Security - NIS 2

Morten Kromann

SIEMENS

NIS 2 – Sommer 2024

Spørgsmål, du kan stille dig selv

- Er jeg omfattet?
- Hvilke krav vil det medføre?
- Er der et kunde-/leverandør- forhold, der gør, jeg er omfattet?
- Hvad skal jeg skrive i mine kontrakter?
- Hold øje med andre krav, så du kan slå 2 fluer med et smæk.

SIEMENS

NIS 2 – hvad kan man gøre i dag?

Artikel 18

CRM measures shall include **at least** (technical + methodological requirements will be **defined via implementing acts**):

- **risk analysis** + information system security policies;
- incident handling;
- business continuity (e.g. backup management, disaster recovery) + crisis management;

SIEMENS

NIS 2 – hvad kan man gøre i dag?

Artikel 18

- **supply chain security** incl. security-related aspects re. the relationships between each entity and its direct suppliers or service providers;
- security in network and information systems **acquisition**, development + maintenance, incl. vulnerability handling + disclosure;
- policies + procedures to assess the effectiveness of CRM measures;
- basic computer hygiene practices + **cybersecurity training**;

SIEMENS

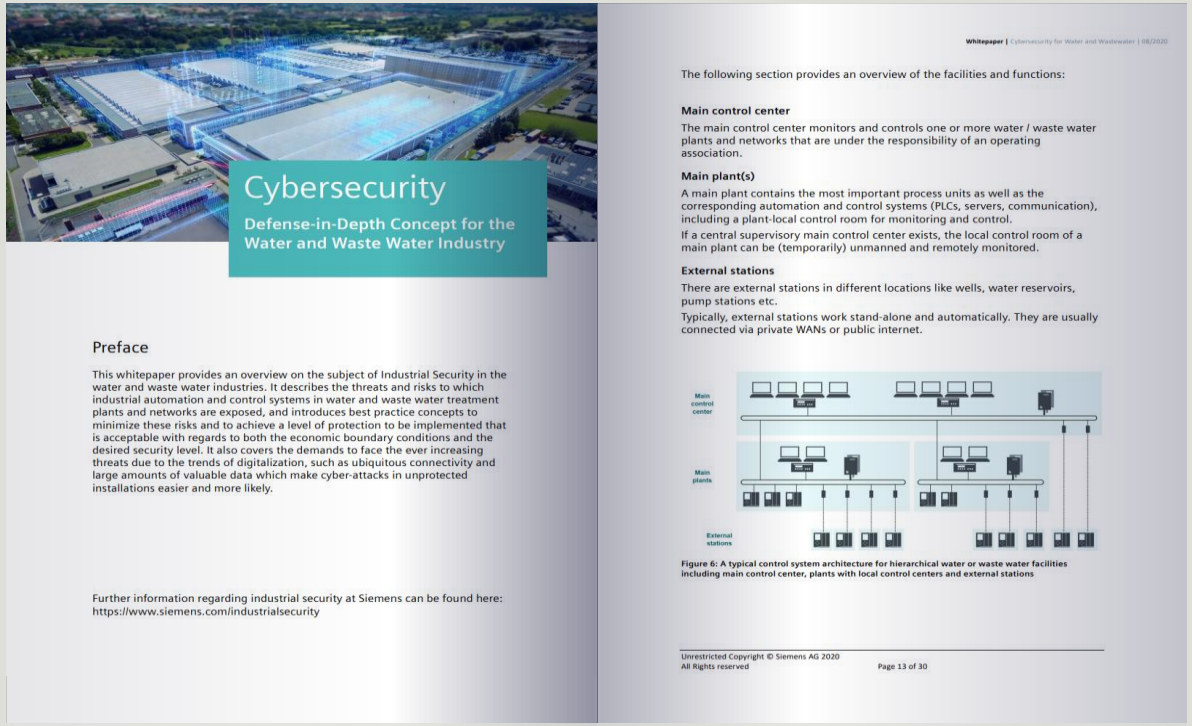
NIS 2 – hvad kan man gøre i dag?

Artikel 18

- policies + procedures re. the **use of cryptography** +, where appropriate, encryption;
- human resources security, access control policies + **asset management**;
- the use of **multi-factor authentication** or continuous authentication solutions, secured voice, video + text communications + secured emergency communications systems within the entity, where appropriate.

SIEMENS

Hvor er der hjælp at hente?



Cybersecurity

Defense-in-Depth Concept for the Water and Waste Water Industry

Preface

This whitepaper provides an overview on the subject of Industrial Security in the water and waste water industries. It describes the threats and risks to which industrial automation and control systems in water and waste water treatment plants and networks are exposed, and introduces best practice concepts to minimize these risks and to achieve a level of protection to be implemented that is acceptable with regards to both the economic boundary conditions and the desired security level. It also covers the demands to face the ever increasing threats due to the trends of digitalization, such as ubiquitous connectivity and large amounts of valuable data which make cyber-attacks in unprotected installations easier and more likely.

Further information regarding industrial security at Siemens can be found here:
https://www.siemens.com/industrialsecurity

The following section provides an overview of the facilities and functions:

Main control center

The main control center monitors and controls one or more water / waste water plants and networks that are under the responsibility of an operating association.

Main plant(s)

A main plant contains the most important process units as well as the corresponding automation and control systems (PLCs, servers, communication), including a plant-local control room for monitoring and control.

If a central supervisory main control center exists, the local control room of a main plant can be (temporarily) unmanned and remotely monitored.

External stations

There are external stations in different locations like wells, water reservoirs, pump stations etc.

Typically, external stations work stand-alone and automatically. They are usually connected via private WANs or public internet.

Figure 6: A typical control system architecture for hierarchical water or waste water facilities including main control center, plants with local control centers and external stations

IEC62443 Blueprints

- Generelle
- Branchespecifikke

www.siemens.dk/industrial-security
https://support.industry.siemens.com/cs/dk/en/view/109802750

SIEMENS