Xertified point of view: Network and Information Security (NIS2) directive

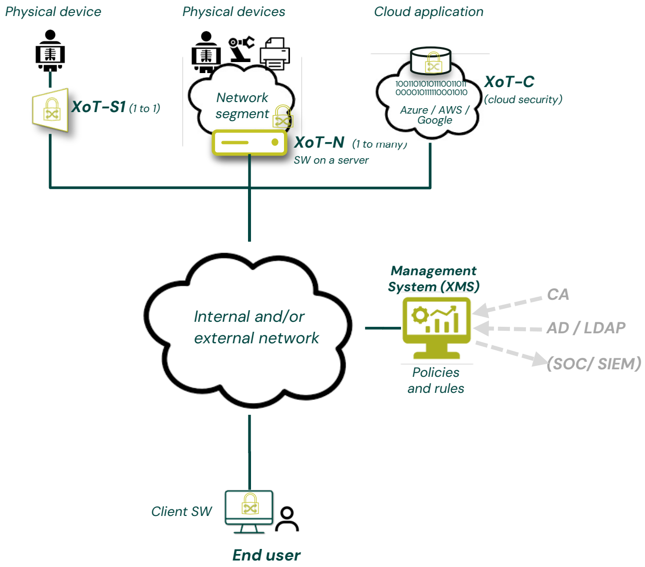
Xertified

XoT technology™ basics

The digital lock 3.

Allow/deny access 2.

The digital key 1.



- A digital lock, **preventing** unauthorised access
- Secures critical devices **within minutes**
- Requires **no configuration** of clients or protected devices
- Brings undeniable digital identities to **legacy systems and new devices**
- **Secures the traffic** between devices and users
- High level security for **any type of device**
- **Multi-layered security** with encryption, digital identities, authentication and traceability

Oct 18, 2024 – NIS 2 becoming law

- The NIS 2 Directive replaces the NIS Directive (Directive 2016/1148/EC).
- Member states must incorporate the provisions of the NIS 2 Directive into national law in 21 months from the entry into force of the directive, that means it becomes a law, complete with all penalties, on October 18, 2024.
- Furthermore, management bodies at relevant companies and organisations will have a crucial and active role in the supervision and implementation of these measures. If an essential operator is non-compliant several measurements may apply:
  - Fines up to 10 million EUR or 2% of the total global annual turnover may be invoked
  - Management liability, making security violations public including naming responsible individuals
  - Temporary bans against individuals to hold a management position in affected organisations

What is NIS 2

The NIS2 (Network and Information Security) directive aims to improve the collective cybersecurity in EU

1. **increase cyber resilience** across essential service providers

2. streamline cyber resilience through **stricter security requirements and penalties for violations**

3. **improve the EU's preparedness** to deal with cyber-attacks

NIS -> NIS 2

Broadening the scope, tightening of governance and significantly increased penalties

NIS

The Network and Information Security (NIS) Directive specific aim was to achieve a high common level of cybersecurity across the EU Member States.

While it increased the Member States' cybersecurity capabilities, the implementation resulted in fragmentation at different levels across the members

The original NIS-directive considers sectors critical for a functional society:

- Healthcare
- Digital infrastructure
- Transport
- Water supply
- Digital service providers
- Banking and financial market infrastructure
- Energy

NIS 2

The NIS directive has been extended to further enhance security and ensure similarity between Members States and new sectors have been added:

- Providers of public communications NW or services
- Wastewater and waste management
- Manufacturing of certain critical products (e.g., pharmaceuticals, medical devices, and chemicals)
- Food
- Digital services (e.g., social networking platforms and data centre services)
- Space (e.g., aerospace)
- Postal and courier services
- Public administration

Governance: Increased minimum security and reporting requirements. Stricter supervisory measures and compliance requirements for authorities.

Penalties: Administrative fines has been made possible together with increased cooperation and information sharing between Member States' authorities

NIS2 vs CER

CER covers a wide range of unexpected events, whereas NIS2 covers only cybersecurity

Natural disasters

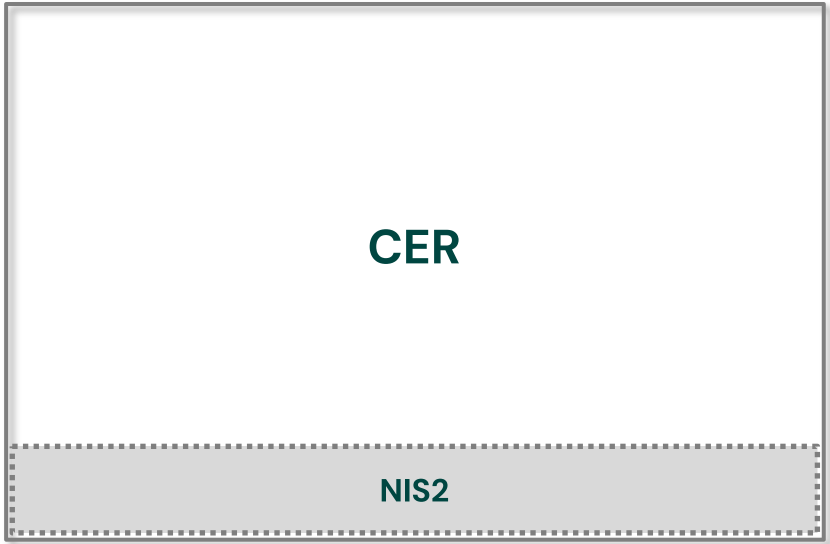
Terrorist attacks

Sabotage

Pandemics

Other critical events

Cybersecurity



Critical Entities Resilience Directive

CER is an EU-wide security-oriented legislation that replaces Directive 2008/114/EC. While NIS2 has a focus on cybersecurity, CER aims to create an overarching framework addressing the resilience of critical entities in respect of all hazards, whether natural or man-made, accidental or intentional

CER Directive operates on the premise that resilience should not be limited to cybersecurity but must also extend to physical threats such as terrorist offences, sabotage, and natural disasters.

NIS2 vs DORA

DORA: Digital Operational Resilience Act, focusing on financial systems and organisations

WHAT IS DORA?

DORA ensures that organisations within the financial system also follow rules for the protection, detection, containment, recovery and repair capabilities against ICT-related incidents.

DORA explicitly refers to ICT risk and sets rules on ICT risk-management, incident reporting, operational resilience testing and ICT third-party risk monitoring.

This Regulation acknowledges that ICT incidents and a lack of operational resilience have the possibility to jeopardise the soundness of the entire financial system, even if there is "adequate" capital for the traditional risk categories.

DORA OR NIS2?

According to NIS2 everything that is considered society critical or society important shall adhere to this regulation

HOWEVER, if an organisation falls under sector-specific requirements, in this case DORA, the NIS2 requirements regarding areas covered by DORA no longer apply as long as the requirements are not lower that what NIS2 stipulates.

In short, the sector-specific requirements that DORA sets beyond NIS2 relates mainly to major ICT-related incident reporting (Article 17 et seq.), as well as on digital operational resilience testing, (Art 24 et seq.) information-sharing arrangements (Article 25) and ICT third-party risk (Article 28 et seq.) where DORA regulations shall apply instead of those provided for in the NIS 2 Directive.

Cybersecurity risk management

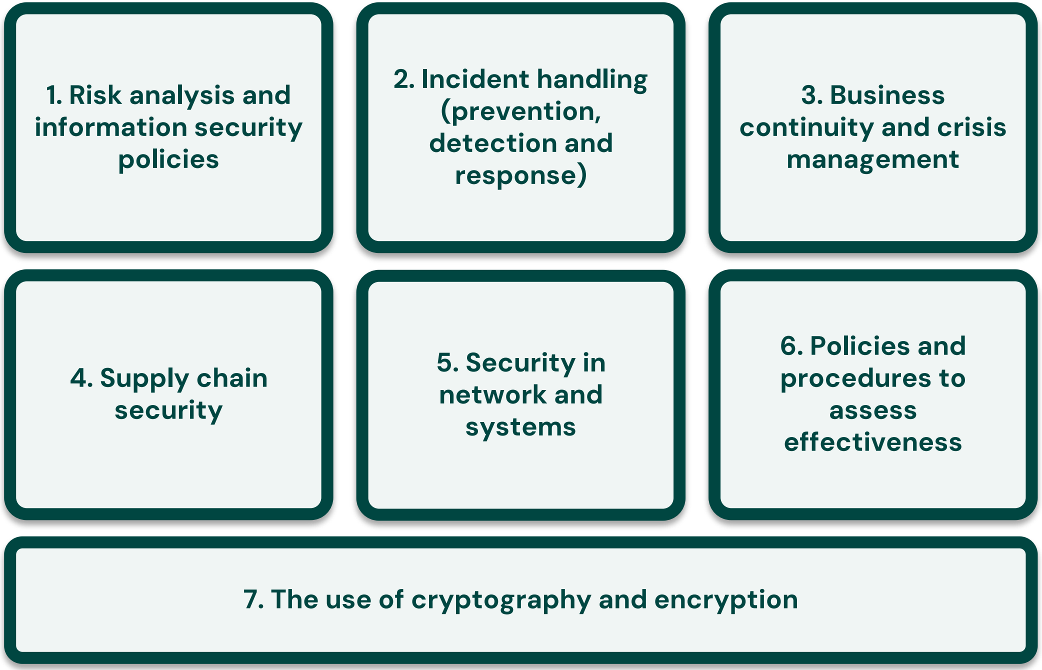
Analyse, plan, prevent and mitigate

CYBERSECURITY RISK MANAGEMENT MEASURES

NIS2 aims for an aligned cybersecurity management approach to mitigate inconsistencies in cybersecurity resilience across the in-scope sectors.

NIS2 outlines **seven key measures** that all essential and important entities shall take to manage risks posed to the security of those entities' network and information systems when providing their services.

What constitutes a “significant impact” on an entity has been clarified. It will no longer be a defined metric (number of impacted users) but rather whether there was disruption to critical services, or financial or material loss.



1. Risk analysis and information security policies

2. Incident handling (prevention, detection and response)

3. Business continuity and crisis management

4. Supply chain security

5. Security in network and systems

6. Policies and procedures to assess effectiveness

7. The use of cryptography and encryption

XoT technology adherence to NIS 2

XoT technology is focused on preventing breaches and significantly enhance the security posture

At the core of NIS 2 is a requirement to implement access control and firm network and systems security. XoT technology is centred around a zero-trust solution, using undeniable digital identities and encryption for everyone and everything.

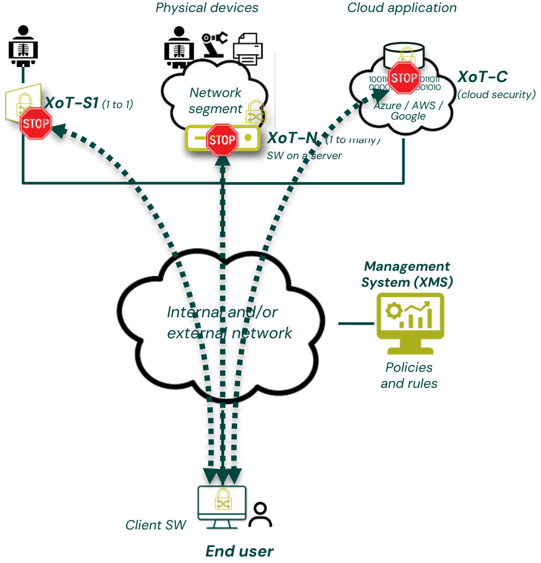
NIS 2 Key Measure	Directly	Indirectly	How
1 – Risk analysis and information security policies			
2 – Incident handling (prevention, detection and response)	✓		Strict access control to prevent unauthorised access to critical equipment or systems. Recording events and actions.
3 – Business continuity and crisis management		✓	Supports resilient IT and OT operations
4 – Supply chain security	✓		Creating a fully secure network between various entities in the value-chain using undeniable digital identities and encryption
5 – Security in network and systems	✓		Access control, undeniable digital identities, encryption end-to-end, tracking usage and users, creating event records
6 – Policies and procedures to assess effectiveness			
7 – The use of cryptography and encryption	✓		XoT technology is based on undeniable digital identities, zero trust and two layered encryption end-to-end

Key Measure 2

Incident handling incl. prevention

The core of XoT technology – to prevent unauthorised access and secure the communication user->device

Access control and encryption



Incident handling (prevention, detection and response)

Incidents primarily needs to be prevented, and in order to do so they must be understood and anticipated.

If a breach occurs, then they need to be timely detected and responded to

Prepare –> mitigate -> improve

Mitigation through XoT tech.

XoT technology prevents unauthorised access to critical equipment, devices and systems, and enables secure communication between users and devices.

Prevention of breaches through:

- Strict access control
- Undeniable digital identities
- Two-layered encryption for all communication

Detection of potential and actual breaches:

This is possible through continuous event logs from each XoT HW and SW unit, data that then can be analysed any standard SIEM system.

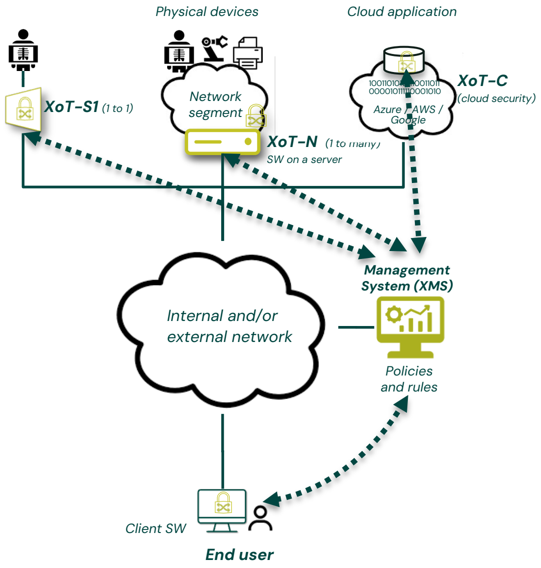
- Access attempts by unauthorised users
- Access made by users or devices
- Disconnected devices or power outage
- Traffic patterns and key users

Key Measure 4

Supply chain security

Policy based access control that allows users from multiple organisation to communicate securely

Policies for users and devices



Supply chain security

Supply chain security focuses on the risk management of external suppliers, vendors, logistics and transportation. The goal is to identify, analyse and mitigate the risks inherent in working with other organizations as part of a supply chain and involves both physical security relating to products, and cybersecurity for software and services.

A wide variety of activities including monitoring external connections, review ports and tools used for 3rd party access to the network, specifying machines and access control policies.

Mitigation through XoT tech.

Creating full security through access control based on undeniable digital identities for man and machine

Creating solid supply chain security through:

- Authentication of each user and each device, across several organisations.
- Policy based access control to machines, systems and data sources.
- Using undeniable digital identities and end-to-end encryption over any type of IP network.

Policy based access controlled based on:

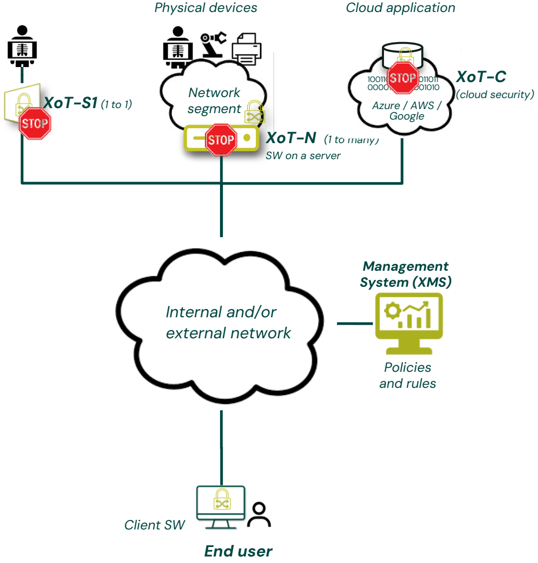
- Geographic location of secured device
- Geographic location of user
- Date/time
- Type of secured device/system/data source

Key Measure 5

Security in NW and systems

Only trusted users (and devices) can access secured devices/machines/equipment/systems

NW independent security



Security in networks and systems

Network security is defined as the process of creating a strategic defensive approach that secures a company's data and its resources across its network. It protects the organization against a potential threat or unauthorized access.

Mitigation through XoT tech.

Dedicated access control secures critical resources even if there is a breach in the network security and enables any type of equipment to operate on any type of network.

Protection through rigid access control:

- Allowing trusted users and devices access based on role and associated policies
- Blocking all other users and warning when someone tries to breach the security
- Tracing all key aspects of access, communication and traffic flows

End-to-end encryption of all data in motion:

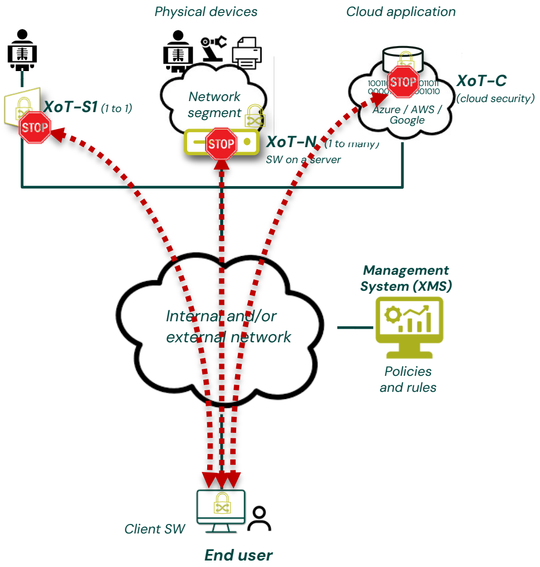
- A multi-layered security approach using both HW and SW to create state-of-the-art security
- PKI to secure user identities and enable challenge-response methodology
- Wireguard with session-based keys for all communication

Key Measure 7

Cryptography and encryption

Only trusted users (and devices) can access secured devices/machines/equipment/systems

PKI & Wireguard encryption



The use of cryptography and encryption

Encryption is the method by which information is converted into secret code that hides the information's true meaning.

The science of encrypting and decrypting information is called cryptography

Mitigation through XoT tech.

XoT technology is based on zero trust and the use of undeniable digital identities and full end-to-end encryption

Access control cryptography :

The access control function is based on the use of PKI and X.509:

- Trusted and proven technology (standard)
- Everything based on certificates
- Creating undeniable digital identities
- Using elliptic curves

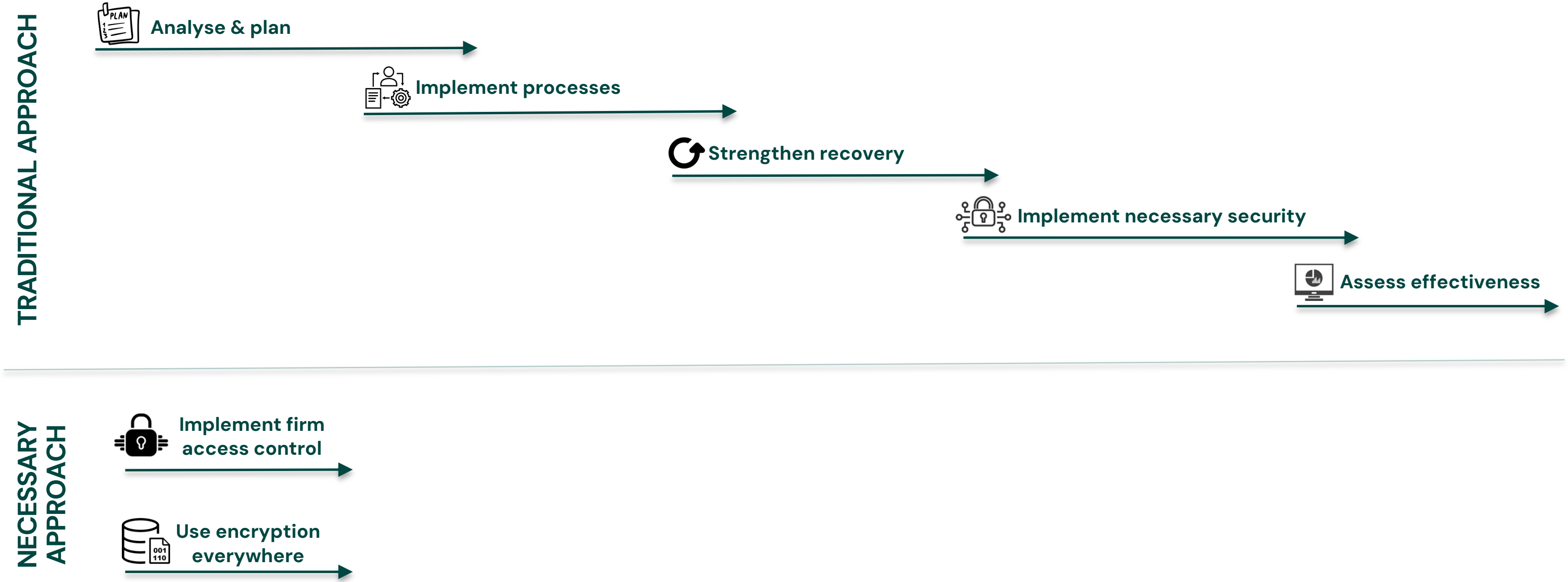
Communication cryptography:

Any communication uses two sets of encryption for high security:

- PKI used to continuously secure end user reliability (including challenge response)
- Wireguard used for all data transport
- Session based keys/crypto certificates

Act now, your adversiaries are not waiting

The threat is already here, solve the most imminent and obvious needs immediately



TRADITIONAL APPROACH

Analyse & plan

Implement processes

Strengthen recovery

Implement necessary security

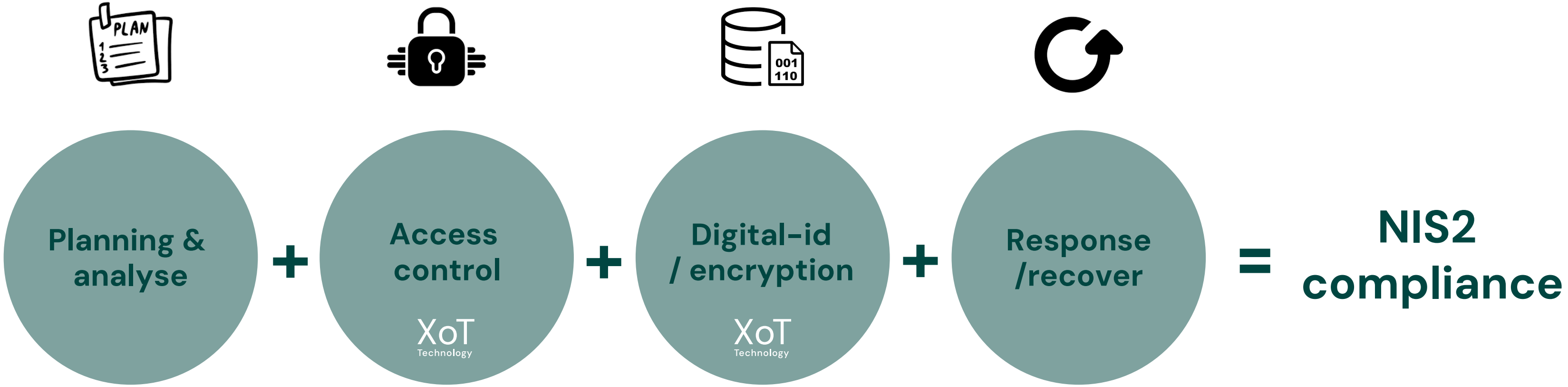
Assess effectiveness

NECESSARY APPROACH

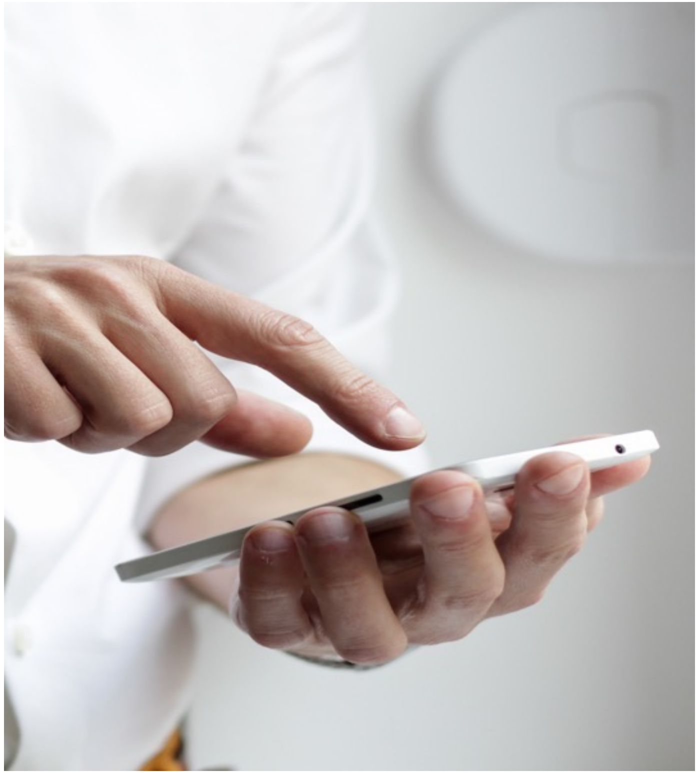
Implement firm access control

Use encryption everywhere

Summary



Planning & analyse + Access control + Digital-id / encryption + Response /recover = NIS2 compliance



Everything connected can be exposed.

Until now.