2024-11-20
KCD Denmark

From Neglected to Necessary

Securing Kubernetes Under NIS2

```
$ kubectl auth whoami
Groups [Kubernetes GDPR NIS2 nerd]
```

Cristian Klein, PhD

Product Owner of Welkin

Data Protection Officer

@Elastisys | Sweden

Hi! I’m Welkin! The Kubernetes platform for software critical to our society.

elastisys

Cloud Native Security Made in Sweden

We support organizations throughout Europe in accelerating their innovation with open source, cloud native technology.

elastisys.com

Managed Service

Self-Managed

Consulting

Training

You will be affected by NIS2

NIS2: You have two choices

Get involved

Influence the security policies you get. Work on **meaningful** security measures.

Wait and see

Receive whatever security policies you get. Work on **meaningless** security measures.

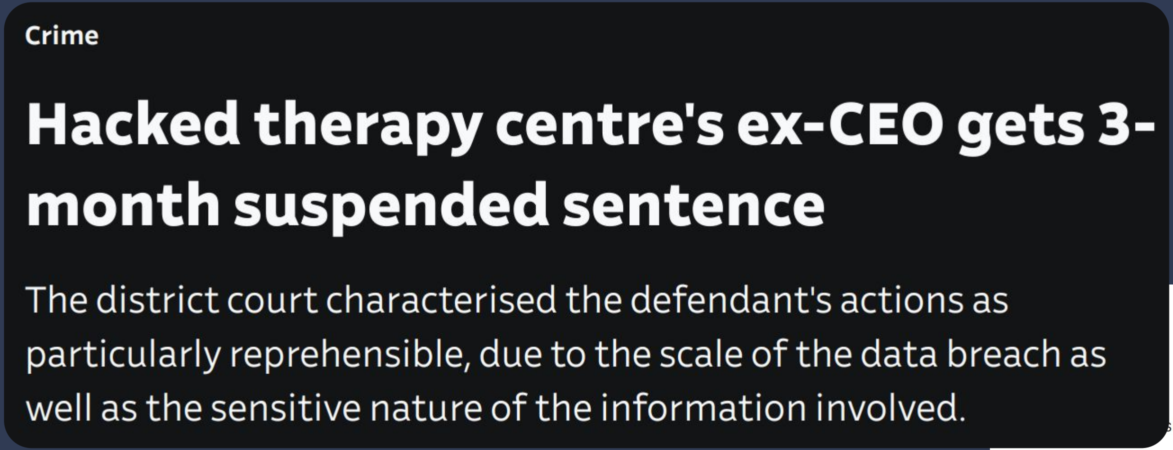
Think about your healthcare provider 🤔

How would you feel if…

… your patient journal leaks … and your needed to pay ransom for privacy?

… your friend, a dev at the provider, can change your patient journal?

… you are unable to book an appointment for 24 hours?



Crime

Hacked therapy centre's ex-CEO gets 3-month suspended sentence

The district court characterised the defendant's actions as particularly reprehensible, due to the scale of the data breach as well as the sensitive nature of the information involved.

TECHNOLOGY

Russian hackers down sites of several Danish traffic organisations

Military

Seven in ten Danes 'fear attack' on critical digital infrastructure

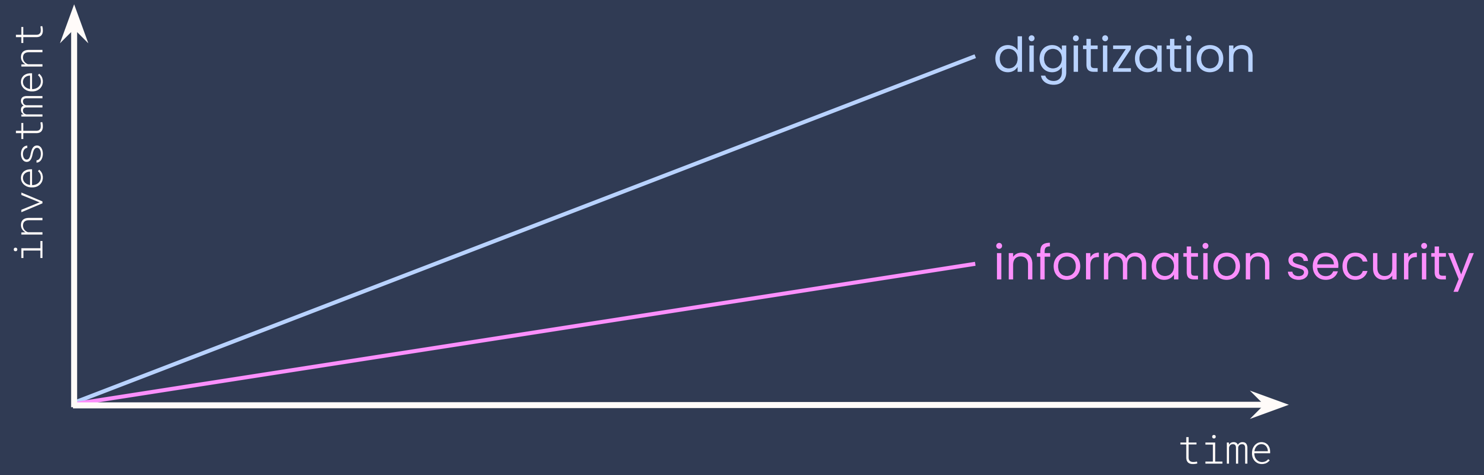
Michael Barrett - michael@thelocal.dk
Published: 2 Jul, 2024 CET. Updated: Tue 2 Jul 2024 16:08 CET

The IT attack in Kalix: Back up copy saves employees' salaries

UPDATED DECEMBER 20, 2021 PUBLISHED DECEMBER 20, 2021

https://yle.fi/a/74-20027665
https://www.thelocal.dk/20240702/seven-in-ten-danes-fear-attack-on-critical-digital-infrastructure
https://cphpost.dk/2024-02-26/news/technology/traffic-websites-were-attacked-by-russians-on-sunday/
https://www.svt.se/nyheter/lokalt/norrbotten/kalix-kommun-backupkopia-raddar-de-anstalldas-loner

Why is this happening?



Why is security hard?

Two reasons:

1 | Funding gap

“Market forces” lead to security being chronically underfunded

2 | Knowledge gap

Asymmetry between attacker and defender

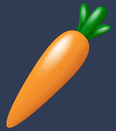
- Cyber attackers only need to find **one gap.**
- Defenders needs to mitigate **“all” security risks.**

What is the EU NIS2 Directive?

- Improvement of the NIS1 Directive
- **Directive** → Needs to be implemented in national law of each Member State (more on this later)

30,000 feet summary:

Close the "funding gap"
Fines of 2% total annual turnover



Close the "knowledge gap"
Essentially create a hierarchical DevSecOps loop (more on this later)

NIS2
Directive

Who is in scope of NIS2 … everyone?

Essential Entities since NIS 2016

- Energy
- Transport
- Banking
- Financial Market Infrastructures
- Health
- Drinking Water
- Digital Infrastructure
- Digital Service Providers

Additional Sectors since NIS2 2022

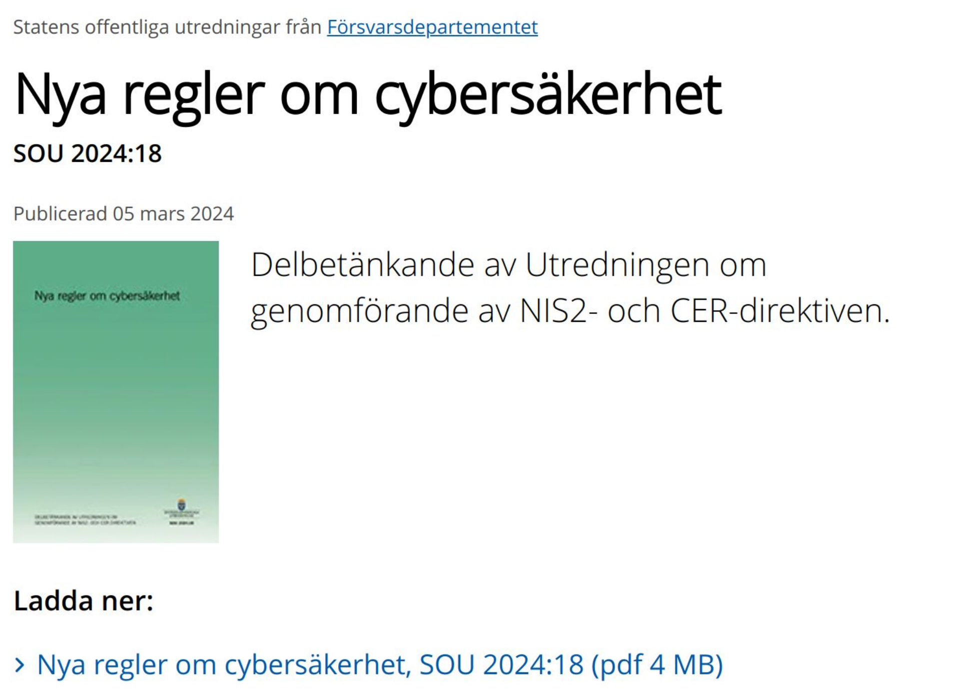
ADDED ESSENTIAL ENTITIES

- Waste Water
- ICT Service Management
- Public Administration
- Space
- Manufacturing

NEW

IMPORTANT ENTITIES

- Postal and Courier Services
- Waste Management
- Digital Providers
- Research
- Manufacture, production and distribution of chemicals
- Production, processing and distribution of food



Statens offentliga utredningar från Försvarsdepartementet

Nya regler om cybersäkerhet

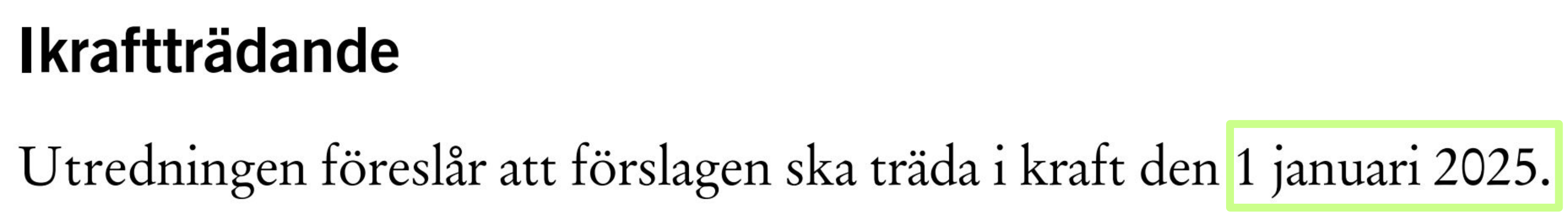
SOU 2024:18

Publicerad 05 mars 2024

Delbetänkande av Utredningen om genomförande av NIS2- och CER-direktiven.

Ladda ner:

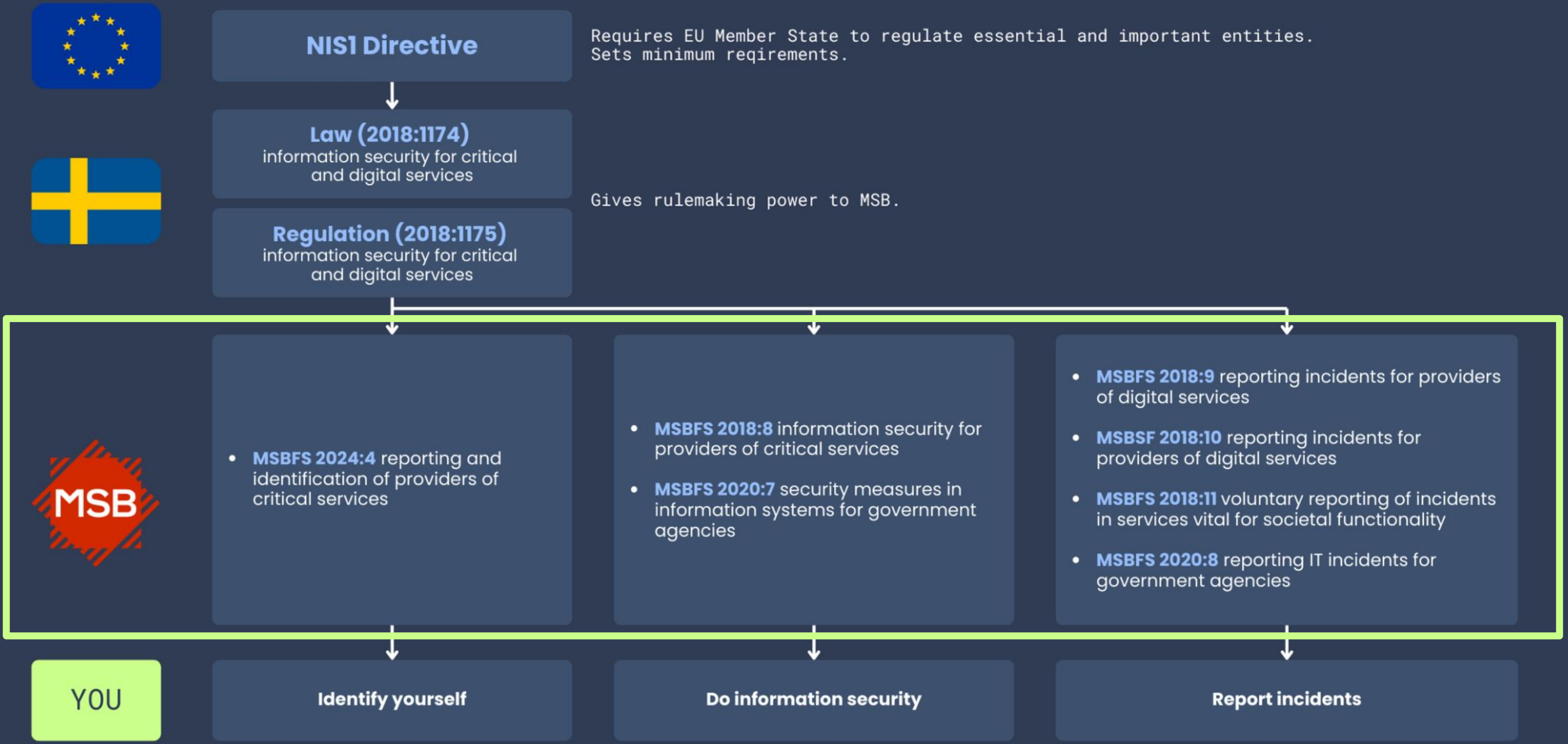
› Nya regler om cybersäkerhet, SOU 2024:18 (pdf 4 MB)



Ikraftträdande

Utredningen föreslår att förslagen ska träda i kraft den 1 januari 2025.

What do I need to do?



NIS1 Directive

Requires EU Member State to regulate essential and important entities.
Sets minimum reqirements.

Law (2018:1174)
information security for critical and digital services

Regulation (2018:1175)
information security for critical and digital services

Gives rulemaking power to MSB.

MSB

- **MSBFS 2024:4** reporting and identification of providers of critical services

- **MSBFS 2018:8** information security for providers of critical services
- **MSBFS 2020:7** security measures in information systems for government agencies

- **MSBFS 2018:9** reporting incidents for providers of digital services
- **MSBSF 2018:10** reporting incidents for providers of digital services
- **MSBFS 2018:11** voluntary reporting of incidents in services vital for societal functionality
- **MSBFS 2020:8** reporting IT incidents for government agencies

YOU

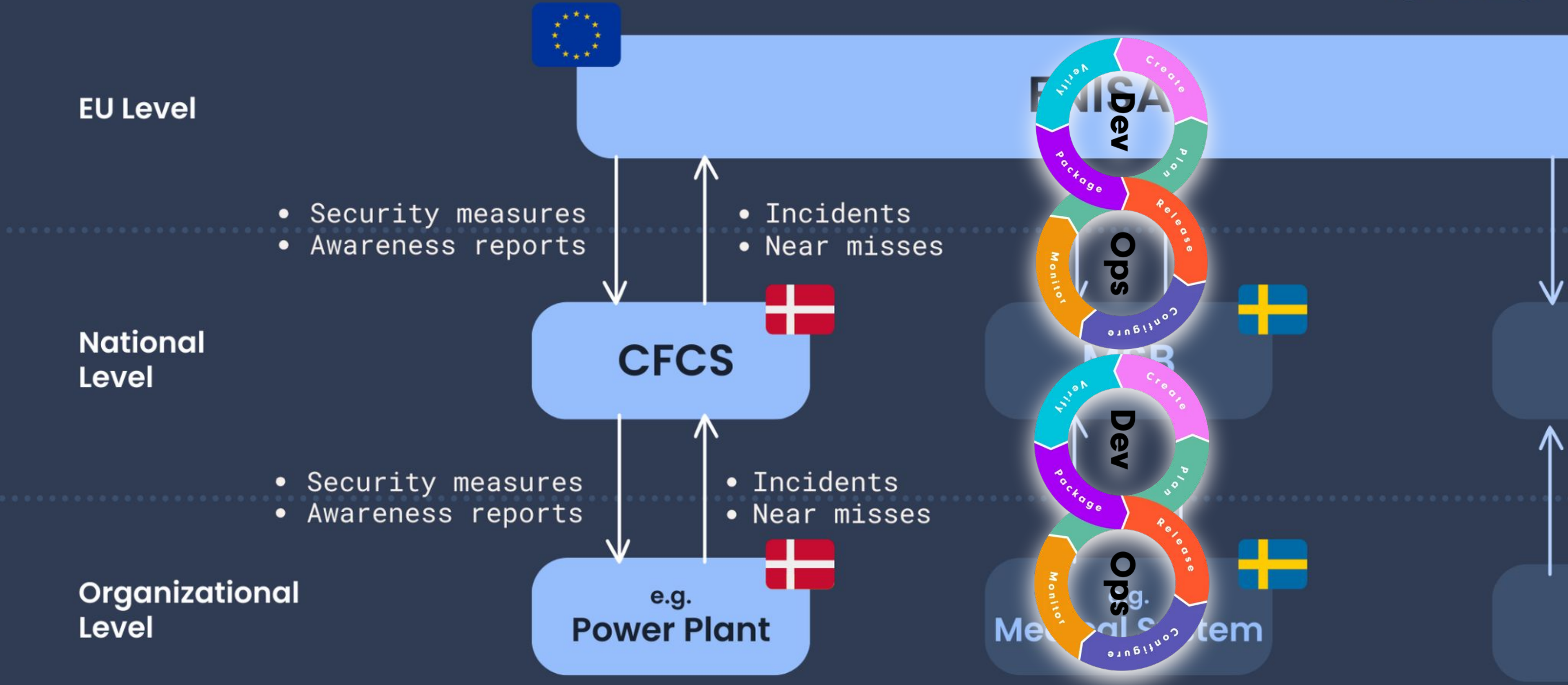
Identify yourself

Do information security

Report incidents

Hierarchical DevSecOps loop 🤔

Created by elastisys



EU Level

National Level

Organizational Level

- Security measures
- Awareness reports

- Incidents
- Near misses

CFCS

- Security measures
- Awareness reports

- Incidents
- Near misses

e.g.
Power Plant

Report(worthy) Incidents

Various rules precisely define what is a **report-worthy incident** for each industry sector.

- If ambulance service was somehow affected `(MSBFS 2018:9 7 kap. 1 § 2)`
- If a patient journal system is down for more than 2 hours `(MSBFS 2018:9 7 kap. 1 § 3)`
- Transportation: If 1000 users or a region of 10000 km^2 were affected for at least 1 hour. `(MSBFS 2018:9 4 kap. 1 § 1)`

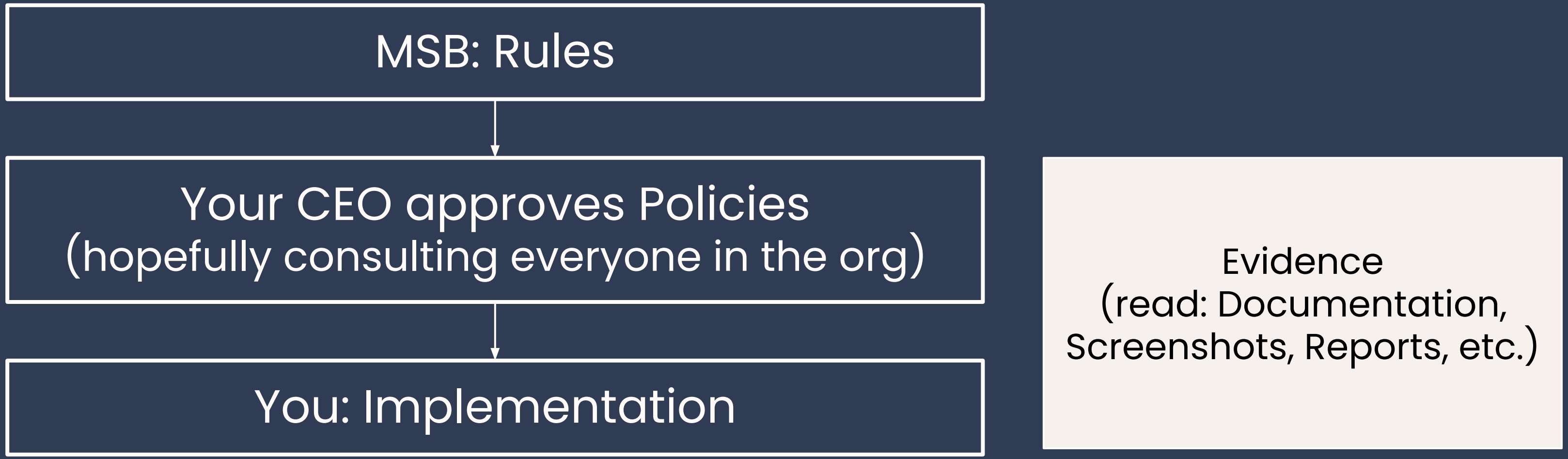
You need to **send in reports at quite a pace.**

- Initial report after 6 hours from the start of the incident;
- Interim report after 24 hours;
- Final report after 4 weeks.

Do Information Security! 🎉🥳

Caveat for software engineers

NIS2 sets requirements on Information Security **Management**



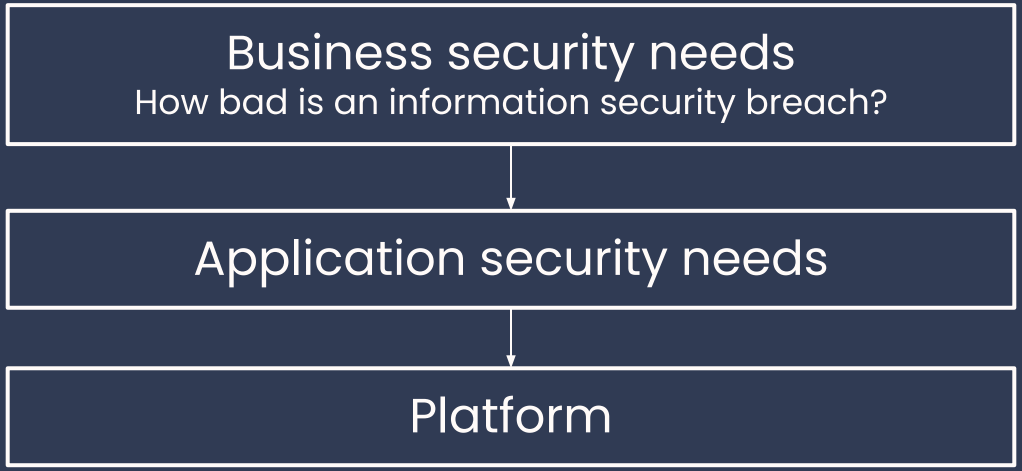
MSB: Rules

Your CEO approves Policies
(hopefully consulting everyone in the org)

You: Implementation

Evidence
(read: Documentation,
Screenshots, Reports, etc.)

Caveat for platform engineers



Business security needs

How bad is an information security breach?

Application security needs

Platform

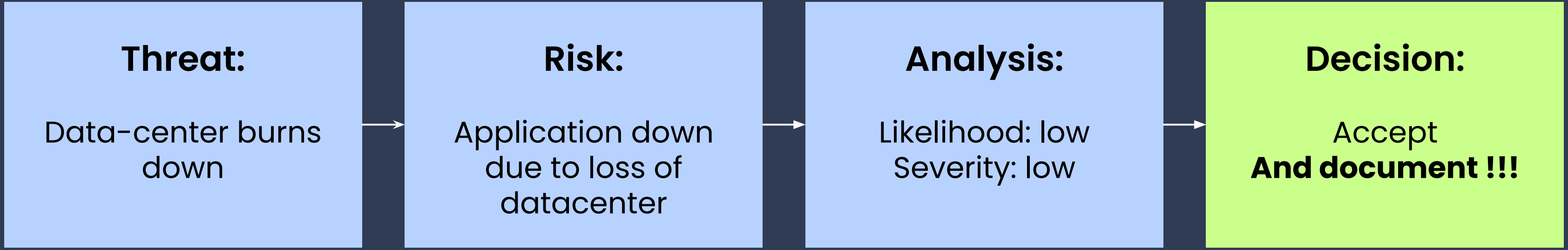
NIS2: Risk management

TL;DR:

1. Brainstorm on **things which can go wrong**
2. Assess **how bad they are**
3. Decide:
    - **Accept** → read: don't do anything, but **DOCUMENT THE DECISION (!)**
    - **Transfer** → make it someone else's problem
    - **Mitigate** → read: do something about it

What can you do about the risk?

- Take **technical**, **operational** and **organisational** measures



Threat:

Data-center burns down

Risk:

Application down due to loss of datacenter

Analysis:

Likelihood: low
Severity: low

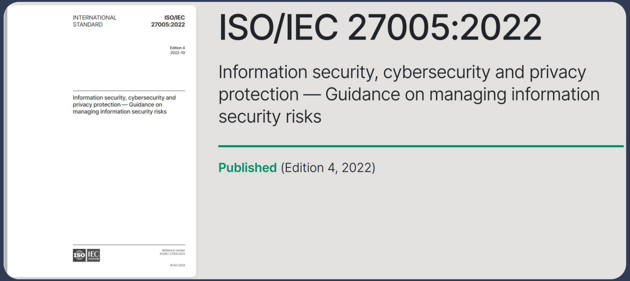
Decision:

Accept
And document !!!

ENISA THREAT LANDSCAPE 2024

July 2023 to June 2024

SEPTEMBER 2024



INTERNATIONAL STANDARD

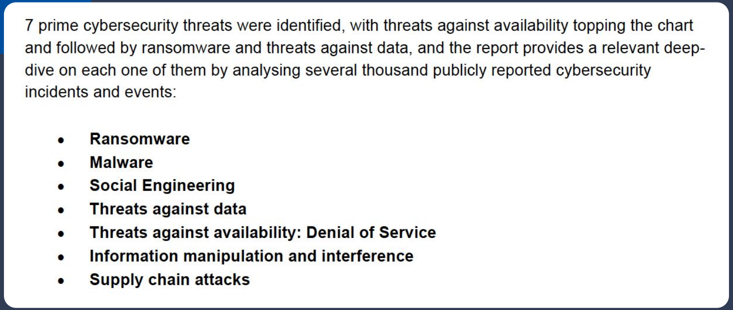
ISO/IEC 27005:2022

Information security, cybersecurity and privacy protection — Guidance on managing information security risks

ISO/IEC 27005:2022

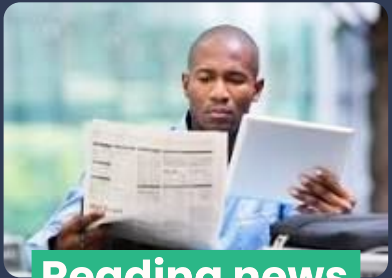
Information security, cybersecurity and privacy protection — Guidance on managing information security risks

Published (Edition 4, 2022)

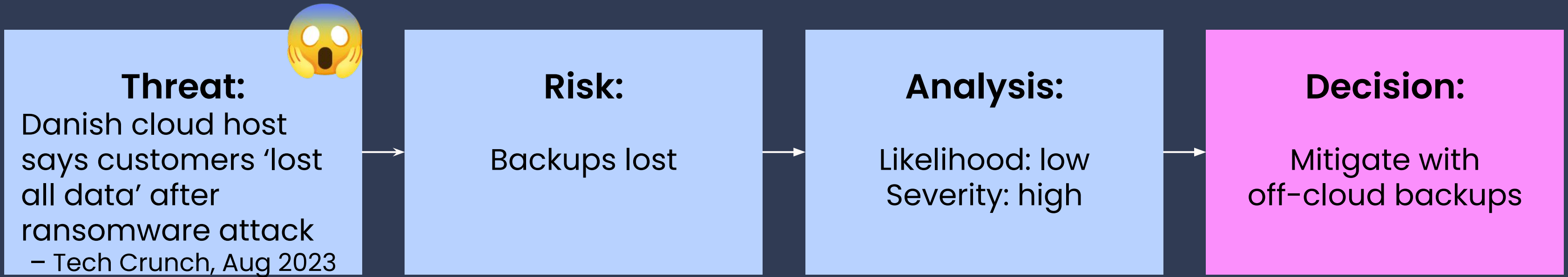


7 prime cybersecurity threats were identified, with threats against availability topping the chart and followed by ransomware and threats against data, and the report provides a relevant deep-dive on each one of them by analysing several thousand publicly reported cybersecurity incidents and events:

- **Ransomware**
- **Malware**
- **Social Engineering**
- **Threats against data**
- **Threats against availability: Denial of Service**
- **Information manipulation and interference**
- **Supply chain attacks**



Reading news.



Threat: 😱
Danish cloud host says customers 'lost all data' after ransomware attack
– Tech Crunch, Aug 2023

Risk:
Backups lost

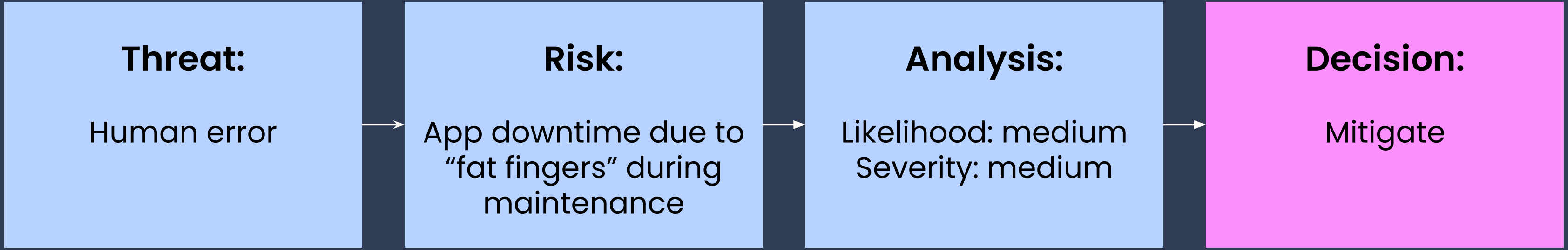
Analysis:
Likelihood: low
Severity: high

Decision:
Mitigate with off-cloud backups

Let each application team deal with it 💰🥵

OR

RCLONE VELERO 🙌🤑



Threat:

Human error

Risk:

App downtime due to “fat fingers” during maintenance

Analysis:

Likelihood: medium
Severity: medium

Decision:

Mitigate

Technical

Open Policy Agent

Kyverno

Operational

Staged rollout
(e.g., staging, production)

Organizational

Training
(CKAD)

NIS2 “Minimum Requirements”

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

IMPLEMENTING GUIDANCE

On **Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024** laying down rules for the application of Directive (EU) 2022/2555 as regards **technical and methodological requirements of cybersecurity risk-management measures**

with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

DRAFT FOR PUBLIC CONSULTATION

155 pages

* simplified from NIS2 Article 21(2)

NIS2 “Minimum Requirements” (1–5)*

1	**Information security** policy	
2	**incident handling**	fluentd Prometheus
3	**backup** management and **disaster recovery**	RCLONE VELERO
4	**supply chain security**	
5	**network security**	Kubernetes Network Policies Open Policy Agent

* simplified from NIS2 Article 21(2)

NIS2 “Minimum Requirements” (6–10)*

6	**vulnerability** management	aqua trivy
7	basic cybersecurity **hygiene** and **training**	CERTIFIED kubernetes SECURITY SPECIALIST
8	use of **cryptography** and **encryption**	CERT MANAGER
9	human resources security, **access control policies** and asset management	Kubernetes RBAC
10	**use of multi-factor authentication or continuous authentication solutions**	dex

* simplified from NIS2 Article 21(2)

Requirements and Implementation

🇸🇪 MSBFS 2020:7

(NIS1-era / public administration)

- Separate non-production from production environments
- Separate admin from non-admin access
- Do proper change management
- Have tamper-proof backups

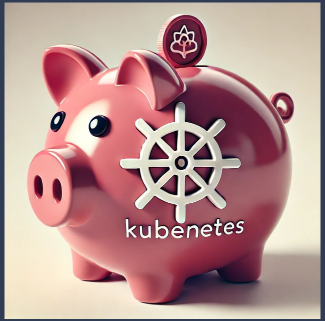
🇩🇪 BSI IT Grundschutz

APP.4.4 Kubernetes (Edition 2022)

- APP.4.4.A7 Separierung der Netze bei Kubernetes (S)
  - Use SecurityGroups and NetworkPolicies
- APP.4.4.A9 Nutzung von Kubernetes Service-Accounts (S)
  - Don’t use the “default” ServiceAccount
- APP.4.4.A11 Überwachung der Container (S)
  - Have startup, liveliness and readiness probes

Takeaways

- If you work with software, you'll be affected by NIS2
- NIS2 plugs the security funding gap and knowledge gap
- You can influence the security measure which you will have to implement.
- **You can help the organisation reduce compliance burden with Kubernetes and Cloud Native.**



"Kubernetes" misspelling courtesy of ChatGPT

Resources

- ENISA Threat Landscape 2024
- ENISA Implementation guidance on NIS 2 security measures
- Welkin NIS2 Overview
- All You Need to Know About NIS2
- NIS2: But what exactly do I need to do?

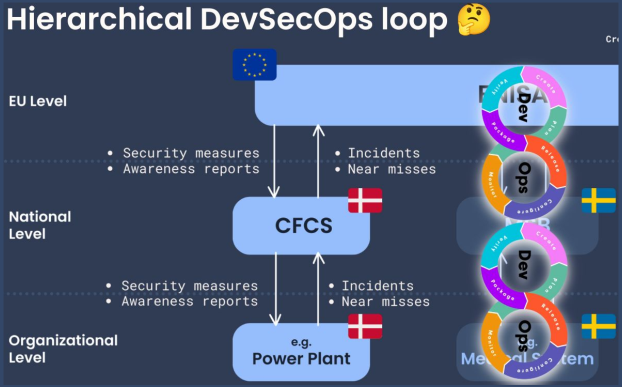
Thank you and happy to connect!

Cristian Klein, PhD

DPO and Product Owner
@Elastisys | Sweden

in [@cristianklein]

✉ [cristian.klein@elastisys.com]



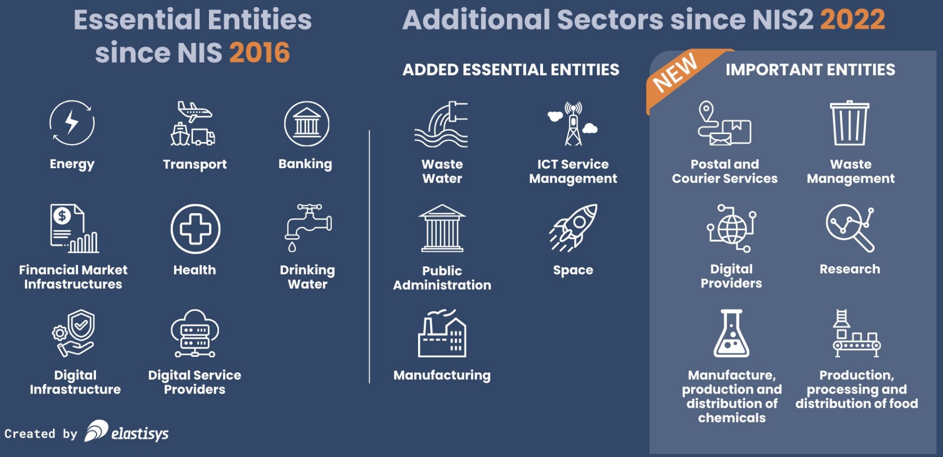
Hierarchical DevSecOps loop 🤔

- Security measures
- Awareness reports

- Incidents
- Near misses

- Security measures
- Awareness reports

- Incidents
- Near misses



Essential Entities since NIS 2016

Energy, Transport, Banking, Financial Market Infrastructures, Health, Drinking Water, Digital Infrastructure, Digital Service Providers

Additional Sectors since NIS2 2022

ADDED ESSENTIAL ENTITIES

Waste Water, ICT Service Management, Public Administration, Space, Manufacturing

NEW IMPORTANT ENTITIES

Postal and Courier Services, Waste Management, Digital Providers, Research, Manufacture, production and distribution of chemicals, Production, processing and distribution of food

Created by elastisys