NIS, NIS2, CER och Art 3

Skånelandsmöte

20220301

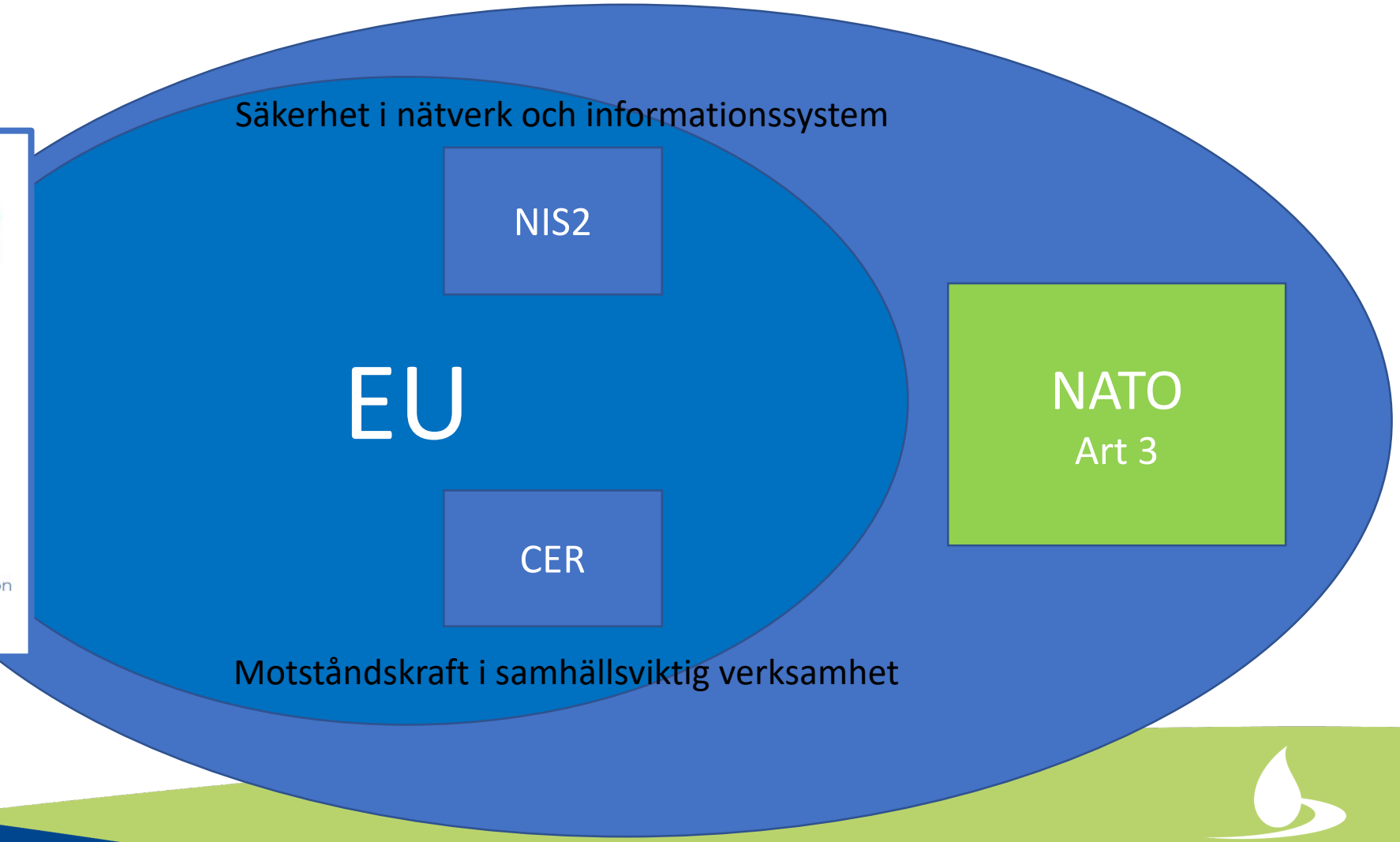
Henrik Kjellgren

Säkerhetsansvarig Laholmsbuktens VA

Laholmsbuktens VA

Resiliens, kontinuitet, driftsäkerhet

1. The NIS 2 Directive
2. The European Cyber Resilience Act
3. The Digital Operational Resilience Act (DORA)
4. The Critical Entities Resilience Directive (CER)
5. The Digital Services Act (DSA)
6. The Digital Markets Act (DMA)
7. The European Health Data Space (EHDS)
8. The European Chips Act
9. The European Data Act
10. European Data Governance Act (DGA)
11. The Artificial Intelligence Act
12. The European ePrivacy Regulation
13. The European Cyber Defence Policy
14. The Strategic Compass of the European Union
15. The EU Cyber Diplomacy Toolbox



Vad är NIS och NIS 2?

EU-direktivet för att skapa en mer enhetlig nivå för informationssäkerhet/cybersäkerhet över medlemsstaterna

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)"

Vad innebär NIS 2?

NIS ersätts med NIS2.

Hårdare och tydligare krav på att bedriva ett systematiskt informationssäkerhetsarbete

Kan (i stort sätt) omfatta alla typer av organisationer

Sanktionsavgift vid brist på efterlevnad

Träder i kraft oktober 2024

Nationell anpassning behövs

NIS2 = NIS + GDPR på steroider (?)

Vad är nytt jämfört med NIS?

Omfattar fler aktörer än tidigare

Mer detaljerade krav på säkerhetsåtgärder

Ledningen får ett tydligare (personligt) ansvar

Skärpta krav kring rapporteringsskyldighet vid incidenter som anses ha ”betydande” inverkan

Sanktionsavgifter delas ut om man inte lever upp till lagkravet

Sanktionsavgifter

Väsentlig entitet	Viktig entitet	Övrigt
Högst €10M	Högst €7M	Lägre belopp om överträdelsen
2% av global omsättning	1,4 % av global omsättning	Är ringa eller ursäktlig

Vilka omfattas av NIS2?

Samhällsviktiga tjänster inom:

- Energi
- Transport
- Bankverksamhet
- Finansmarknadsinfrastruktur
- Hälso-och sjukvård
- Leverans av och distribution av dricksvatten
- **Avloppsvatten + Gas**
- Digital infrastruktur
- Offentlig förvaltning
- **Rymd**

Digitala tjänster:

- Internetbaserad marknadsplats
- Sökmotorer
- Molntjänster

Väsentliga

Viktiga

Hur efterlever vi direktivet?

Säkerställa att ledningen tar ansvar

1. Risk analysis and information system security policies
2. Incident handling (prevention, detection, and response to incidents)
3. Business continuity and crisis management
4. Supply chain security – including security-related aspects of relationships between each entity and
   (i) its suppliers or
   (ii) service providers (such as data storage providers and processing services or managed security services providers)
5. Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosures
6. Policies and procedures to assess the effectiveness of cybersecurity risk management measures
7. The use of cryptography and encryption

CER - The Critical Entities Resilience Directive

Enligt CER-direktivet ska medlemsstaterna säkerställa förmågan hos samhällsviktig verksamhet att **förebygga**, **motstå** och **hantera störningar eller avbrott** i verksamheten. Detta ska gälla oavsett om störningen eller avbrottet har föranletts av till exempel naturolyckor, terroristattacker, pandemier eller **andra allvarliga händelser.**

Direktivet omfattar följande sektorer:

- energi,
- transporter,
- bankverksamhet,
- infrastruktur för finansiella marknader,
- hälso- och sjukvård,
- **dricksvattenförsörjning**,
- **avlopp,**
- digital infrastruktur,
- offentlig förvaltning och
- rymd.

CER - The **C**ritical **E**ntities **R**esilience Directive

- Började gälla 16 januari 2023
- Implementerad senast 17 oktober 2024 i nationell lagstiftning
- Ersätter European Critical Infrastructure Directive från 2008

Hur påverkas samhällsviktiga verksamheter av CER-direktivet?

När den statliga offentliga utredningen (SOU) som omhändertar implementeringen av CER- och NIS 2 direktiven är klar så kommer MSB att ge mer detaljerad information.

En ny version av NIS-direktivet, NIS2, som ska ersätta det ursprungliga NIS-direktivet, har förhandlats fram inom EU under första halvåret av 2022. En utredning om genomförandet av NIS2-direktivet i svensk rätt kommer att tillsättas under 2022.

NATO artikel 3

"Each NATO member country needs to be resilient to **resist and recover** from a major shock such as a **natural disaster, failure of critical infrastructure, or a hybrid or armed attack.** Resilience is a society's ability to resist and recover from such shocks and combines both civil preparedness and military capacity**. Civil preparedness is a central pillar of Allies' resilience and a critical enabler for the Alliance's collective defence,** and NATO supports Allies in assessing and enhancing their civil preparedness."

Henrik Kjellgren
Säkerhetsansvarig
henrik.kjellgren@lbva.se
0722460917