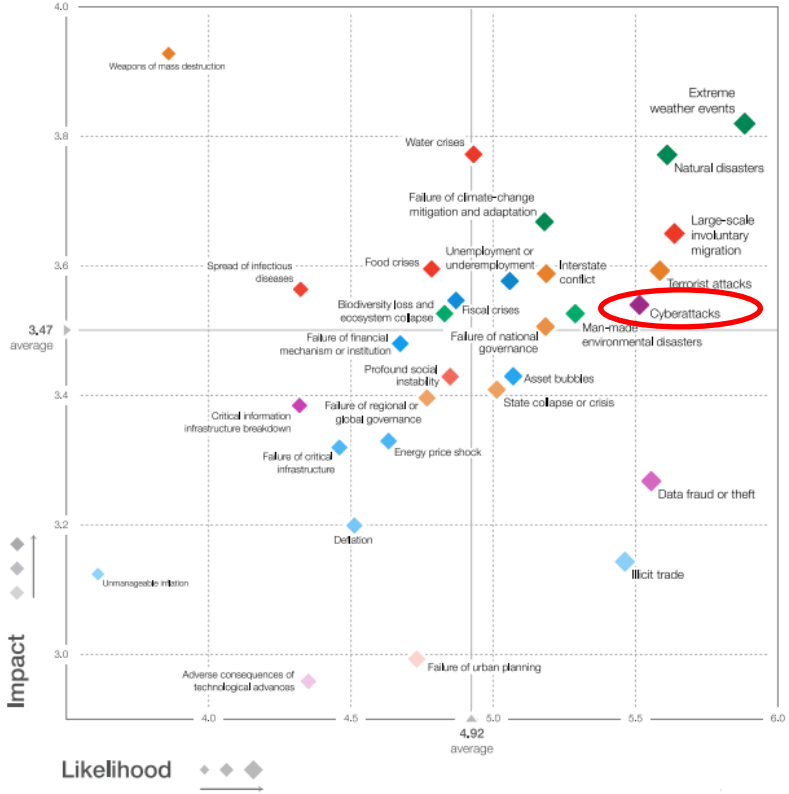
Industrial Cyber Security

Crispino Davide

Cyber Attacks: A risk among the most feared

World Economic Forum 2017:

«Cyber Attacks are considered to be one of the highest risks for the economy in terms of IMPACT and PROBABILITY»



Does this concern the industrial world?

1980s
- Fieldbus with proprietary protocols

1990s
- Standard PCs with Windows operating system come into operation as HMIs, SCADA systems, and so on

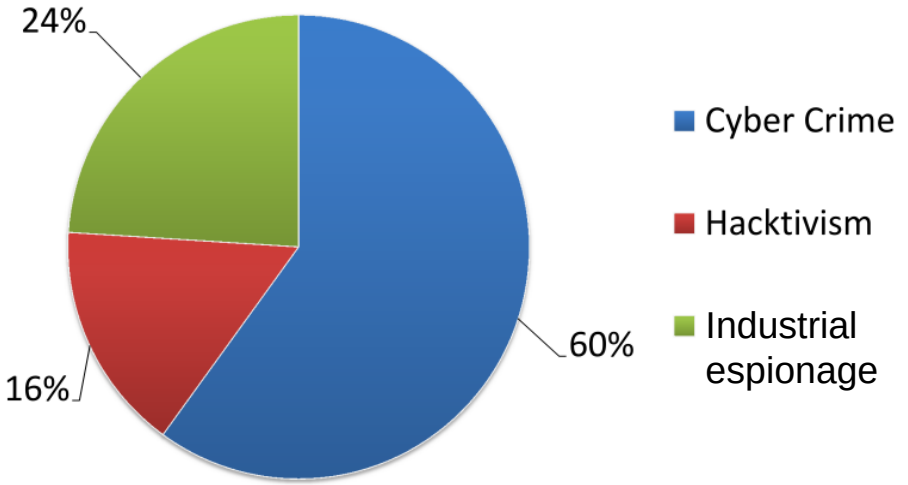
2000s
- Increasing demand for connectivity to the production network

Today
- Industrial networks are increasingly based on Ethernet (Profinet, Ethernet IP, etc.), with a homogeneous communication medium from MES to field network



What drives someone to attack?

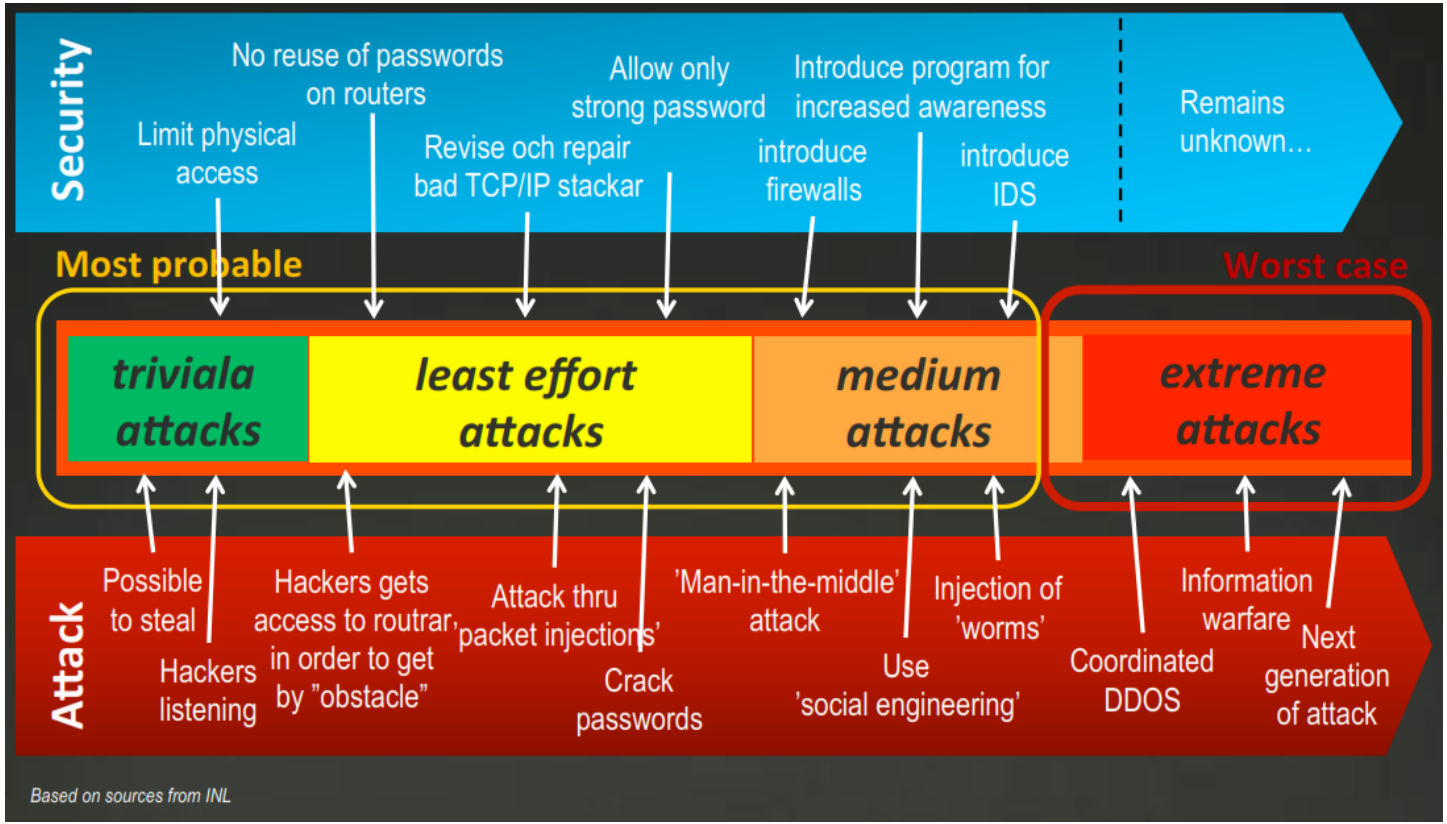
¼ of the attacks to the Industry are for espionage



Protecting plants is a necessity

Fonte: Rapporto Clusit 2014, dati Fastweb

Most common type of attack



Real attack on critical infrastructure

12/24/2015

Dear customers!

Dec. 23, 2015, from 15:35 - 16:30, third parties were made illegal entry into information-technological system of remote access to equipment telecontrol substations of 35-110 kV JSC "Kyivoblenergo."

As a result, it was disconnected 7 (seven) 110 kV substations and 23 (twenty three) substation 35 kV. This led to the repayment of about 80,000 different categories of customers on the reliability of electricity supply.

Electricity was restored to all consumers employees of the Company at **18:56** the same day.

We apologize for the situation and thank you for your understanding.

PJSC "Kyivoblenergo"

Phishing E-mails

BlackEnergy 3

VPN & Credential Theft

Network & Host Discovery

Malicious Firmware Development

SCADA Hijack (HMI/Client)

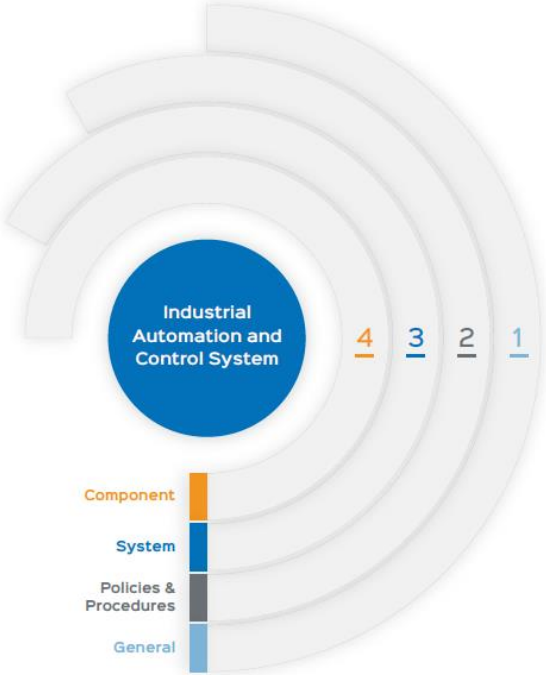
Breaker Open Commands

UPS Modification
Firmware Upload
KillDisk Overwrites

Power Outage(s)

Industrial CyberSecurity solution

ANSI/IEC-62443: Defense in Depth concept



GENERAL

- 1-1 Terminology, concepts and models
- 1-2 Master glossary of terms and abbreviations
- 1-3 System security compliance metrics
- 1-4 IACS security lifecycle and use-case

POLICIES & PROCEDURES

- 2-1 Requirements for an IACS security management system
- 2-2 Implementation guidance for an IACS security management system
- 2-3 Patch management in the IACS environment
- 2-4 Installation and maintenance requirements for IACS suppliers

SYSTEM

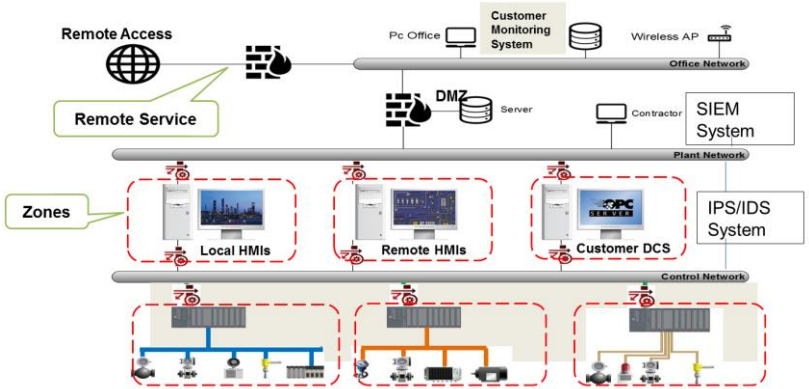
- 3-1 Security technologies for IACS
- 3-2 Security levels for zones and conduits
- 3-3 System security requirements and security levels

COMPONENT

- 4-1 Product development requirements
- 4-2 Technical security requirements for IACS components

Industrial Network Security

Vulnerabilities must be made unavailable without affecting the normal operation of the plants



- Divide the industrial network in separate "Zones"
- The zones communicate with each other using only the previously identified "Conduits"
- All incoming / outgoing traffic from a conduit is protected by firewalls or dedicated systems that guarantee the integrity and confidentiality of communication (eg VPN)

This approach is also suggested by ICS-CERT and the ISA99 standard

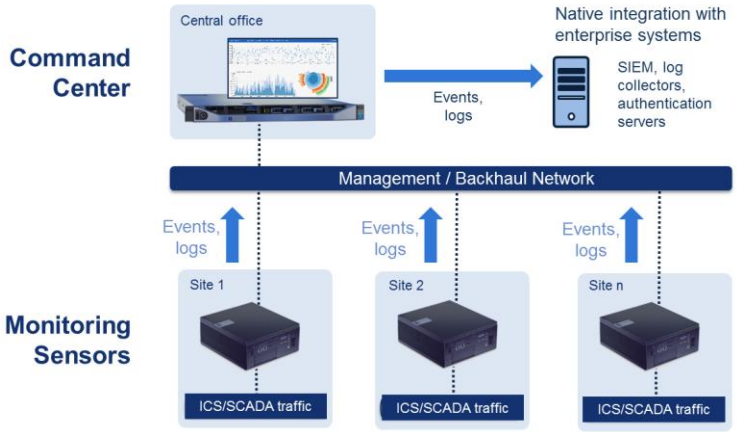
Industrial Cyber Resilience

IDS / IPS Systems

- Intrusion Detection / Prevention
- Monitor all traffic within the network at certain points
- Requires hardware sensors throughout the network
- IPS also automatically blocks suspicious traffic

SIEM

- Security information & event management
- Collect logs from all relevant hardware as well as IDS/IPS and Firewall appliances
- Centralized real-time display and activity report with correlation analyses



Security Levels

ISA 62443 defines SLs in terms of five different levels (0, 1, 2, 3 and 4), each with an increasing level of security:

- SL 0: No specific security protection capability
- SL 1: Capability to protect against casual or coincidental violationSL 2: Capability to protect against intentional violation using simple means with low resources, generic skills and low motivation
- SL 3: Capability to protect against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate
- motivation
- SL 4: Capability to protect against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

ISA 62443 defines 7 Foundational Requirements:

FR 1 Identification & authentication control (IAC)
FR 2 Use control (UC)
FR 3 System integrity (SI)
FR 4 Data confidentiality (DC)
FR 5 Restricted data flow (RDF)
FR 6 Timely response to events (TRE)
FR 7 Resource availability (RA)

SL of a zone, component or system can be expressed as a vector:
SL {IAC UC SI DC RDF TRE RA}

Protection Levels

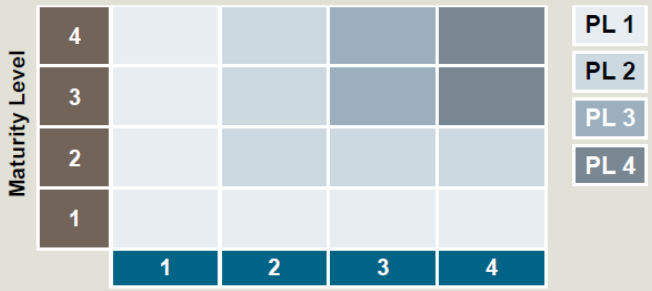
Security process

- Based on IEC 62443-2-4 and ISO27001
- Maturity Level 1 - 4

Protection Level (PL)

Security functions

- Based on IEC 62443-3-3
- Security Level 1 - 4



Protection Levels is a methodology to evaluate the protection of plants in operation

It is not a question of whether,
but when