



www.ean.care

EUROPEAN
AGEING
NETWORK

Please MUTE



When not speaking



We care...
since 1989

www.ean.care



PROGRAMME

NIS2 and Social Services

Experiences from EAN Member States

- **The Netherlands** – Richard Plug (Z-CERT)
- **Czech Republic** – Miroslav Kvapil (Lexnova)
- **France** – Philippe Passis & Thomas Aczel (Ressourcial)
- **Austria** – PPT of Lebenswelt Heim Bundesverband by Jiří Horecký
- **Q&A**

16 March 2026, 13-14 CET

Webinar



Z-CERT

CSIRT for Dutch Healthcare

Richard Plug

16 maart 2026

Z-CERT

2



TLP: AMBER + STRICT



About us

Let me introduce myself



Richard Plug

Business Consultant

Noteworthy:

- Responsible for mental healthcare and elderly care accounts
- Former CISO at IT-service provider
- BA in Japanology

richardplug@z-cert.nl

+31626251729



Our mission

Dutch healthcare digitally secure





Z-CERT About us

The CERT for Dutch healthcare



Statutory task NIS2

Founded

June 1st 2017



Non-profit foundation

No commercial services
No market disruption



Funding

Member contributions
Funding from health ministry



402 Participants

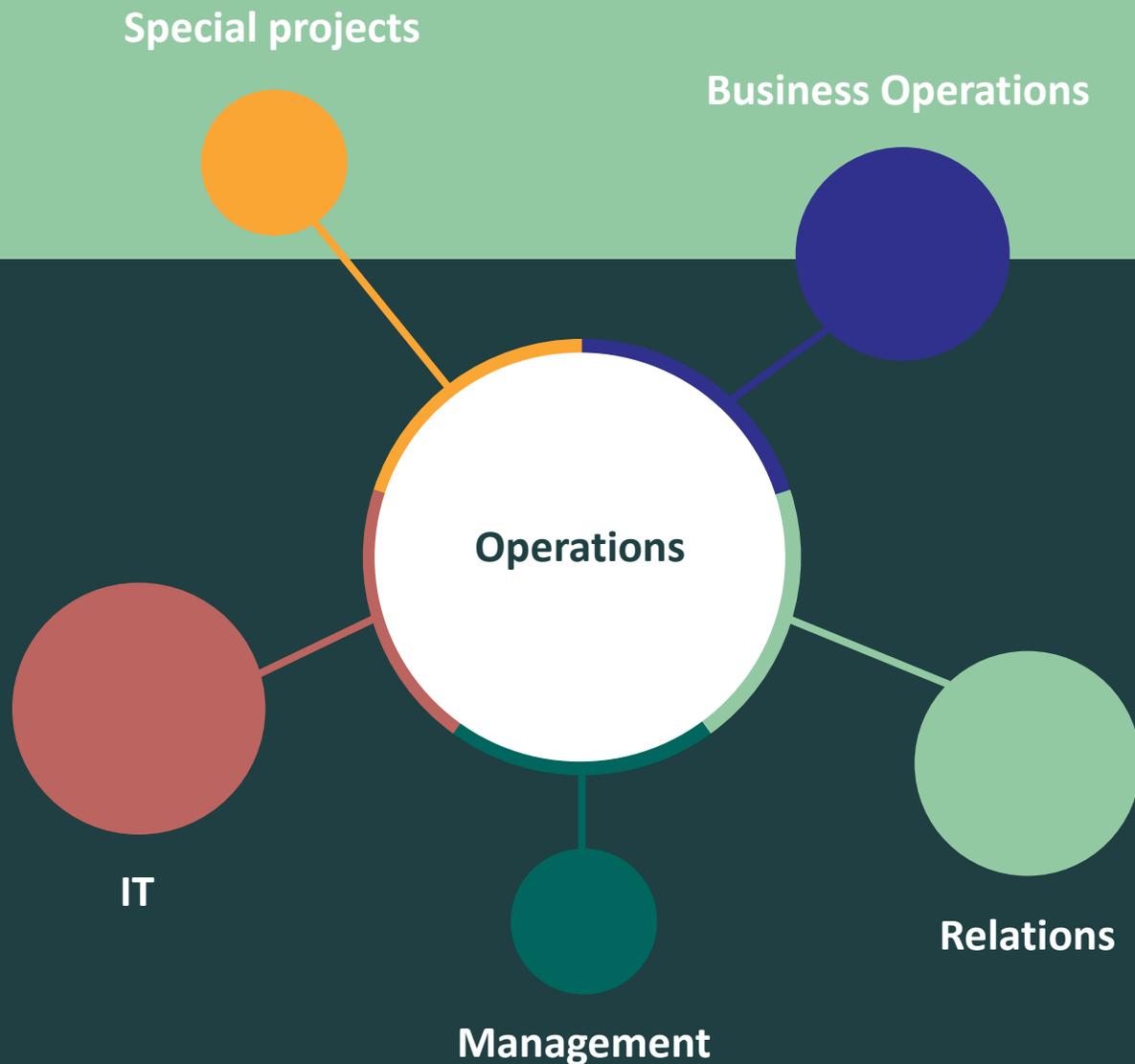
102 NIS2 entities
Expected growth: 1500+





Z-CERT Our team

Start of 2026:
± 70 employees

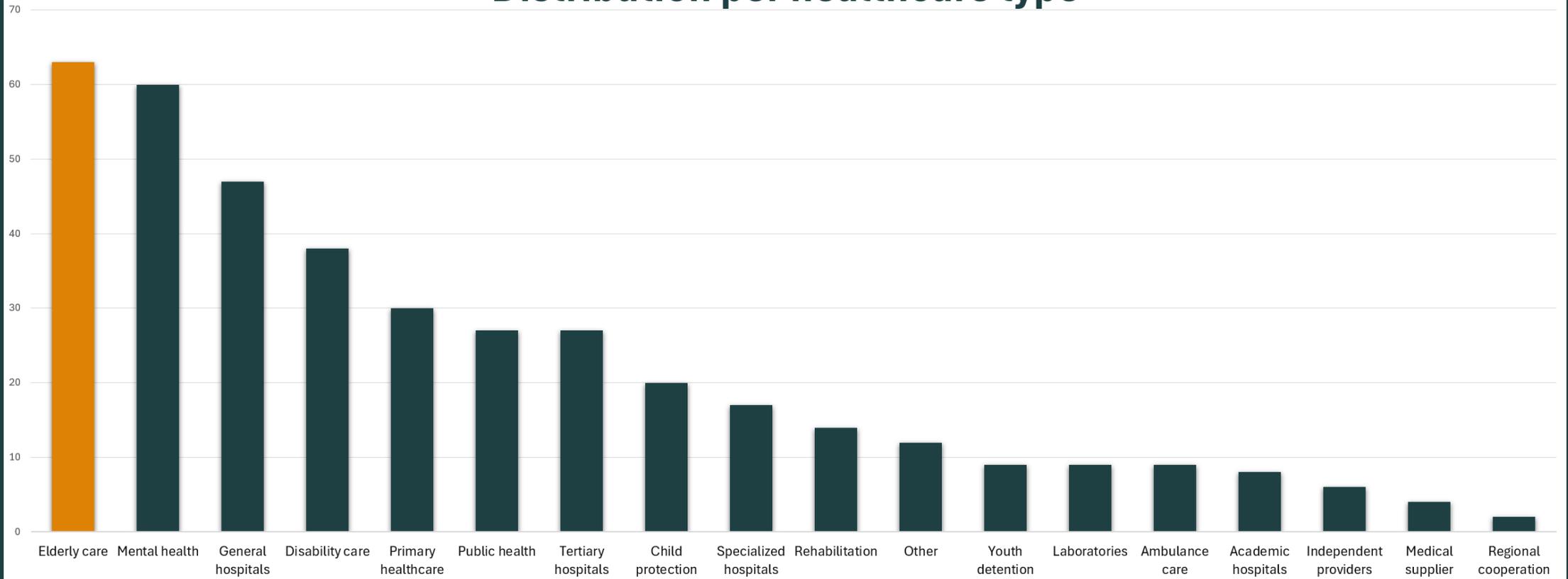




Z-CERT

Our participants

Distribution per healthcare type

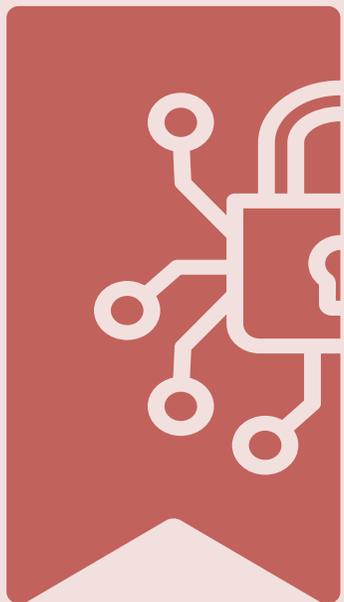


Z-CERT



Z-CERT

One CERT, two labels



csirt

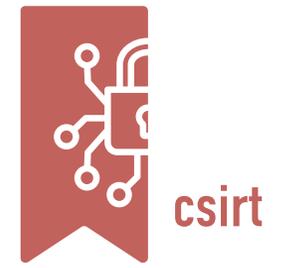


academy



Z-CERT
CSIRT

Our statutory duty



Warning service

Advisories
Active threats
Crisis notifications



Incident coordination

24/7 Advice and coordination
Who does what and when?
Backed by a very large network



Monitoring service

Scanning IP-addresses and domain names
Monitoring breaches, leaks, darkweb, proprietary analysis



Coordination Ethical Hackers

Z-CERT assesses and communicates
Central Hall of Fame!



Knowledge base

Whitepapers, guidelines, factsheets, etc.

Made by us, our participants and partners



Self-service portal

Insight & administration

Contact - preferences



Events

A large event every other year

Multiple smaller events

Attending numerous industry events



Webinars

Monthly webinars

Own content combined with input from our community



Personal contact

Business consultant as first point of contact

'knowledge brokers'



Large community

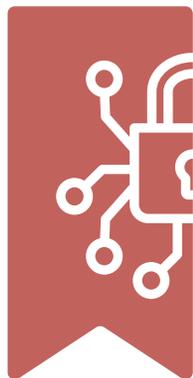
Over 1000 active users

Connect to the whole healthcare sector



Z-CERT

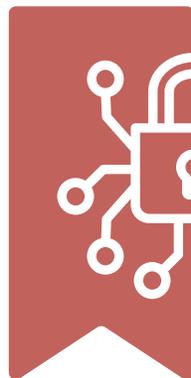
Obligations for healthcare providers



csirt

Mandatory registration

Through the National Cyber Security Center for all entities



csirt

Mandatory Reporting

For incidents exceeding a certain threshold.



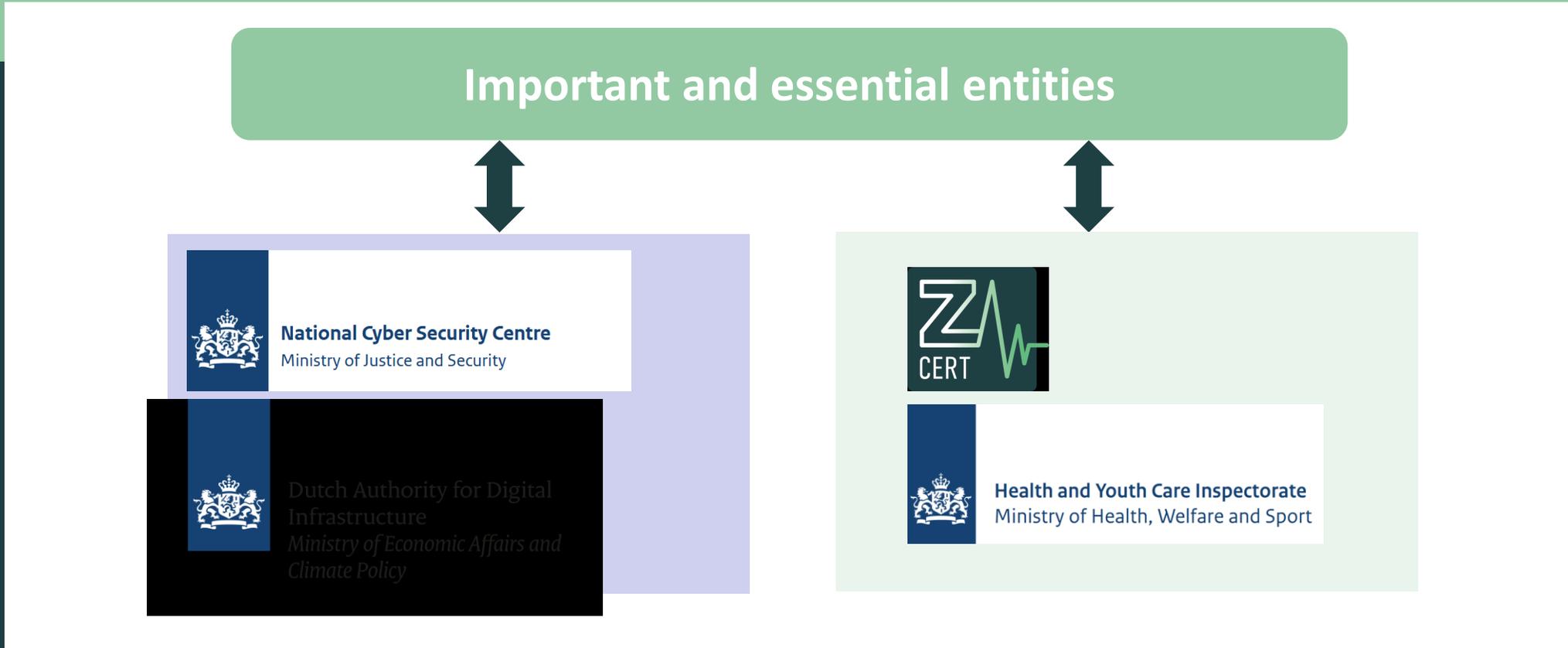
academy

Duty of care

Mostly comprised of compliance with national security in healthcare standard

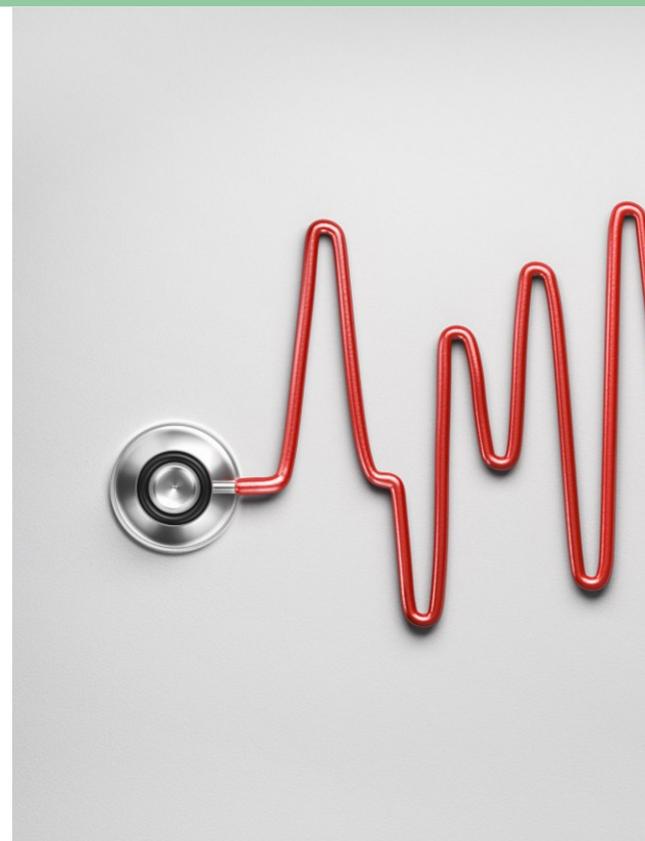


Z-CERT NIS2 in the Netherlands





Z-CERT NIS2 in the Netherlands





Z-CERT Annual threat report



✓ Quarterly

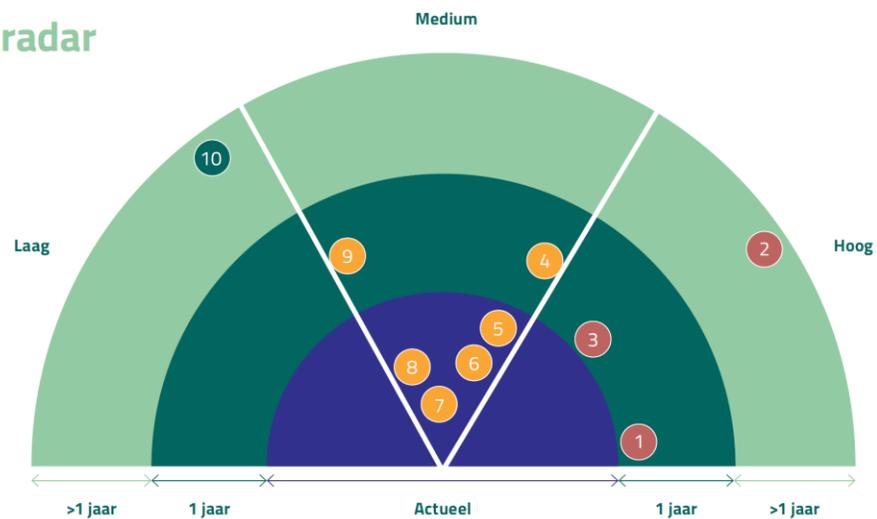
✓ Yearly





Z-CERT Threat Radar

Dreigingsradar



- | | |
|---|--|
| 1 Ransomware of afpersen met datalekken | 6 Credential phishing |
| 2 Spionage (onderzoek) | 7 Insider threats |
| 3 Ransomware of afpersen met datalekken bij leverancier | 8 Financiële fraude |
| 4 DDoS bij leverancier | 9 DDoS |
| 5 Malware | 10 Spionage (reguliere zorginstellingen) |

Lees ook de uitgebreide uitleg over de radar op pagina 90.



European Health ISAC Project proposal

Strengthening Cyber Resilience for EU Health



European action plan
on the cybersecurity of hospitals
and healthcare providers
(15 January 2025)

Call for Proposals
DIGITAL-ECCC-2025-DEPLOY-
CYBER-08-CYBERHEALTH

Projects
30 mln in co-funding



European Health ISAC
Join us!



Consortium



- Assistance Publique - Hôpitaux de Paris
- Brest University Hospital
- Danish Health Data Authority
- Hospices Civils de Lyon
- Hôpital Universitaire de Bruxelles
- Stichting Z-CERT





EUROPEAN
AGEING
NETWORK

Please MUTE



When not speaking

We care...
since 1989
www.ean.care



PROGRAMME

NIS2 and Social Services Experiences from EAN Member States

- **The Netherlands** – Richard Plug (Z-CERT)
- **Czech Republic** – Miroslav Kvapil (Lexnova)
- **France** – Philippe Passis & Thomas Aczel (Ressourcial)
- **Austria** – PPT of Lebenswelt Heim Bundesverband by Jiří Horecký
- **Q&A**

16 March 2026, 13-14 CET

Webinar



EUROPEAN
AGEING
NETWORK

Webinar



NIS2 in Czechia PRACTICAL IMPLICATIONS

Author:
Miroslav Kvapil MSc.

Date: March 16, 2026

We care...
since 1989
www.ean.care

NIS2 Implementation in Czechia

Supporting social service providers with practical NIS2 implementation.

- Cooperation with the **Association of Social Service Providers**
- Focus on **practical cybersecurity implementation for regulated entities**

Goal of the presentation:

- Share our **practical experience implementing NIS2 in the Czech social services sector.**

Legislation

European framework

- The **NIS2 Directive** significantly expands cybersecurity obligations across the EU.
- The directive now covers sectors providing **essential or sensitive services**, including **healthcare**.

Czech implementation

- NIS2 is transposed mainly through:
 - **Cybersecurity Act No. 264/2025** - Implementing regulations defining:
 - regulated services
 - lower vs. higher regulatory regimes.

Key change

- Thousands of new entities fall under cybersecurity regulation.
- Social service providers delivering healthcare services are newly included.

Management implication

- Cybersecurity is no longer only a technical issue.
- **Statutory management is legally responsible** for cybersecurity governance.

Basic Obligations Under NIS2

1. Registration of regulated service

- Organizations must **register their regulated service** with the national cybersecurity authority (NÚKIB).
- Registration is required once the organization meets the criteria defined by the law.

2. Incident reporting

- Organizations must **report significant cybersecurity incidents** to the competent authority within defined timelines.

3. Management responsibility

Senior management is responsible for:

- Approving cybersecurity measures
- Ensuring sufficient resources
- Overseeing the effectiveness of security controls.

4. Implementation of security measures

- Organizations must implement security measures covering areas such as:
- risk management
- access control and identity management
- protection of networks and information systems
- incident detection and response
- business continuity and backup management.

Starting Point

Where social service providers usually start

- In practice, most social service providers begin with very limited cybersecurity maturity.

Starting Point Situation

- Very limited attention to cybersecurity or IT as such
- Cybersecurity handled only by external IT support
- No formal information security management system
- Lack of risk management or asset inventory
- Limited documentation and governance

Typical Vulnerabilities

- Phishing and human-factor attacks
- Insufficient (non-existent) backup testing
- Unsecured IoT devices (cameras, smart devices, building systems)
- Employees using private email or cloud services.

Main Challenges

- Limited internal IT expertise
- Limited budgets
- Complex legal requirements
- Dependence on external IT suppliers
- Need to educate management.

How We Proceed

Services supporting NIS2 compliance

Our approach focuses on **practical implementation**, not just formal compliance. We create new SHARED standard in social service sector.

Cybersecurity Audit

- Evaluation of the current state
- Mapping against legal requirements
- Identification of priority risks.
- Definition of the optimization steps
- Optimization roadmap

Governance & Documentation

- Cybersecurity policies
- Risk management framework
- Incident response procedures
- Asset and supplier management.

Cybersecurity manager (outsourced role)

- Management and coordination of security activities
- Communication with regulators.

This allows smaller organizations to meet legal requirements without building internal security teams.

Training

- Staff cybersecurity awareness
- Phishing prevention
- Management training.

Lessons Learned from Implementing NIS2

Management awareness is the biggest challenge

- Cybersecurity has historically been seen as an IT issue.

Small organizations need practical solutions

- Complex frameworks must be translated into simple operational steps.

Human factor remains the biggest risk

- Training and awareness are critical.

Key Message

Cybersecurity under NIS2 should be understood as:

“Digital hygiene for organizations providing essential services.”

The goal is not to build complex security centers, but to ensure that organizations:

- understand their cybersecurity risks
- implement basic security measures
- maintain continuous management oversight.

NIS2 therefore represents a shift from IT security to organizational governance.

For more insights and experience SWAP
KEEP IN TOUCH

Miroslav Kvapil MSc.
Kvapil@Lexnova.cz

EAN partners



Helps. Cares. Protects.



EMPOWERING MOVEMENT





EUROPEAN
AGEING
NETWORK

Please MUTE



When not speaking

We care...
since 1989
www.ean.care



PROGRAMME

NIS2 and Social Services Experiences from EAN Member States

- **The Netherlands** – Richard Plug (Z-CERT)
- **Czech Republic** – Miroslav Kvapil (Lexnova)
- **France** – Philippe Passis & Thomas Aczel (Ressourcial)
- **Austria** – PPT of Lebenswelt Heim Bundesverband by Jiří Horecký
- **Q&A**

16 March 2026, 13-14 CET

Webinar



EUROPEAN
AGEING
NETWORK



NIS 2 - France

Webinar



Laurent ACZEL
Philippe PASSIS

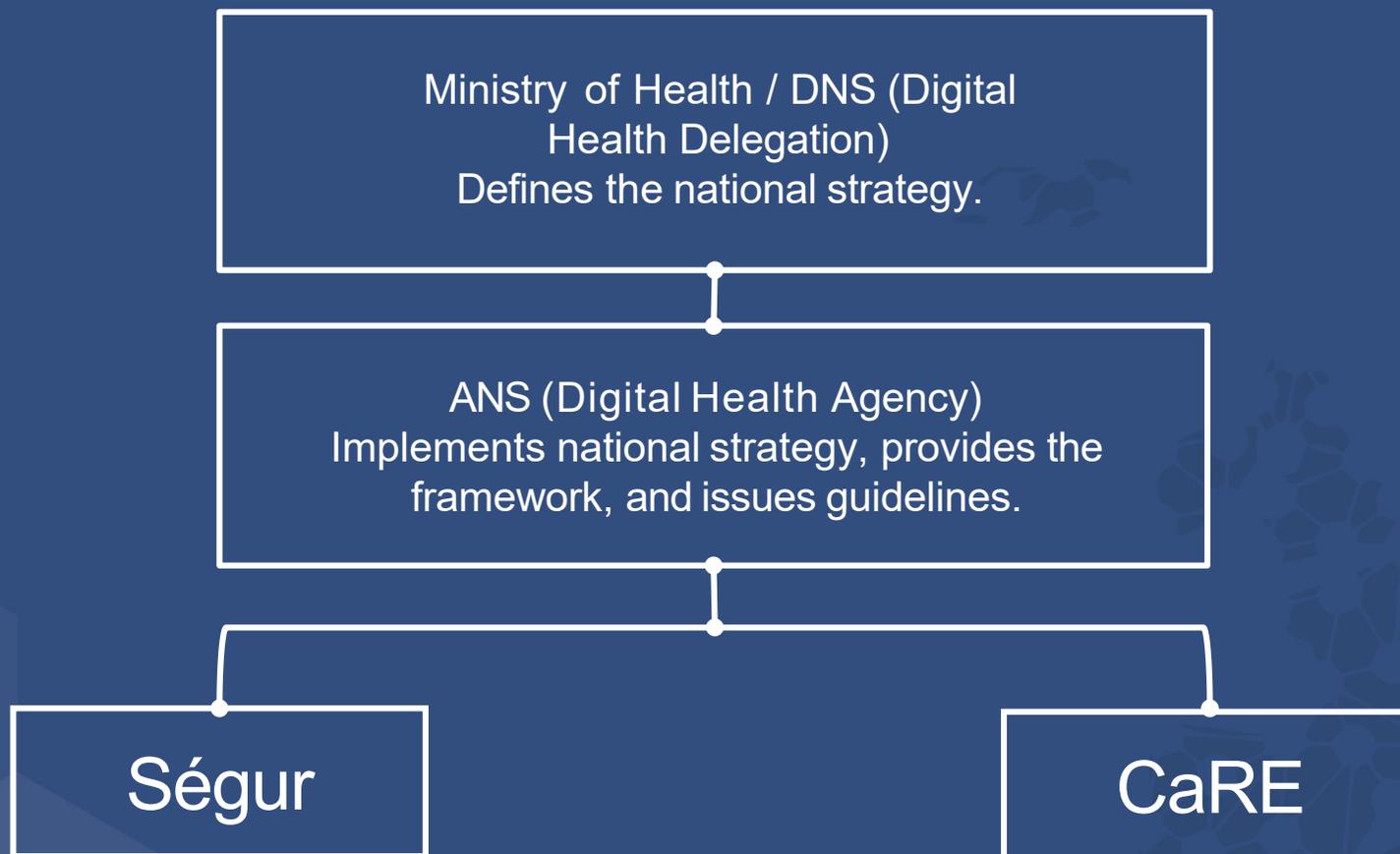
We care...
since 1989
www.ean.care

March 16, 2026

NIS2 implementation

Context & actors in France

How the Ministry of Health and its agencies architect the digital foundation for medical-social services.



The NIS2 Directive has not yet been transposed into French national law.

Specific, actionable global programs driving digitalization across medical and medical-social fields.

NIS2 implementation

Context & actors in France

The Multi-Year Push for Digital Maturity

Launch of the digital hospital environment program, accelerated by the COVID crisis and feeding into the broader Segur digital initiative.

2019 – Hop'en Program

Focus on tooling the medico-social Information System with unique shared medical records, secured health messaging, and software standardization.

2021 - Interoperability

Implementing secured applications to manage computerized user files, heavily driven by the **HAS (High Health Authority) regulatory and control certification program.**

2022/2023- Certification & Security

Upgrading the hospital and medico-social fields from basic digital environments to secure, certified ecosystems

The medico-social sector has only recently been integrated into national digital transformation policies, following the COVID-19 (SARS) crisis.

NIS2 implementation

Context & actors in France



Dual Pillars of National Cybersecurity Governance

Entities directly attached to the Prime Minister's Office secure digital systems of interest to the nation.

Standards & Rules

ANSSI

(National Agency for Information System Security)



Core Function: Produces technical standards, guidelines, and rules for IS administration.

Key Takeaway: ANSSI's recommendations are the national benchmarks. Any organization—public, private for-profit, or non-profit—must apply these NIS2 recommendations.

Operational Defense

CERT-FR

(French Computer Emergency Response Team)



Core Function: Governmental entity ensuring operational implementation of digital defense.

CERT Santé (Health)

(maintained by ANS)

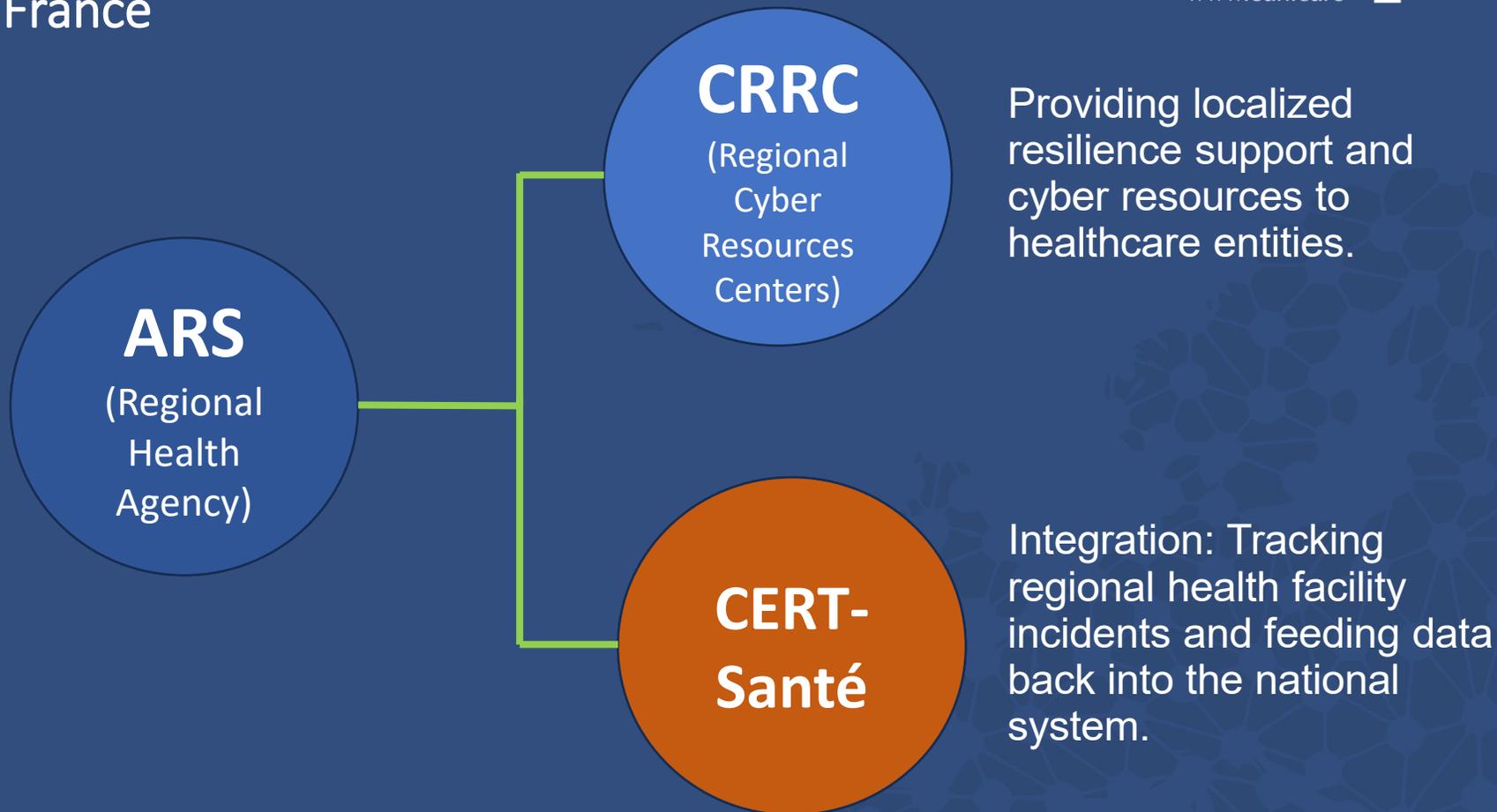
Dedicated specifically to the follow-up of incidents in health facilities.

NIS2 implementation

Context & actors in France



The central organizing body supporting institutions within their specific regional territory.



Translating National Defense into Regional Support
Empowering local health networks to build resilience against cybercrime

NIS2 implementation

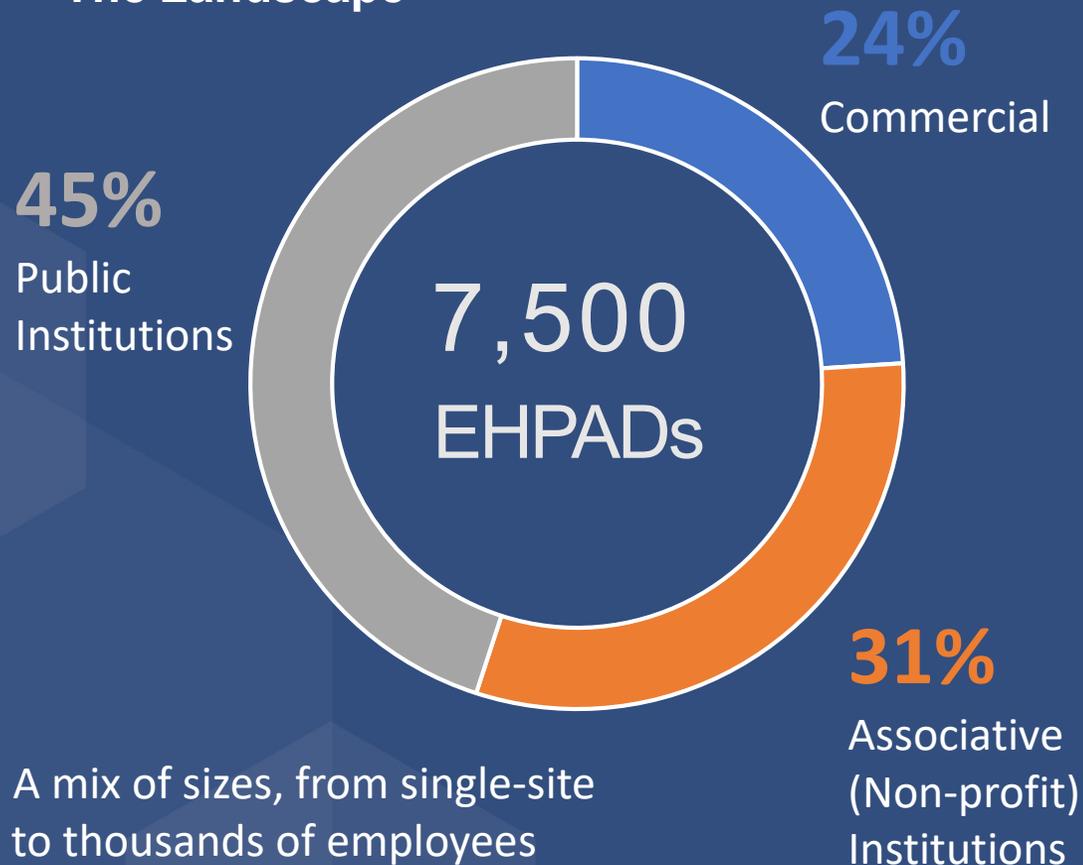
Medico-social sector in charge of the elderly



The Ground Reality of Elderly Care Facilities

7,500 highly fragmented institutions facing a structural IT resource deficit.

The Landscape



The Core Challenge

High focus on patient / accompanied person care

Low financial capacity and low supervision of IT, purchasing, and contracting



NIS2 implementation

Medico-social sector in charge of the elderly

State-Provided Toolkits for Transformation

How the ANAP agency equips medical-social governance to manage the effort of change.

To support social and health organisations lacking internal skills, the state (ANAP) provides visibility and arbitration elements through frameworks and tools



Maturin SMS

The official digital maturity framework tailored specifically for social and medico-social structures



Purchasing guides

Standardized recommendations and guides to safely procure external IT and cyber services

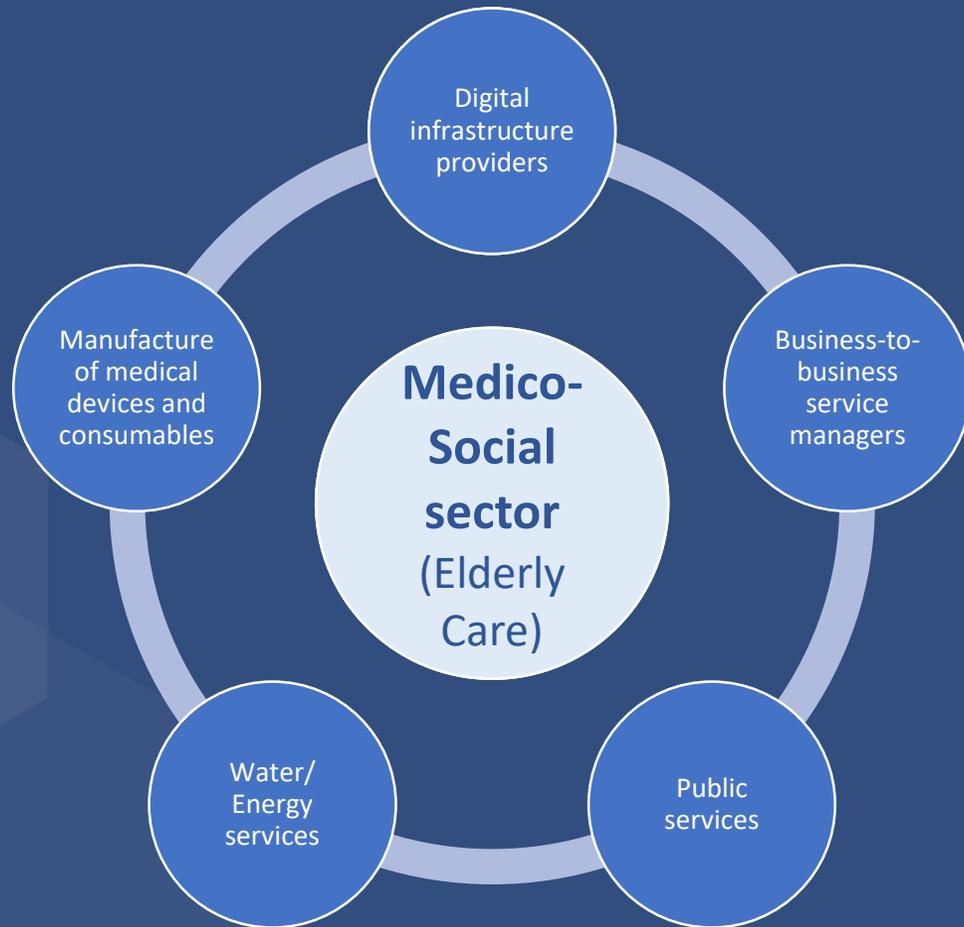


Mapping Tools

Methodological tools required to « urbanize » and map out existing complex information systems

NIS2 implementation

Some perspectives



Site-Specific Analysis :

Risk analysis must be carried out locally for each individual site based on these exact dependencies

Acculturation

The existing culture is not inherently risk-oriented. A gradual acculturation process is required to build robust, compliant services

Mapping Systemic Risk and Cultural Acculturation

NIS2 mandates site-specific risk analysis across all critical dependencies.

Thanks for your attention.

www.ressourcial.fr

contact@ressourcial.fr

EAN partners



Helps. Cares. Protects.

ARJO

EMPOWERING MOVEMENT





EUROPEAN
AGEING
NETWORK

Please MUTE



When not speaking

We care...
since 1989
www.ean.care



PROGRAMME

NIS2 and Social Services Experiences from EAN Member States

- **The Netherlands** – Richard Plug (Z-CERT)
- **Czech Republic** – Miroslav Kvapil (Lexnova)
- **France** – Philippe Passis & Thomas Aczel (Ressourcial)
- **Austria** – PPT of Lebenswelt Heim Bundesverband by Jiří Horecký
- **Q&A**

16 March 2026, 13-14 CET

Webinar



EUROPEAN
AGEING
NETWORK



NIS2

Austrian situation

Webinar

Lebenswelt Heim Bundesverband

2026/03/16

We care...
since 1989
www.ean.care

General level of IT preparedness

- Wide range from very well prepared to completely unprepared
 - esp. larger organisations are well prepared: WiFi, software based documentation, speech recognition, mobile devices, electronic data transmission...
 - esp. smaller organisations have no facilities at all or less facilities
- Differences due to
 - federal laws and federal authorities
 - size of organisation
 - financial possibilities of organisations

NIS2 legislation

- corresponding law was discussed in Austria in Aug. 2024, but not passed
- currently no law to transpose the EU directive
- current legal interpretation:
 - NIS2 refers to directive 2011/24/EU to define the health care sector
 - 2011/24/EU explicitly excludes nursing homes
 - Austrian draft law excludes nursing homes
 - -> nursing homes are not effected by the NIS2
 - -> providers of further health services are effected; this affects only a few care organisations in Austria

Financing of cybersecurity sector

- costs are usually totally covered by the organisation itself
- in certain cases government funding possible
- in certain cases and certain federal states grant funds available

Thanks for your attention.

EAN partners



Helps. Cares. Protects.



EMPOWERING MOVEMENT





EUROPEAN
AGEING
NETWORK



QUESTIONS & ANSWERS

Webinar



We care...
since 1989
www.ean.care

Thanks for your participations.
See you next time 😊

EAN partners

