We are working for the good of the Internet

NIS 2
What you need to know

Fredrik Lindeberg PhD, Security Expert

The good, the Bad and the Ugly

NIS2 introduction

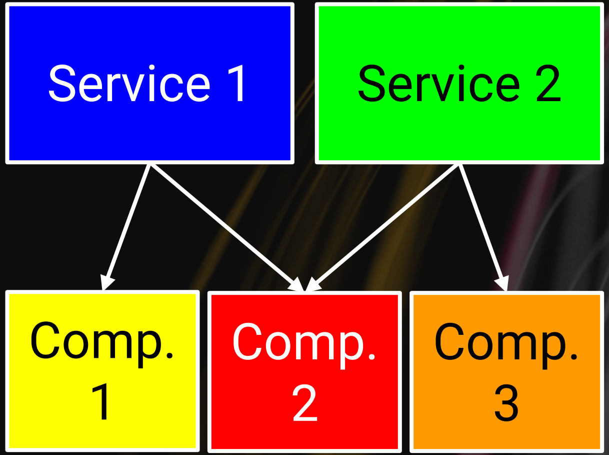
- Covers 15 sectors
  - Infrastructure to public administration to research
- Essential ("väsentliga") entities
  - Infrastructure (incl digital infrastructure), finance, public administration etc
    - incl. DNS, electronic communications networks and services, etc
  - Wider provisions for governmental oversight, higher penalties for non-compliance, etc
- Important ("viktiga") entities
  - E.g. services, goods and research
  - Oversight only after incident / event, lower penalties for non-compliance, etc

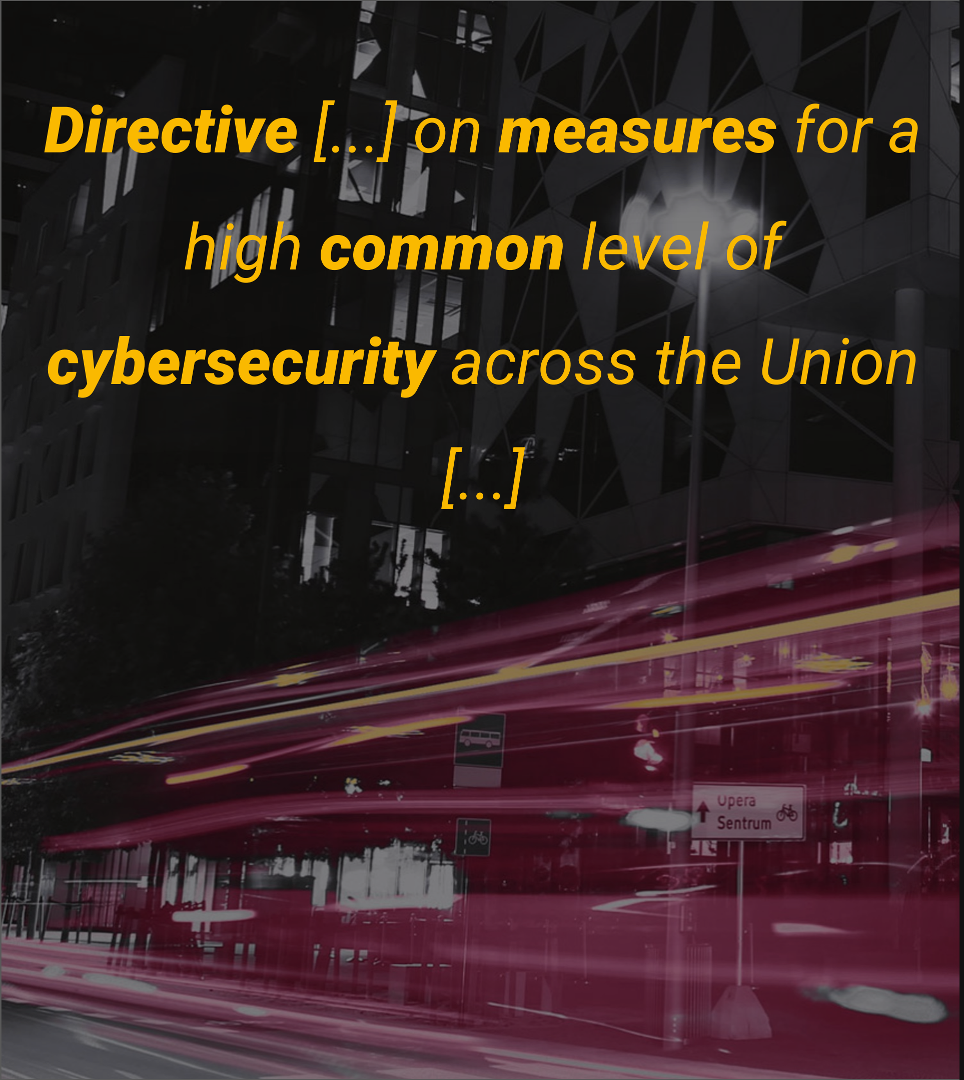
NIS, NIS2, Sweden and Netnod

- NIS(1) covers a subset of Netnod DNS services (e.g. not root servers)
- NIS2 expected to cover subset of Netnod IX and DNS services
  - *However, NIS2 covers the **entire legal entity** except where subsidiary to other laws*
  - Netnod is an **essential** entity (current Swedish draft law)
- Swedish draft law for NIS2 released 5 March 2024
  - Consultation until 28 May 2024
- Electronic communication networks and publicly available electronic communications services covered even if not established in Sweden
  - *ne bis in idem*, but is limited to sanction / consequence, not oversight 1 kap, 5 § / p. 37 of draft law

Netnod and NIS2

- Successfully worked with RIPE NCC to ensure DNS root name server system not part of NIS2
- Where possible note the potential pitfalls of current and suggested regulation
  - esp. concerning ex ante process regulation, and
  - aggregates of wholesale services in supply chains





***Directive** [...] on **measures** for a high **common** level of **cybersecurity** across the Union [...]*

***directive** -*
actual implementation in member states

***measures** -*
“something should be done”

***common** -*
“the same thing [should be done]”

***cybersecurity** -*
*“the activities necessary to protect network and information systems, the users of such systems, and other persons affected by **cyber threats**”*
(Regulation (EU) 2019/881)

Directive

Approved by EU-parliament

Dec 2022

Guidelines

Approved by EU-commision and ENISA

Continuously

Laws

Approved by member states

By Oct 2024

The Good

Perspectives in which NIS2 makes perfect sense

Bureaucracy (🏛️)

með lögum skal land byggja en
með ólögum eyða

society should build on law;
without, it perishes

— Njáls saga, proverb

Think like a bureaucrat 101

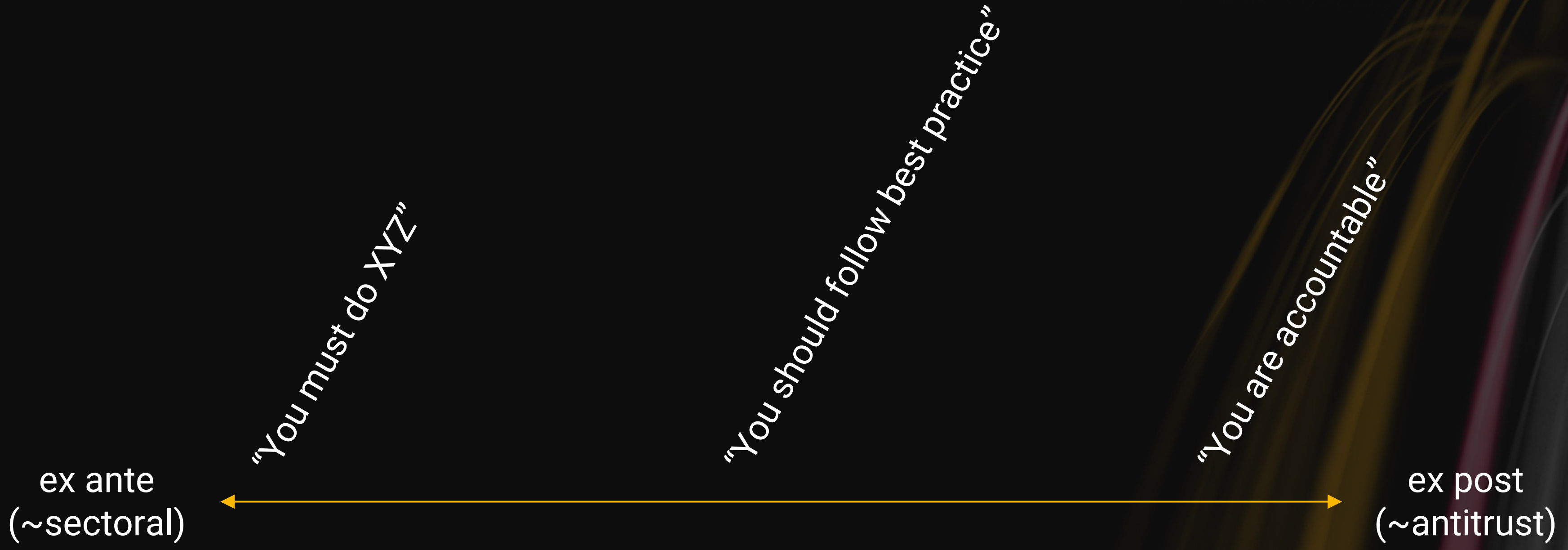
Possibility of sanctions, order, rule of law, jurisdictions …

Prevention of degenerate behaviour through law and order

Public policy 101 - the bureaucrat’s toolbox

- The public policy toolbox (in most cases) consists of two main tools:
  - Regulation
    - Rules that must be followed
    - ex ante legislation describe what is allowed / not allowed explicitly
    - ex post regulation focus on management of liabilities after events have occurred, such as competition / anti-trust after market failure
  - Financing
    - Direct financing of functions / infrastructure / services / …
    - Procurement of services

Regulation - not black and white



ex ante
(~sectoral)

“You must do XYZ”

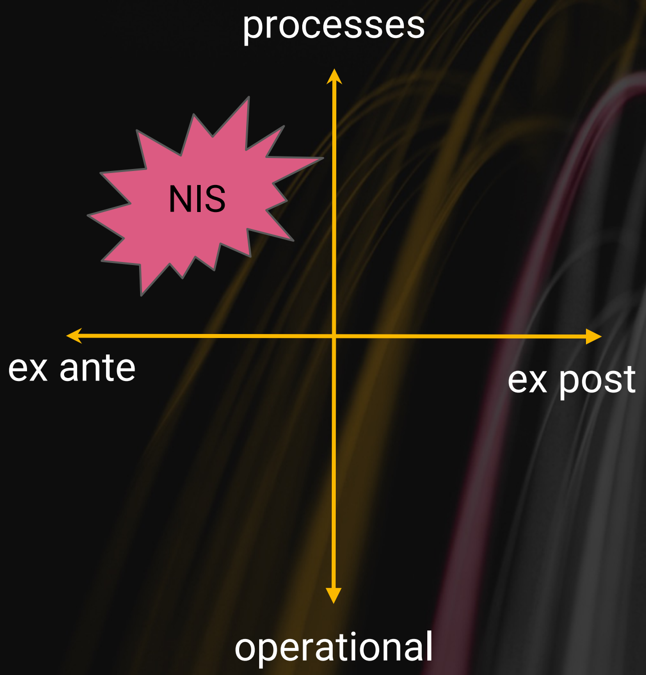
“You should follow best practice”

“You are accountable”

ex post
(~antitrust)

NIS2 - ex ante regulation

- Describe clear process measures you are held accountable to:
  - *cybersecurity risk-management measures and reporting obligations for entities*
  - *rules and obligations on cybersecurity information sharing*
- High level measures relate to structure and order from a cybersecurity perspective



The Bad

The potential pitfalls of NIS2

NIS2 does (primarily) not concern operational cybersecurity capabilities

Process measures in NIS2 concern high level risk management and related processes

NIS2 actors are held accountable for following high level process requirements

Actors are **not** held accountable for damages caused or failing (by NIS)

CRA and PLD put emphasis on liability

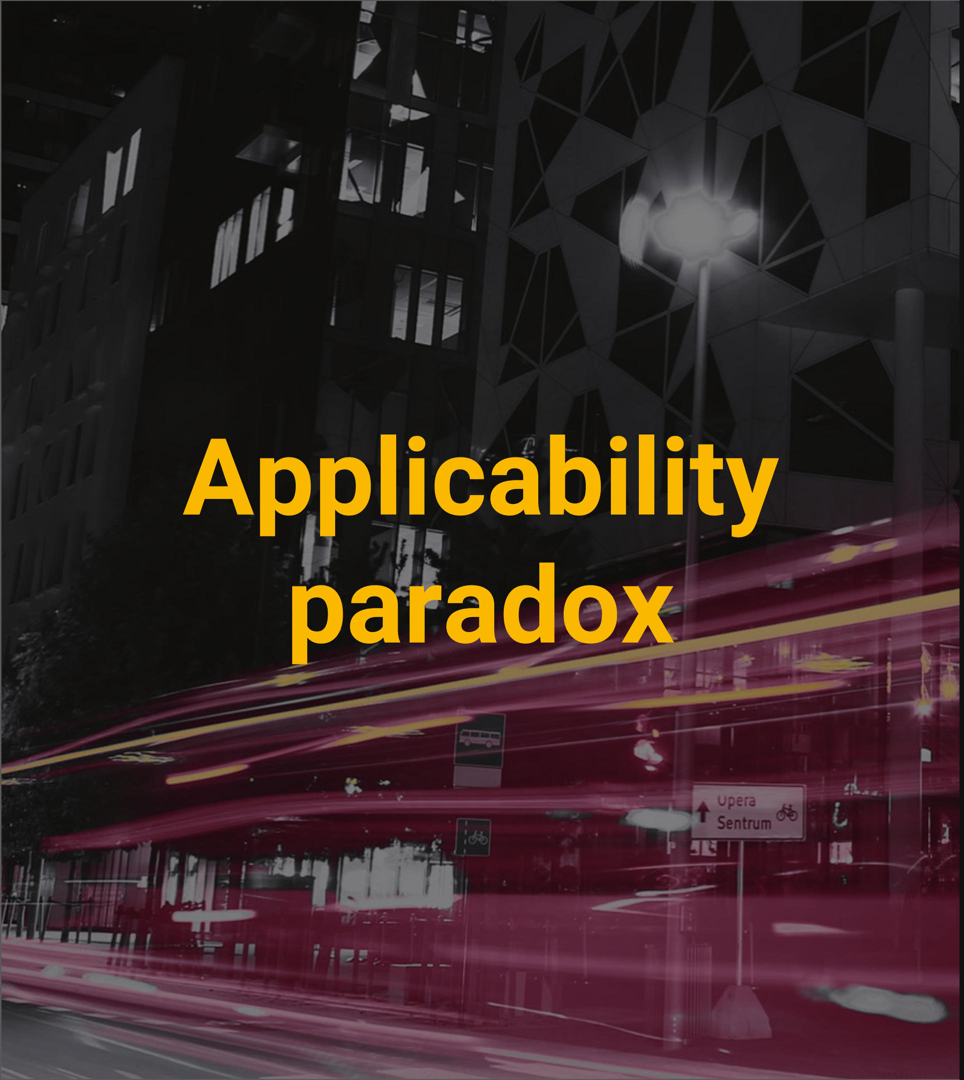
The scarce resource problem

- Most organizations have limited resources
  - Additional pressure on high level processes and administration likely to divert resources from operations, or
  - Increase costs for end-user

- Structure and order is not the same as operational capabilities

The Ugly

NIS2 focuses on process rather than operational cybersecurity



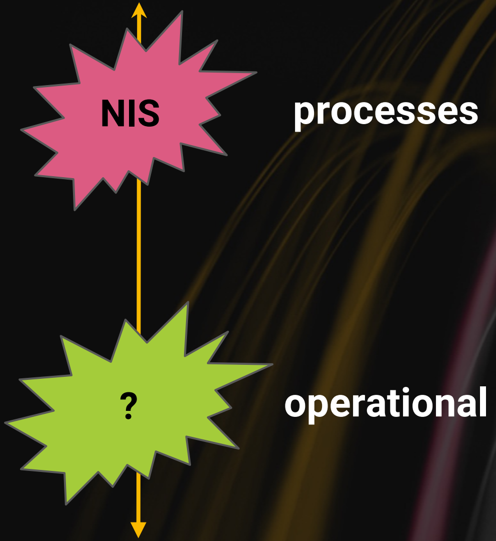
Applicability paradox

It is possible to be NIS2 compliant but still have a very low level of operational cybersecurity

It is possible to **not** be NIS2 compliant while having a very high level of operational cybersecurity

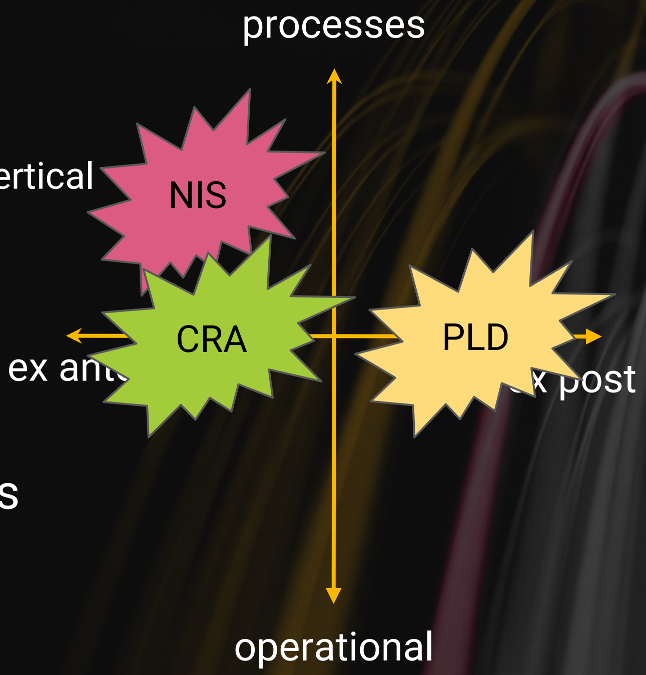
Applicability paradox

- NIS(1) oversight and regulatory requirements
  - governmental oversight done on documentation and administration, not operational capabilities
  - How good is a plan when you get punched in the face?
- Operational cybersecurity
  - Not necessarily part of oversight and regulation
  - Matters when the shit hits the fan



What should you do?

- Take a step back and reflect
  - Let the dust settle, then implement measures
  - Cybersecurity is part of *everything* today, not a separate vertical
- Think about high level measures and reporting
  - Other directives with different foci
- You need to allocate resources for operational cybersecurity as well, not only high level measures
  - Operational cybersecurity is hard, really hard
  - Plan for operational effect where possible
  - Dependencies are a good start, what are you **dependent on**?



What is next in context of NIS2?

- Member states implement directive by 17 October 2024
  - Draft law available in some, not all, member states
  - Read it, comment if possible, especially on your area of expertise
  - Ask around about NIS2!
- EU Commission to review the functioning of the directive by 17 October 2027
  - *How will they do this?*

Want to talk?

Find me!

Current relevant policy topics:

- Cyber Resilience Act
- **Product Liability Directive**
- NIS(1)/2
- European Electronic Communications Code
  - Digital Networks Act
  - EU White paper: “How to master Europe’s digital infrastructure needs?”

Thanks for listening!