transmission system operator), April 2017.
  Installed eavesdropping software / "State sponsored" attack.

- United States (Wolf Creek Nuclear Operating Corporation), May 2017.

- DragonFly 2.0 attack on the electricity grids: United States, Switzerland, Turkey...

Cyberattacks On Energy Sector

Attackers are getting more aggressive.

From information gathering to equipment disruption:

- BlackEnergy malware - crimeware tool (2007)
- BlackEnergy2 malware - modular tool (2010).
- BlackEnergy3 malware - focused on core functionality (2014).
- Havex malware - remote access trojan for ICS (2014), industrial espionage.
- Cyberattack on Ukrainian power grid (2015/2016) - BE for remote access -> power outages.

Sandworm (BE3):

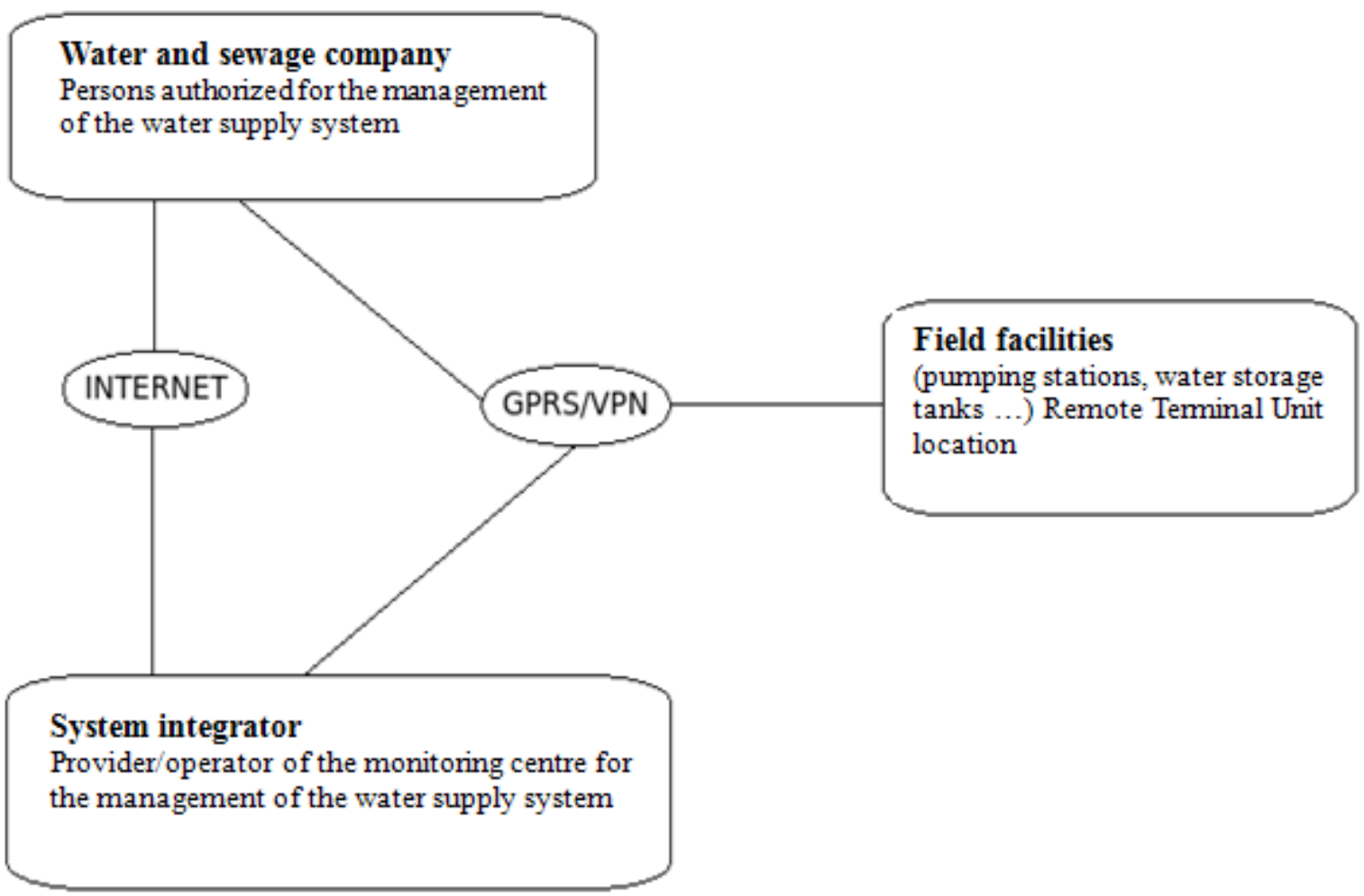
- The use of zero-day vulnerability.
- Access to systems: European Union, NATO, energy sectors.

DragonFly 2.0 (2015 -> 2017):

- Motives: intelligence gathering / sabotage.
- Methods: spear phishing emails / trojanized software / watering hole websites.

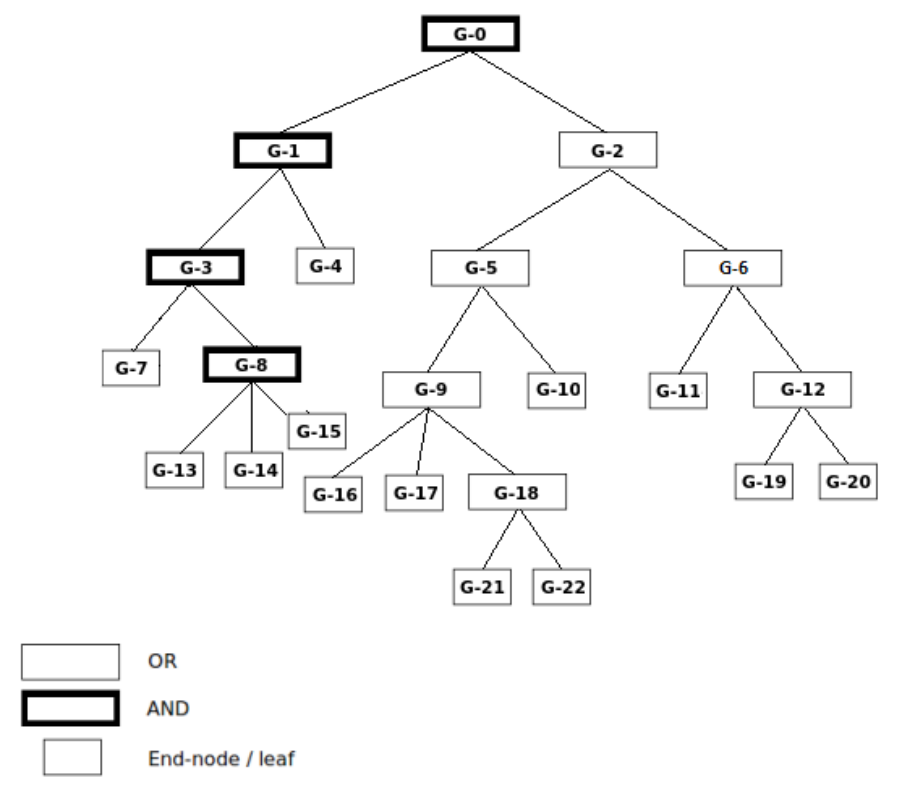
Cyberattacks On Energy Sector

Case Study – Cyber Attack on Critical Infrastructure
(Penetration Test and Cyber Resilience Assessment in 2013)



Cyberattacks On Energy Sector

Analysis:



Node	Description
G-0	Cyber-attacks in critical infrastructure
G-1	Reconnaissance and attack development
G-2	The attack on industrial control systems
G-3	Getting acquainted with the field data
G-4	Development of offensive computer-network operation in the mirrored environment.
G-5	Direct compromising of the industrial control systems
G-6	Attack on the system integrator level
G-7	Acquiring documentation and program files
G-8	Computer network analyses
G-9	Attacks on a field level
G-10	Exploiting the weakness of routine procedures
G-11	Embedding backdoor in IT systems
G-12	Data manipulation
G-13	Capturing data flow traffic
G-14	Data flow emission
G-15	Traffic processing
G-16	Program change in programmable logic controller
G-17	Manipulation on sensor level
G-18	Compromising communication paths
G-19	Remote manipulation through additional users
G-20	Local manipulation of the process database
G-21	Adding communication paths
G-22	Embedding of the MitM attack mechanism

Cyberattacks On Energy Sector

Findings:

The target can often be the system integrator of the industrial control system in the critical infrastructure. This raises the following questions:

- Can the operator of the critical infrastructure prevent concrete information attacks that exploit the system integrator as an entry point?
- Can the operator of the critical infrastructure prevent a security incident resulting from compromising technology on the level of the manufacturer?
- Has the operator of the critical infrastructure considered information attacks originating from compromising higher structures (systems integrator, technology producer) while performing risk assessment and was the operator able to provide concrete security countermeasures?

System supply chain is the appropriate point for compromising, especially in terms of structures that can represent more demanding attack techniques or merely exploit its situation in the required access to the application with simple offensive methods.

Cyberattacks On Energy Sector

Key features of novel cyber-attacks:

The attacks are focused on compromising data integrity with the aim of causing consequences in the physical space.

The attacks reveal new offensive information techniques.

The malicious code dropper can exploit at least one of the unknown software vulnerabilities with the purpose of expanding or raising the privileges.

Autonomous generating of the system specific payload.

Recommendations

Prepare concrete policies, procedures, standards, and guidelines (i. e. gather knowledge and make it available).

Have an understanding of vulnerability management and integrate a cyber intelligence support.

Recognize and defend single point of failure parts.

Have an understanding of security operations concepts.

Provide regular security awareness training for all, including “ordinary” users.

Create ecosystem of knowledge, exchange of experiences and permanent education.

Best practices

We have one infrastructure. ... We get to choose a world where everyone can spy, or a world where no one can spy. We can be secure from everyone, or vulnerable to anyone.

-- Bruce Schneier

And that is why openess, free flow of knowledge and information and continuous education is important.

Discussion...

Matej Kovačič
matej.kovacic@ijs.si

Blaž Ivanc
blaz.ivanc@determinanta.si