Protecting the energy transition

Elbsides 2024, 13.09.2024

Agenda

1 Introduction & actual situation

2 Legal framework

3 Possible measures

Marc Ratfeld

ISMS Consultant

+49 151 57276870

m.ratfeld@pure-ism.de

CISSP, GCIP

25 years of experience in information security in various roles and industries

Personal Interests:

- *Information Security Management Systems*
- *Vulnerability analysis*
- *Risk management*

Expectations

IT/OT cyber attacks

FBI Disinfects Ubiquiti Routers Exploited by Russian Government Hackers

The Kremlin's notorious 'Fancy Bear' hacking group gained access to the routers by working with another Russian cybercriminal gang, the FBI says.

By Michael Kan February 15, 2024

Malware Discovery Associated with Electric Outages

Russia has developed a cyberweapon that can disrupt power grids, according to new research

Hackers allied with the Russian government have devised a cyberweapon that has the potential to be the most disruptive yet against electric systems that Americans depend on for daily life, according to U.S. researchers.

'CRASH OVERRIDE': THE MALWARE THAT TOOK DOWN A POWER GRID

Cyber firms warn of malware that could cause power outages

INDUSTROYER

eset ENJOY SAFER TECHNOLOGY

DRAGOS

CRASH OVERRIDE

Analysis of the Threat to Electric Grid Operations

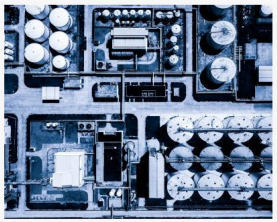
ICS/OT SECURITY | CYBERATTACKS & DATA BREACHES | CYBERSECURITY OPERATIONS | VULNERABILITIES & THREATS

Ransomware, Data Breaches Inundate OT & Industrial Sector

Because of the criticality of remaining operational, industrial companies and utilities are far more likely to pay, attracting even more threat groups and a focus on OT systems.

Robert Lemos, Contributing Writer
December 7, 2023

5 Min Read



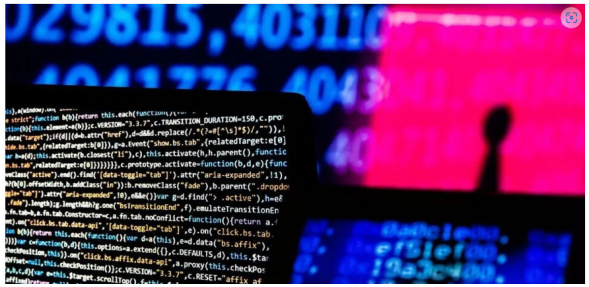
Europe | Cybersecurity

Fulton County and PSI Software SE: A Tale of Two Cyberattacks

The recent cyberattacks on Fulton County and PSI Software SE expose the fragility of digital ecosystems. As critical services are restored and investigations continue, the call for improved cybersecurity measures grows louder.

Justice Nwafor
15 Feb 2024 14:32 EST

Follow Us



Industrial Threats

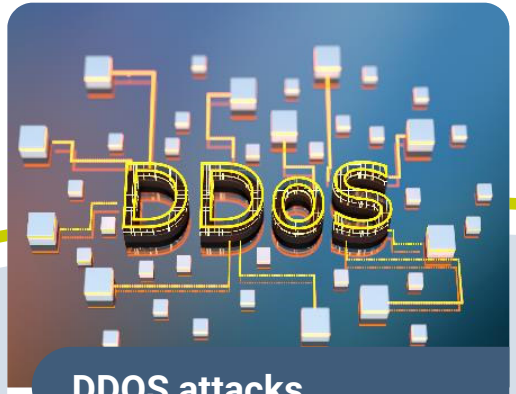
2023 industrial facilities were the focus of 10 threat groups

strongly conflict driven attacks

Intention: sabotage
exfiltration
financially motivated
persistence

Welcome to Hacking Inc.

Examples of current threats

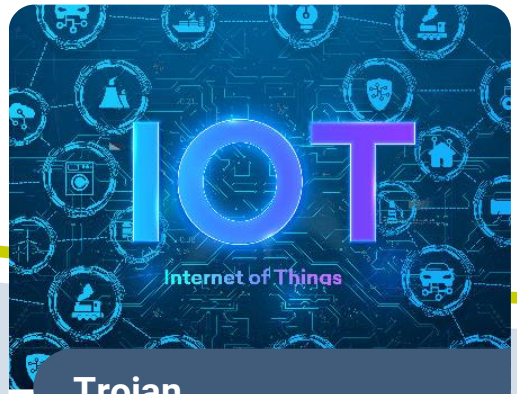


DDOS attacks

Impairment of the availability of services and systems

Supply chain attacks

Permanent manifestation in systems



Trojan

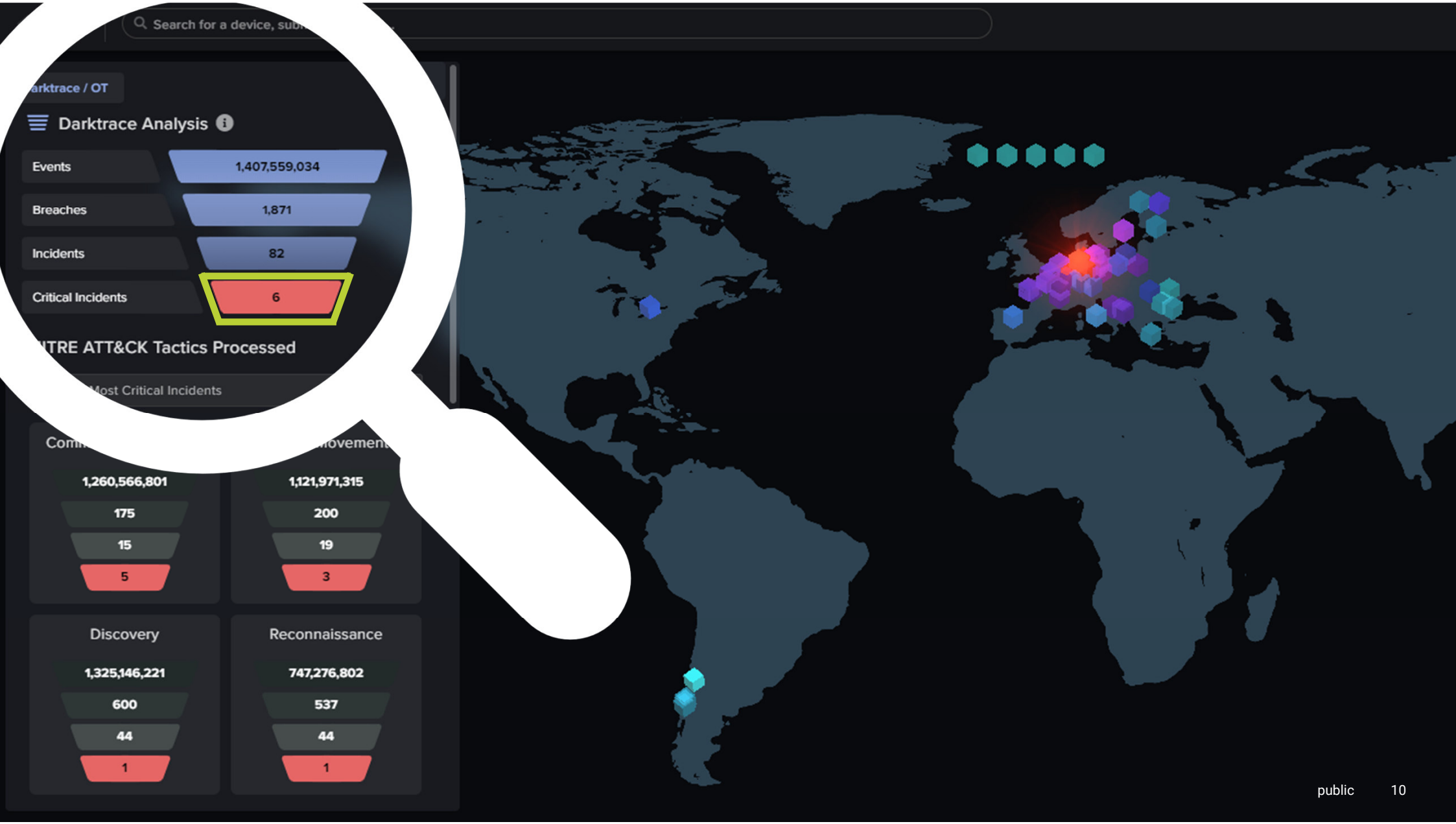
Compromise or data exfiltration

Social engineering

Identity theft or fraud implementation

AI as a special challenge

- Overtrusting
- Deep Fakes
- Automation
- Dialog Poisoning
- Hallucination


Search for a device, sub
arktrace / OT
Darktrace Analysis
Events
1,407,559,034
Breaches
1,871
Incidents
82
Critical Incidents
6
ITRE ATT&CK Tactics Processed
Most Critical Incidents
1,260,566,801
175
15
5
1,121,971,315
200
19
3
Discovery
1,325,146,221
600
44
1
Reconnaissance
747,276,802
537
44
1

Possible risks

Organizational risks

- Uncontrollable remote access
- No IT asset and update management
- Unknown security measures

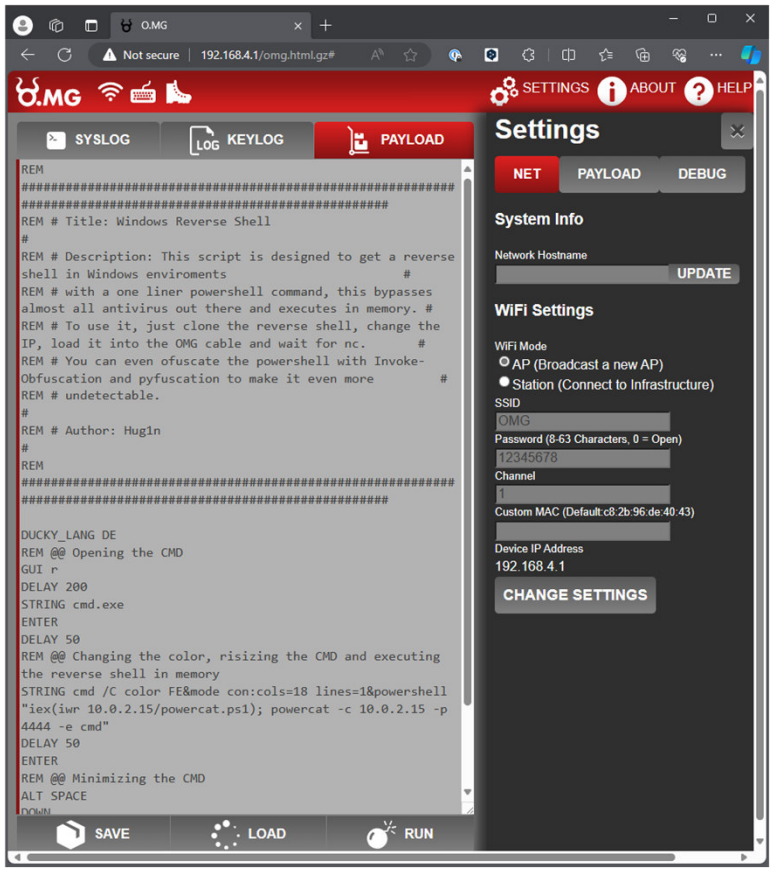
Physical risks

- Insufficient access protection
- Lack of perimeter surveillance

Technical risks

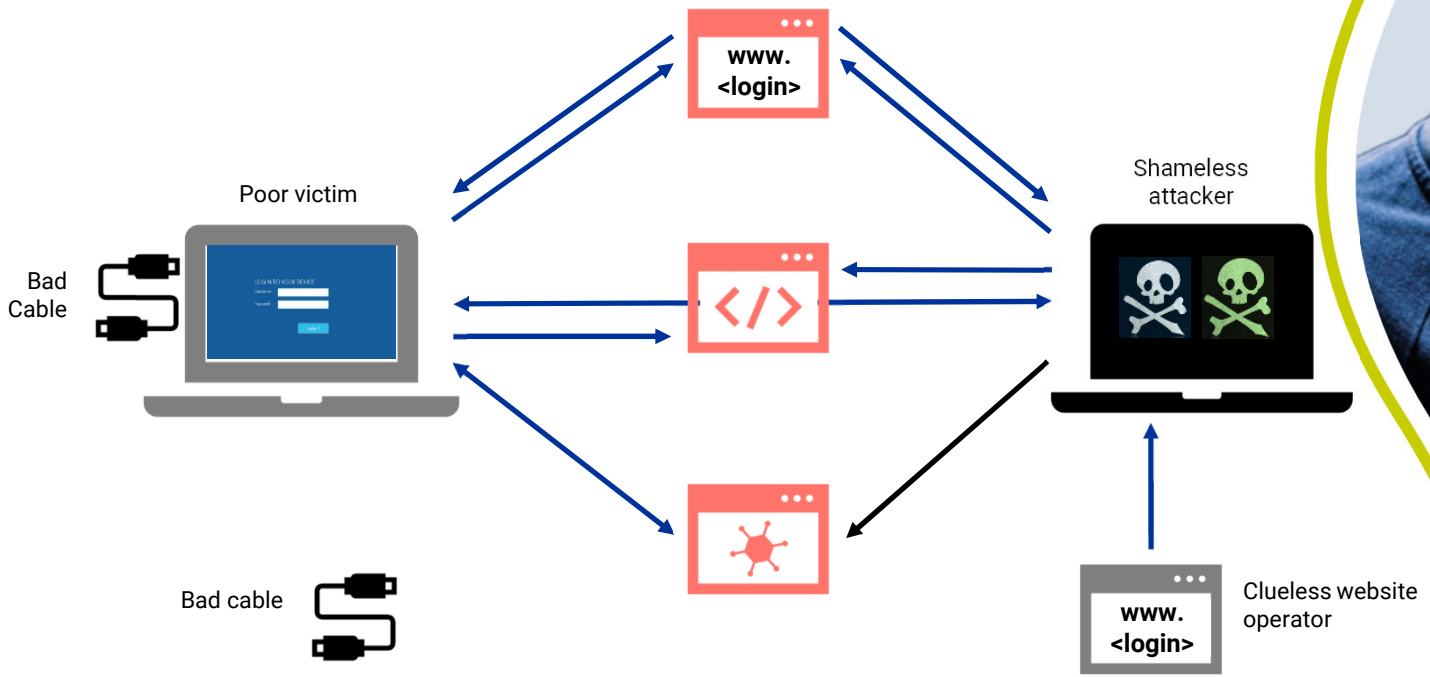
- Publicly accessible connection
- No anomaly detection
- No device control
- Hardly any standardization

Examples of current threats



O.MG Cable
Malicious device

O.MG Cable Attack



- Attacker copies website
- Attacker has malware ready
- Attacker launches "Listener"
- Victim connects USB cable
- Malware launch app for remote access
- Attacker gains real-time access to the victim's system
- Fake login page is launched
- Login data is tapped

Priorities of OT and IT security

Availability
Integrity
Confidentiality

OT

Outage not tolerable

Reliability of data is important

Minor processing of confidential data

Confidentiality
Integrity
Availability

IT

Attack Stages: IT

IT – focused

Blend in with other IT-related scans, probes, viruses and general noise

Cyber Intrusion Preparation and Execution

- Target recon
- Social engineering
- Physical malware delivery
- Interact and pivot
- Escalate privileges, exfil

Attack Stages: OT

ICS – specific indicators and objectives

Enabling, Initiating and Supporting

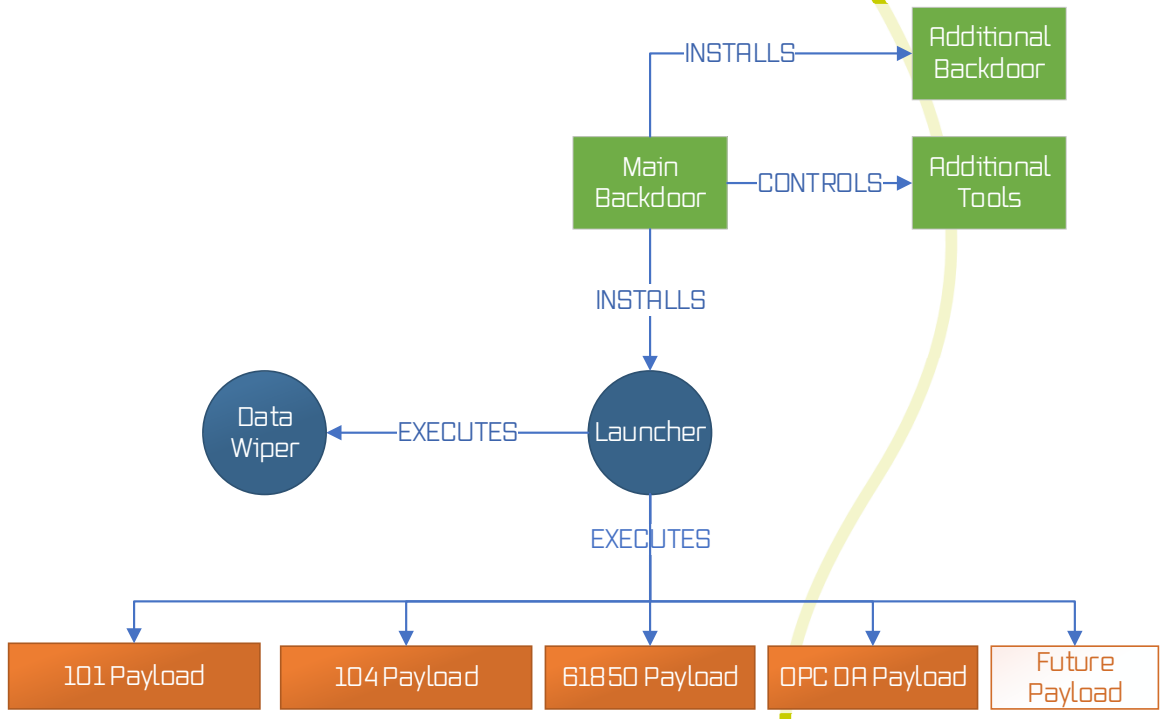
ICS Attack Development and Execution

Identified ICS targets

Remote access device in substation and control facilities

Ability to operate the system or manipulate it

Crash Override, Ukraine 2017



Source: ESET / DRAGOS

Cyber Intrusion Preparation and Execution

The CRASHOVERRIDE malware is a modular framework consisting of an initial backdoor, a loader module, and several supporting and payload modules. The most important items are the backdoor, which provides access to the infected payload modules.

ICS Attack Development and Execution

Two relevant malwares on the targeted industrial control system. One sample was the IEC 104 protocol module, and the other sample was the data wiper. An additional IEC 61850 and OPC module.

Agenda

Threat situation 1

Legal framework 2

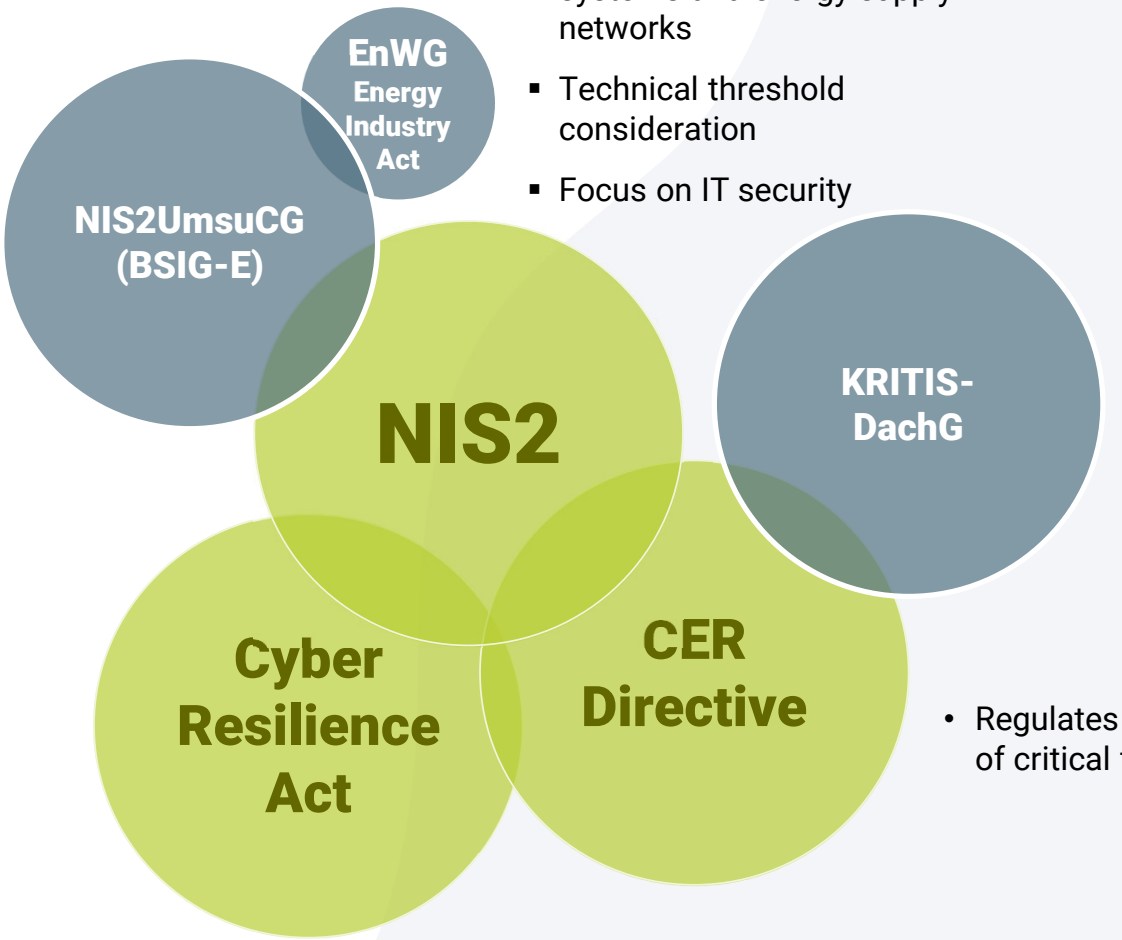
Possible measures 3

Legal framework

Overview

- Regulation of important and particularly important companies
- Focus on IT security

- Regulation of energy systems and energy supply networks
- Technical threshold consideration
- Focus on IT security



- Regulation of operators critical installations
- Technical threshold consideration
- Focus on reliability

- Regulates cybersecurity for **all** non-critical, critical and highly critical products with "digital components"
- Differentiation according to criticality levels
- Focus on product safety

- Regulates the resilience of critical facilities

EU Directive

National law

Classification and threshold values

Facilities/companies	Employees	Turnover and balance sheet
Important facilities	≥ 50	
	or	≥ 10 million and ≥ 10 million
Particularly important facilities	≥ 250	
	or	≥ 50 million and ≥ 43 million

Operators of critical systems	Electrical power
Generating plant	≥ 104 MW
Control/bundling of electrical power	
Power distribution network	3700 GWh /year
Transmission network	
Electricity trading	

Source: openKRITIS

Obligations according to NIS2UmsCG

Measures	Operators of critical infrastructure	Particularly important facilities	Important facilities
IT risk management §30	●	●	●
Special standards for KRITIS §31(1)	●		
Special measures SZA[1)] § 31(2)	●		
Reporting obligations §32	●	●	●
Independent registration §33 §34	●	●	●
Duty to inform (customers) §35	●	●	●
Personal liability of management bodies §38	●	●	●
Requirements for certificates §39	●	partially (§64)	partially (§65)

Source: openKRITIS

[1)] SzA = System for attack detection

Overview of obligations according to NIS2UmsCG

Operators of critical systems			Facilities	
			Particularly important	Important
Law	NIS2UmsuCG	RoofG	NIS2UmsuCG	NIS2UmsuCG
Period	from 2025	from 2026	from 2025	from 2025
Mandatory	§39 (1)	§11	§61	§62
Shape	Audits	Audits	BSI sampling	BSI sampling
Contents	IT security Obligation to report SzA	Resilience	IT security obligation to report	IT security obligation to report
Scope	Critical system	Critical system	The company	The company
Frequency	every three years	Samples	Samples	on occasion
Receiver	BSI	BBK	BSI	BSI

Source: openKRITIS

Regulations under the EnWG on the application of the BNetzA IT security catalog continue to apply

AI Regulation

Risk Class1

Forbidden
social scoring,
Biometric categorization

Risk Class 2

Permitted under specifications in critical infrastructures or medicine
work, education or private and public services

Risk Class 3

limited risk
naturally interacting systems,
generation of artificial content

Risk Class 4

Minimal risk e.g. AI-supported spam filters, video games

Cyber Resilience Act

Main points

- Binding cyber security requirements for planning, design, development and maintenance
- Duty of care for the entire life cycle
- CE label for all products

Area of application

- Products with digital components
- Exceptions: Open source, medicine, aviation, automotive

Agenda

Threat situation 1

Legal framework 2

Possible measures 3

Practical experience: Technology alone is not enough!

Information security management

Four factors for a successful security strategy

Raising awareness of information security

1

Pursue a best practice approach

2

As much as necessary, as little as possible

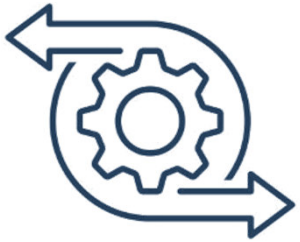
Implement safety measures

3

- Physical
- Organizational
- Technical
- Personnel

Establishing security as a process

4



Important aspects of OT/IT cyber security

DEVELOPMENT

Development of a state-of-the-art system to defend against cyber attacks.

Take the follow-up costs into account as early as the planning phase.

Try to plan a standardized environment for all projects.

Rely on partners with experience in OT and IT security.

OPERATION

Establish incident response procedures and an emergency plan.

Permanent monitoring and evaluation of network activities.

Secure connection, preferably without public access points.

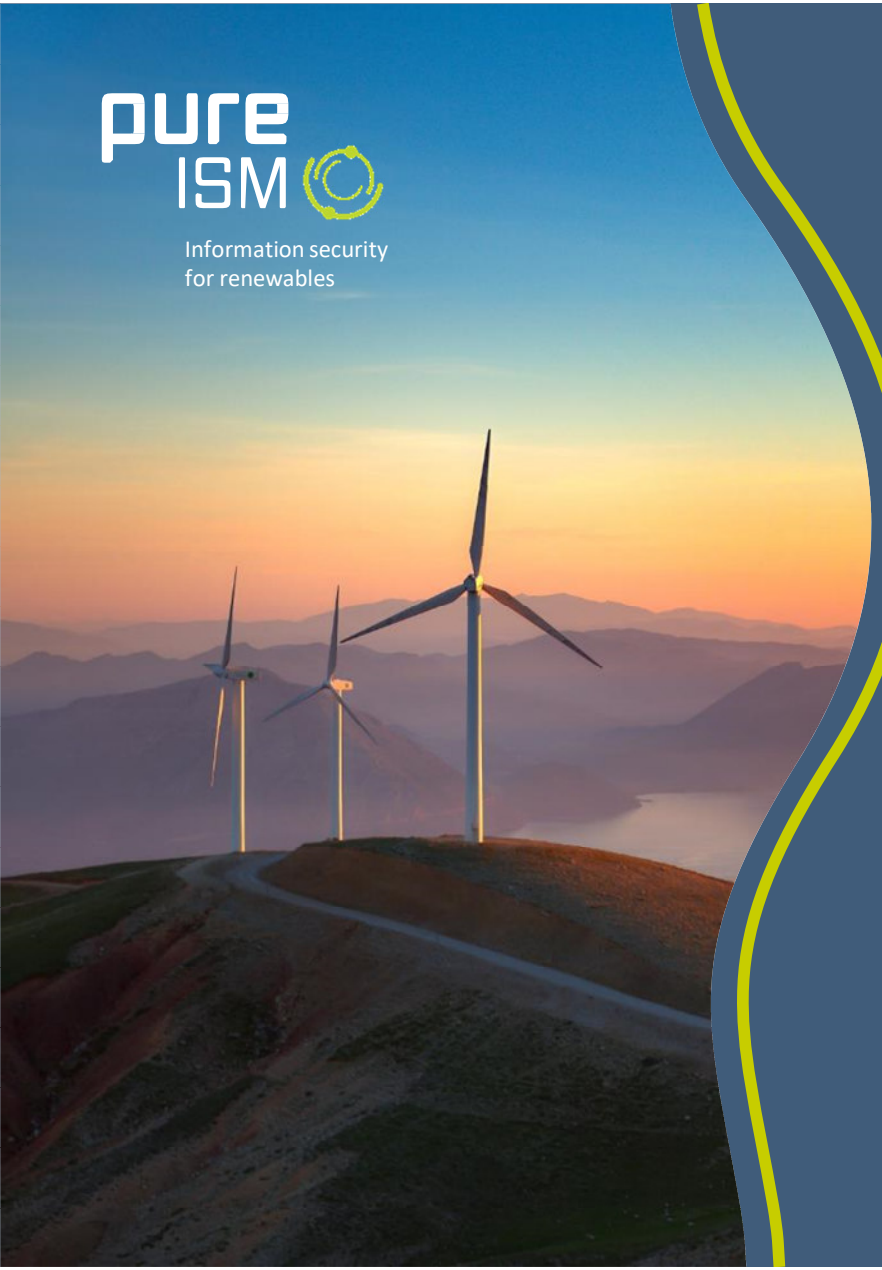
Continue risk-based asset and vulnerability management.

Definition of the measures

How should the measures be monitored?

- Which identified assets require **additional protection**?
- What **measures** are being implemented?
- Who is **responsible** for implementing the measures?
- What is the status of the measure and **when will it be implemented**?

Which asset is worth to be protected? › What measures? › Who is responsible?



pure ISM

Information security
for renewables

Any questions?

+49 421 64376611

m.ratfeld@pure-ism.de