GREYCORTEX

The impact from implementing Cybersecurity on Human Resources and Company Assets

Making sense of the cybersecurity jungle

SCADA Security
27. 4. 2023

Let’s get to know each other

Speaker

Audience

- Vertical
- Roles
- Strategy

GREYCORTEX

Today’s agenda

Attacks

Regulations & Security Standards

Defence strategy

Compliance

Where to start?

Myths

GREYCORTEX

Attacks on OT-infrastructure

Ransomware (encryption of files)

Phishing (Installation of Malware)

Social engineering (physical access & installation of Malware)

Regulations and Standards

GREYCORTEX

NIS2

Revision of European NIS Directive from 2016

Framework for protection of network & information systems

Focus on critical infrastructure, operators & service providers

Enhanced reporting requirements

Stronger security requirements (Authentication & Encryption)

Scope:

- Energy Transport, Banking and finance, Health, Water, Digital infrastructure, Digital services

Defence and compliance

1. Realise you run many legacy systems that are hard to protect or to change
2. Know what you are defending (Inventory Management)
3. Monitor what you want to defend (don’t automatically act IPS in OT-applications)
    a. Behaviour Analytics
    b. Custom signatures
4. Respond to attacks (via MSSP or own team(s))
5. Report attacks (timely) to authorities
6. Report attacks to customers

GREYCORTEX

Dealing with legacy systems

Legacy systems (Lifespan 20-30 years)

Vendor support

(nearly) impossible to make changes, focus on future, while using a sensor (IDS)

Looking at the future, what you need, start replacing systems step-by-step over product life cycle.

Where to (re)start?

Do I need a system?

What type of system? NDR/XDR/SIEM/IDS/IPS?

Do I need Threat Intelligence?

- What leads to an actually actionable event
- False positives

Common myths

- Human is the weakest link
- Implementing cybersecurity is expensive
- We can’t have enough threat Intelligence
- OT security specialists are impossible to find

Demo Bohemia Market follow-up