Hvordan skal produksjonsbedrifter sikre seg mot cyberangrep?

Med Embriq & Secure-NOK

EmbriQ

Eksperter innen cybersikkerhet for industrielle nettverk og kontrollsystemer

Norsk-eid OT-sikkerhetsselskap med egenutviklet teknologi for å detektere og unngå angrep mot industrielle anlegg.

…Unik patentert teknologi…

SNOK
Cybersecurity Monitoring System

…Eksperter innen OT-sikkerhet…

Rådgivnings- og analysetjenester fra Secure-NOK Security Center.

Nina Hesby Tvedt

Chief Commercial Officer,
Secure-NOK

Hvordan skal produksjonsbedrifter sikre seg mot cyberangrep?

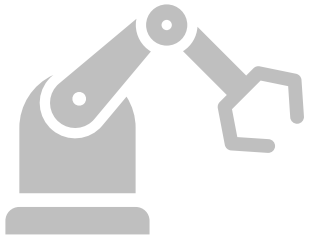
En intro til OT-sikkerhet og hvordan virksomheter kan forberede seg på skjerpede sikkerhetskrav/NIS2

SECURENOK®

Skjerpet trusselsituasjon

Geopolitisk ustabilitet og organisert kriminalitet

OT cyber trusler med opphav i statlig sponsede og velfinansierte kriminelle organisasjoner.



Industri 4.0 og digitalisering

Industri 4.0 vokser raskt og forventes å være en viktig driver for etterspørsel etter OT sikkerhet fremover.

Regulatorisk etterlevelse

Nye statlige reguleringer er på trappene for å styrke motstandskraften mot cybertrusler både i Norge og EU.

Hva er trusselbildet mot produksjonsbedrifter?

Februar 2025:

Kripos' årlige rapport om trussellandskapet innen cyberkriminalitet

- Etablert markedsplass for Cybercrime-as-a-Service.
- Kriminelle tjener store penger på cyberutpressing - ønsker å ramme der betalingsvilligheten er størst.
- Trend internasjonalt mot å angripe OT – på vei mot Norge.

Hvorfor øker interessen for å angripe OT?

Case: Utpressingsangrep mot Colonial Pipeline

Angrepet av gruppen «Darkside» i 2021.

Rammet virksomhetens administrative systemer.

Colonial var ikke i stand til å vurdere om OT var rammet
– valgte å stenge ned produksjonen
– valgte å betalte 4,4 M$ i løsepenger.

Fikk produksjonen i gang etter en uke.

Hvilke forventninger vil samfunnet ha til cybersikkerhet i tiden fremover?

SECURENOK®

Lov om digital sikkerhet og NIS direktivet

Utvikling av lovverket

2014

2015

2016

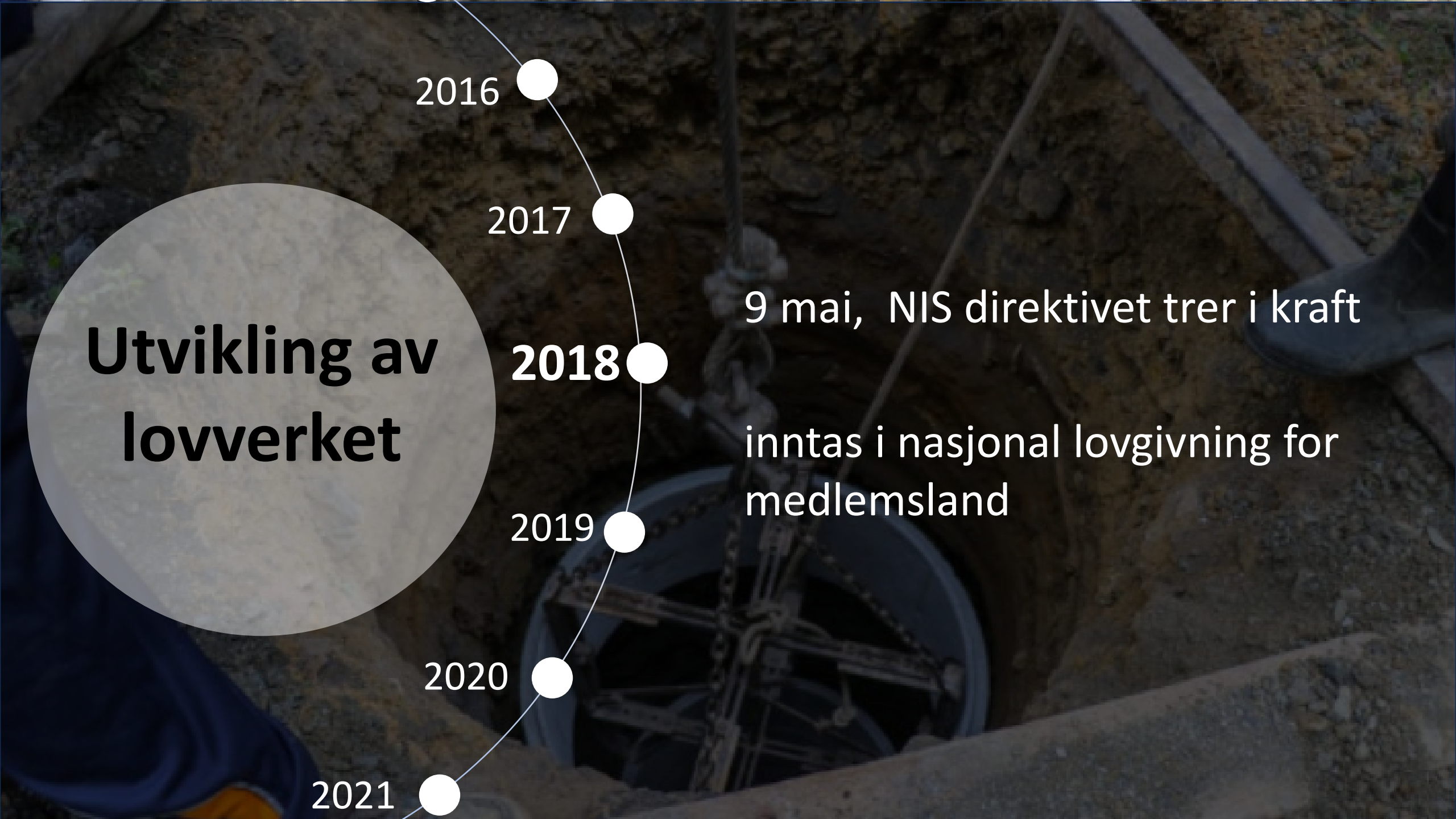
2017

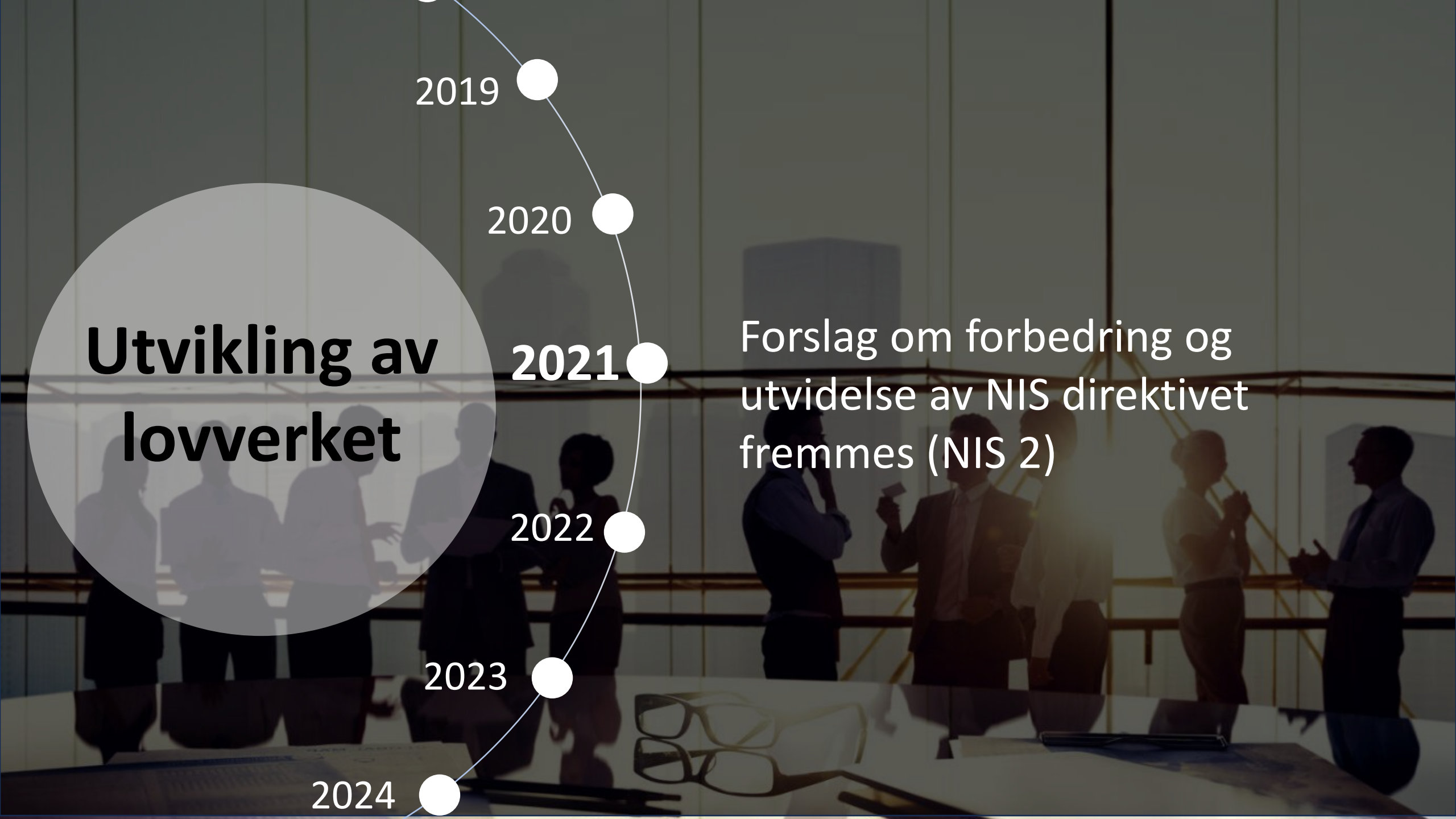
2018

2019

Juli, NIS direktivet blir vedtatt

tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i hele Unionen


Utvikling av lovverket
2016
2017
2018
2019
2020
2021
9 mai, NIS direktivet trer i kraft
inntas i nasjonal lovgivning for medlemsland


2019
2020
Utvikling av lovverket
2021
Forslag om forbedring og utvidelse av NIS direktivet fremmes (NIS 2)
2022
2023
2024

Utvikling av lovverket

2020

2021

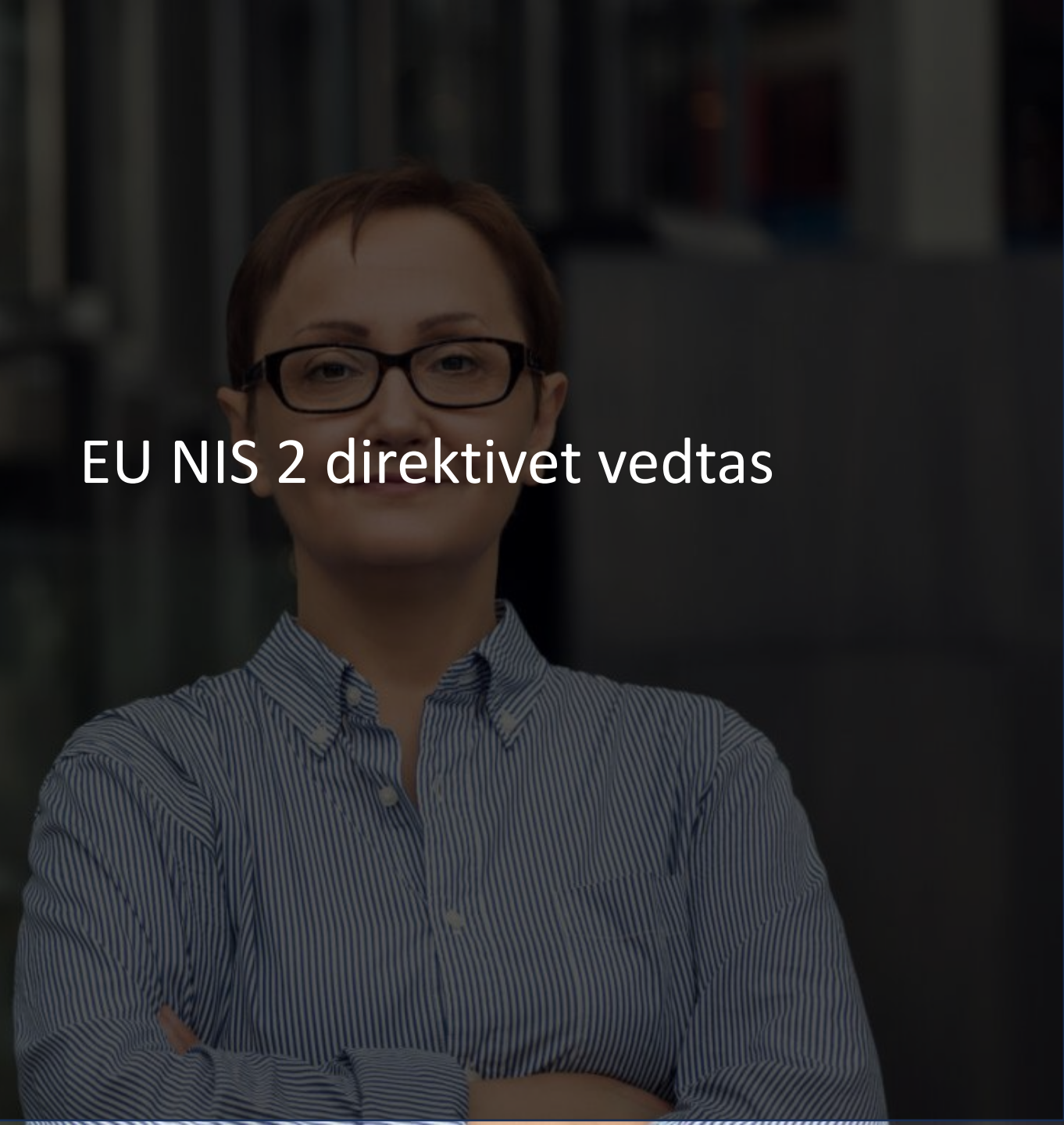
2022

EU NIS 2 direktivet vedtas

2023

2024

2025



Utvikling av lovverket

2021

2022

2023

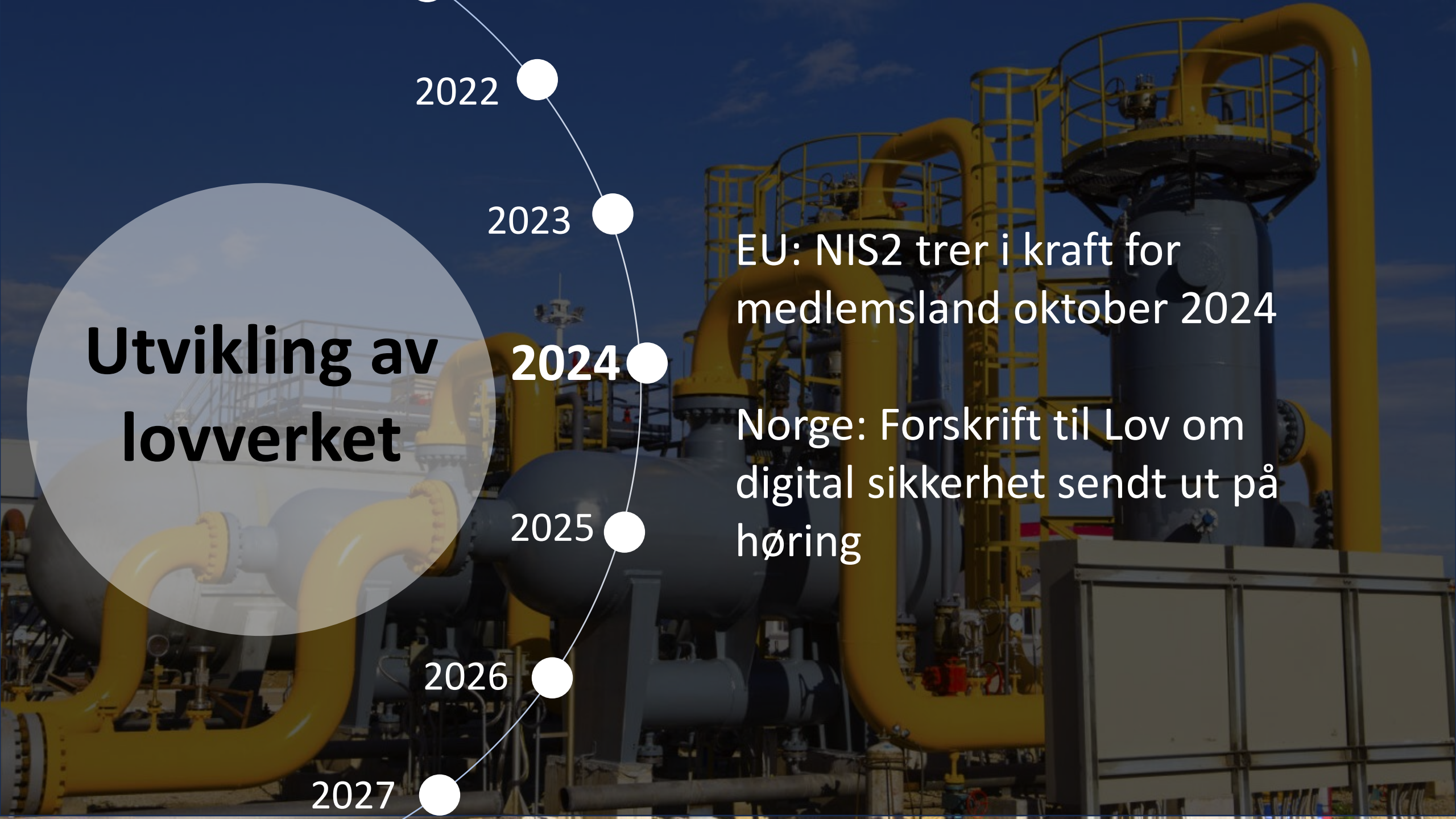
2024

2025

2026

EU: NIS 2 direktivet inntas i nasjonal lovgivning for medlemsland

Norge: Lov om digital sikkerhet vedtas i Stortinget - bygget på NIS-direktivet av 2016 (NIS1)



Utvikling av lovverket

EU: NIS2 trer i kraft for medlemsland oktober 2024

Norge: Forskrift til Lov om digital sikkerhet sendt ut på høring

Utvikling av lovverket

2023

2024

2025

2026

2027

2028

Norge: Lov om digital sikkerhet forventet å tre i kraft i 2025

Forventes utvidet til NIS 2. Når?

1

Hvem er omfattet av NIS2?

Alle virksomheter av en viss størrelse og en viss type

Direktivet skiller mellom «vesentlige/Essential» og «viktige/important»

2

Krav til virksomheter gjennom NIS 2

- Krav til risikobasert tilnærming til cybersikkerhet
- Konkrete tekniske og organisatoriske minimumskrav

Forventningene til hva som er et rimelig tiltaksnivå vil endre seg over tid.

3

Tilsyn og sanksjoner

Tilsynsregime: Både uanmeldt og anmeldte tilsyn.

Sanksjoner ved overtredelse av direktivet.

Energi

Transport

Bank

Finansmarkedsinfrastruktur

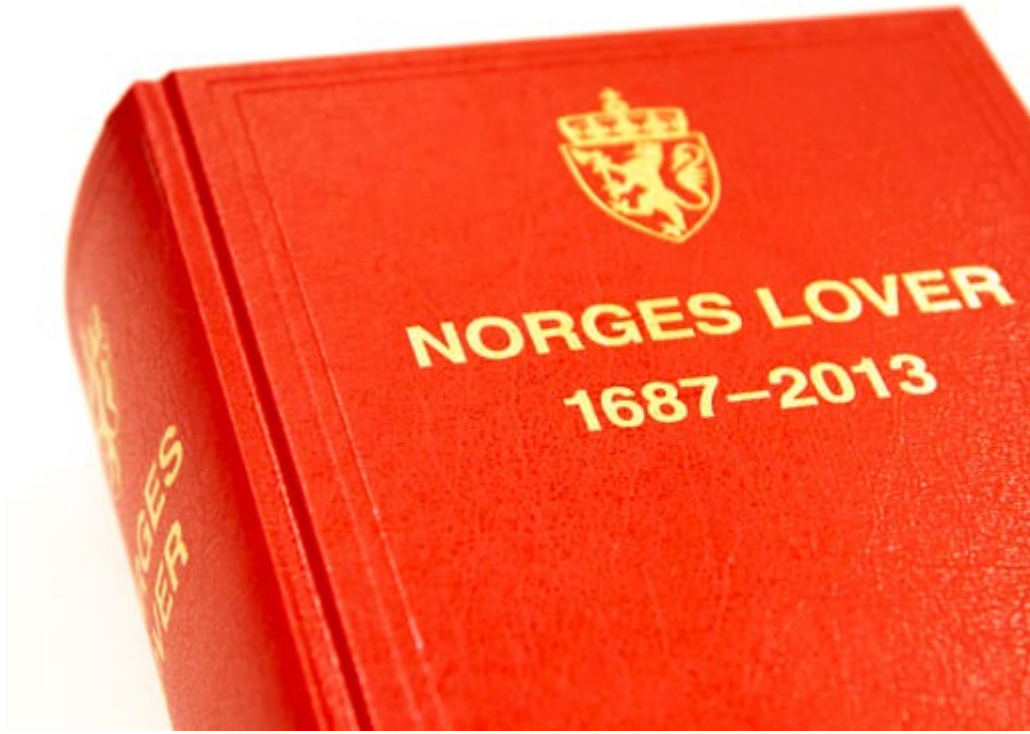
Helse

Vannforsyning

Digital infrastruktur

LOVDATA

Lov om digital sikkerhet



NIS2 sektorer

Energi

Transport

Bank

Finansmarkedsinfrastruktur

Helse

Vannforsyning/avløp

Digital infrastruktur

Romvirksomhet

IKT tjenester

Post

Avfallshåndtering

Kjemikalier

(produksjon og distribusjon)

Matproduksjon

Vareproduksjon

(medisinsk utstyr, IKT-utstyr, kjøretøy, elektronikk, maskiner, transportutstyr)

Digitale tjenester

Forskning

Hvorfor er industrianlegg sårbare?

SECURENOK®

Industrianlegg er avhengig av IT og OT

OT

Styring av fysiske prosesser og maskineriet som utfører dem.

IT

Styring av digital informasjon.

SECURENOK®



Hva kjennetegner OT?

- Høye pålitelighets- og tilgjengelighetskrav.
- Stabil oppførsel og lang levetid.
- Ofte avhengig av bistand fra leverandører for drift og vedlikehold.
- Sikkerheten tradisjonelt ivaretatt gjennom å “air-gappe” systemer.

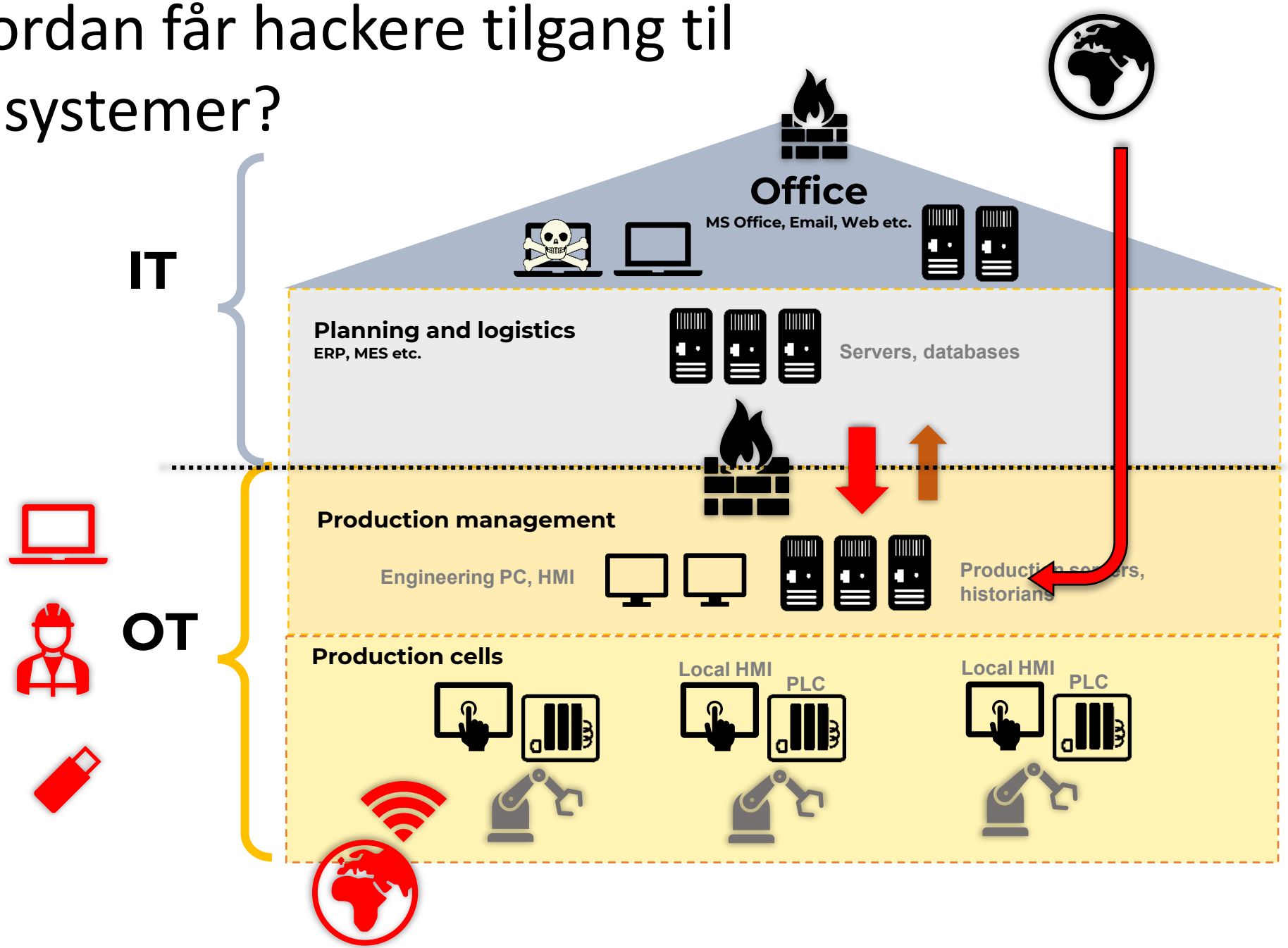
SECURENOK®

Vanlige sårbarheter i OT som oppstår over tid

- Ikke uvanlig med **legacy** firmware/software i OT utstyr.
- Ansvaret for vedlikehold og drift av IT og OT er ofte **oppsplittet** mellom team.
- Etterslep av **vedlikehold**, blant annet fordi vinduer er korte og sjeldne – kvalifiseringskrav er høye.
- Behov for akutt assistanse fra eksperter og leverandører kan føre til bruk av **ad hoc** løsninger for fjerntilkobling.

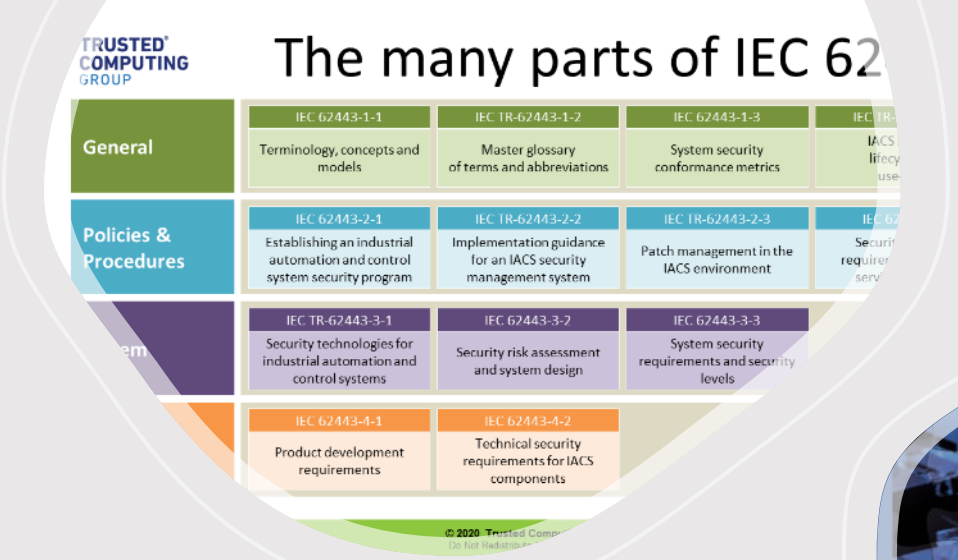
SECURENOK®

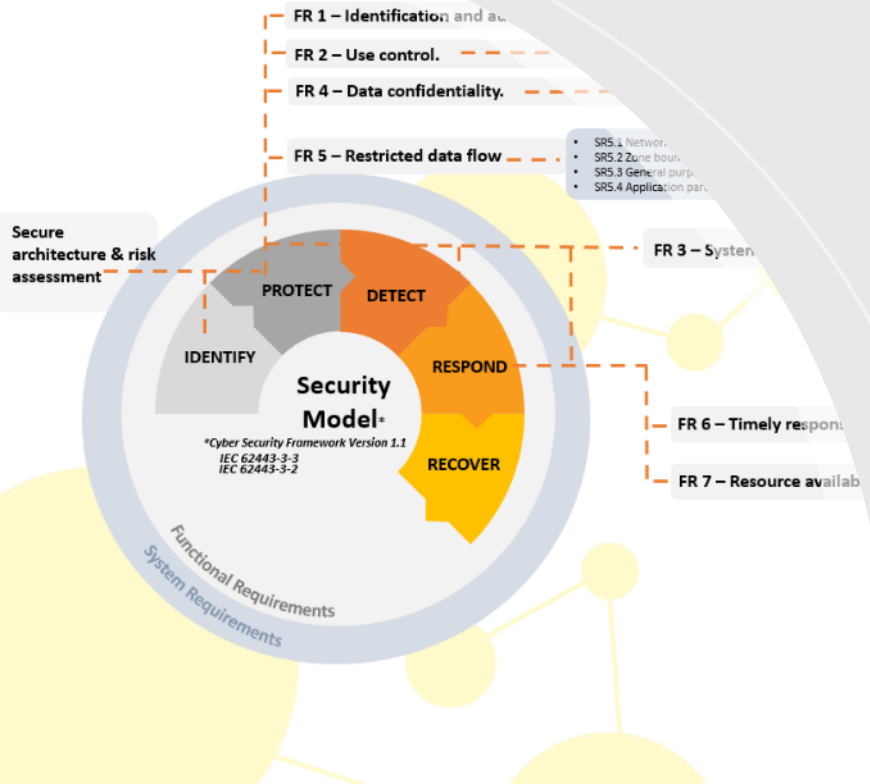
Hvordan får hackere tilgang til OT systemer?



Hvordan kan vi sikre produksjonen?

SECURENOK®





IEC-62443

NIST Cybersecurity Framework

NSM's grunnprinsipper for IKT sikkerhet

.....

Tilpasset IT systemer

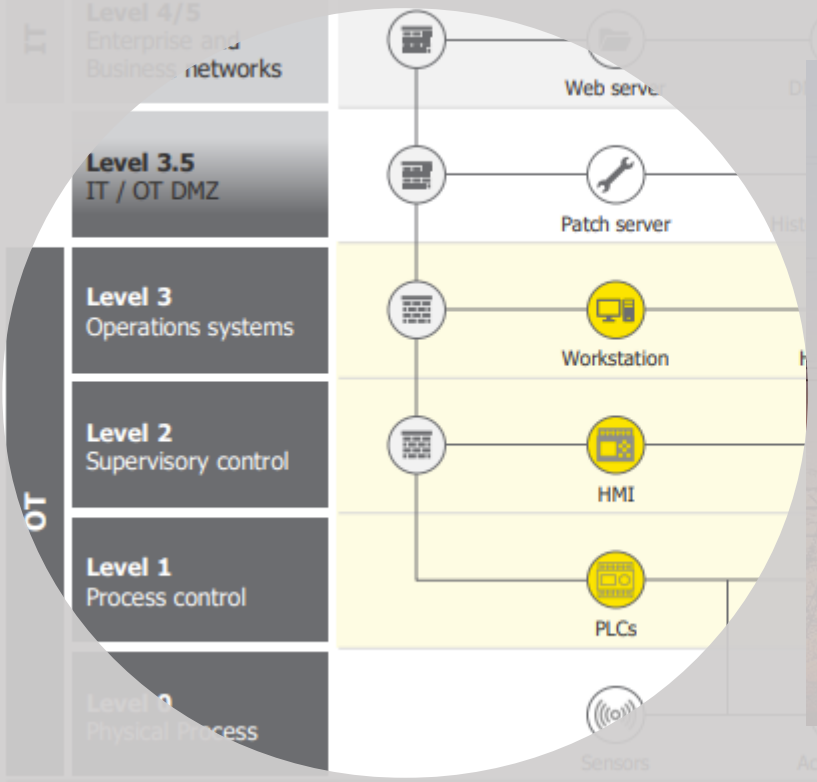
1. Identifisere og kartlegge	2. Beskytte og opprettholde		3. Oppdage	4. Håndtere og gjenopprette
1.1 Kartlegg styringsstrukturer, leveranser og understøttende systemer	2.1 Ivareta sikkerhet i anskaffelses- og utviklingsprosesser	2.2 Etabler en sikker IKT-arkitektur	3.1 Oppdag og fjern kjente sår-barheter og trusler	4.1 Forbered virksomheten på håndtering av hendelser
1.2 Kartl enheter program				
1.3 Kartlegg brukere og behov for tilgang	2.5 Kontroller dataflyt	2.6 Ha kontroll på identiteter og tilganger	3.3 Analyser data fra sikkerhets-overvåkning	4.3 Kontroller og håndter hendelser
	2.7 Beskytt data i ro og i transitt	2.8 Beskytt e-post og nettleser	3.4 Gjennomfør inntrengings-tester	4.4 Evaluer og lær av hendelser
	2.9 Etabler evne til gjenoppretting av data	2.10 Integrer sikkerhet i prosess for endringshånd-tering		

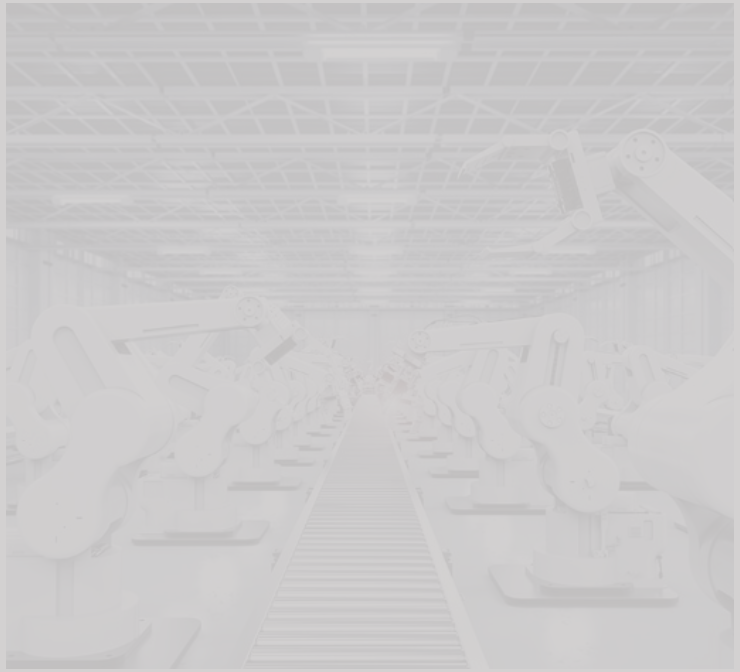
The 5 Critical Controls for ICS/OT cybersecurity

Ved innkjøp av nye systemer – still krav!

SECURENOK®

Krav til arkitektur



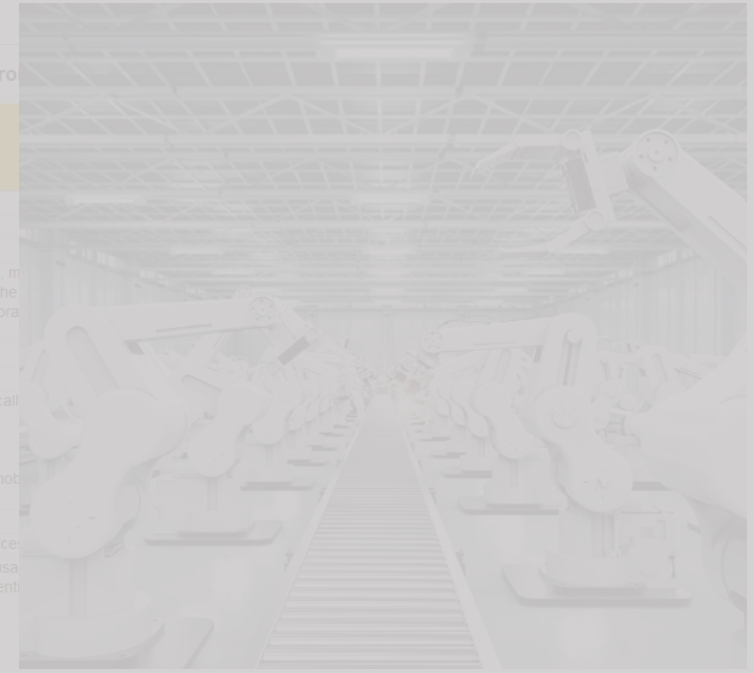


Krav til leveranse av systemer, produkter og tjenester

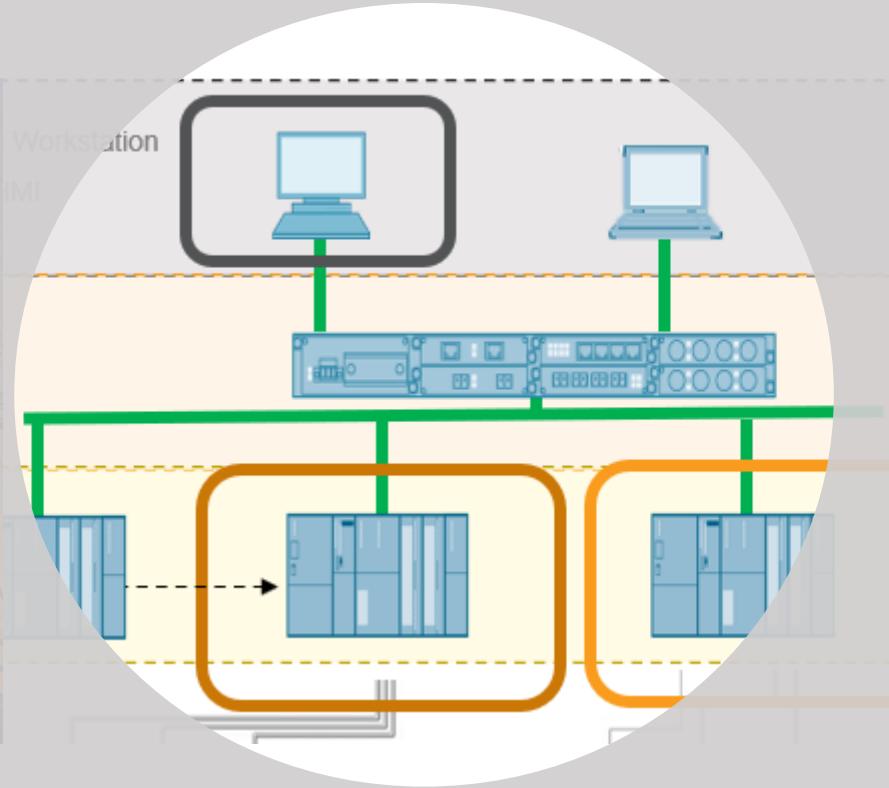
SECURENOK

Functional Requirement (FR) -2 Use Control

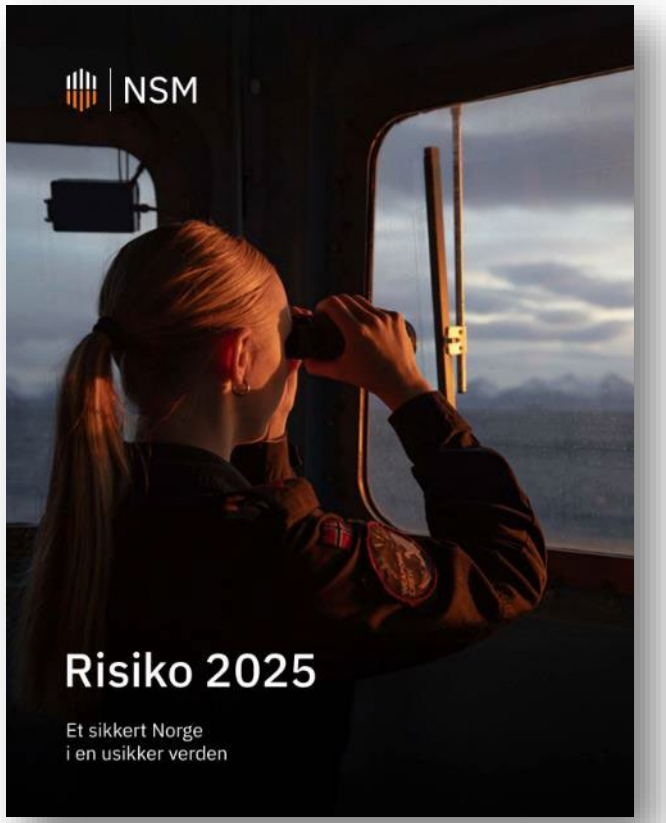
ID	SR (System Requirement)	Description
SR 2.1 RE 2		Permission mapping to roles
SR 2.1 RE 3		Supervisor override
SR 2.1 RE 4		Dual approval
SR2.2	**Wireless use control**	The control system shall provide the capability to authoriz, m and enforce usage restrictions for wireless connectivity to the system according to commonly accepted security industry pra
	Requirement enhancements	
SR 2.2 RE 1		Identify and report unauthorized wireless devices
SR2.3	**Use control for portable and mobile dev**	The control system shall provide the capability to automa call enforce configurable usage restrictions that include: a) preventing the use of portable and mobile devices; b) requiring context specific authorization; and c) restricting code and data transfer to/from portable a nd mob devices.
	Requirement enhancements	
SR 2.3 RE 1		Enforcement of security status of portable and m obile device
SR 2.4	**Mobile code**	The control system shall provide the capability to enforce usa restrictions for mobile code technologies bas d on the potenti cause damage to the control system that include: a) preventing the execution of mobile co de



Krav til leverandørens etterlevelse og vedlikehold



NSM: Risikobildet krever handling



«Norske virksomheter kan ikke påvirke trusselbildet, men de kan absolutt ta grep som sikrer de viktigste verdiene våre, reduserer de største sårbarhetene i samfunnet vårt, og ikke minst reduserer konsekvenser av uønskede hendelser.

Men dette arbeidet går for sakte,

uttaler direktør Arne Christian Haugstøyl i Nasjonal sikkerhetsmyndighet (NSM).»

Møt oss på stand

– rett ved inngangen

EmbriQ

LOVDATA

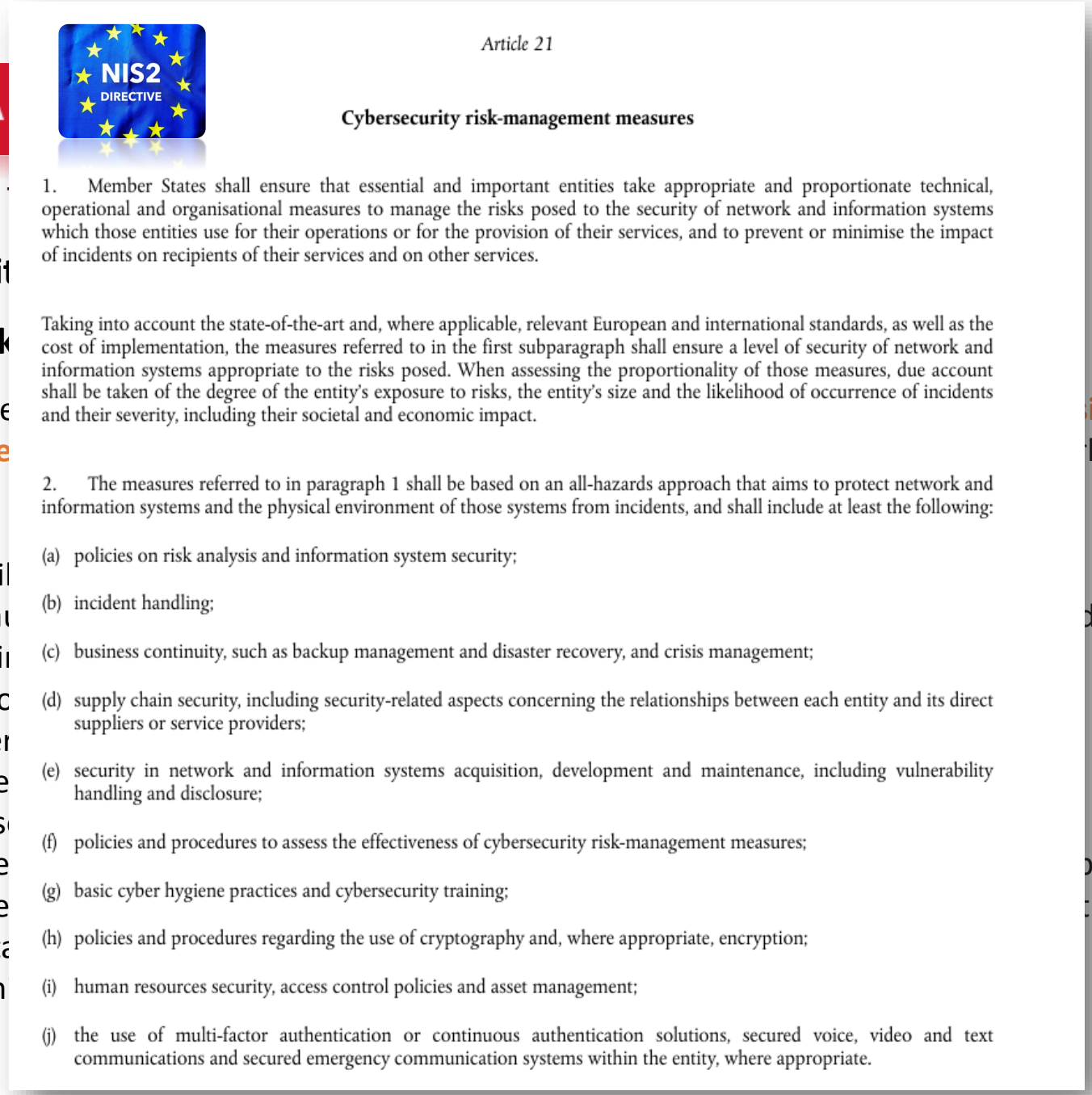
Versjon sendt til høring med

Kapittel 2. Krav til digit

§ 10. Teknologiske sik

Basert på risikovurderinge **ikkerhetstiltak som er**
tilpasset omfang, komple k og
informasjonssystemer.

Teknologiske sikkerhetstil
a. to- eller flerfaktorau dministratorer
b. tilgangskontroll til i
c. styring av og kontrc
d. tiltak for segmenter
e. tiltak som skal sikre og gjenopprettes innen
rimelig tid uten ves
f. tiltak som skal sikre belastning og utstyrssvikt
g. tiltak som skal sikre oppdateringer
kvalitetssikres, insta
h. sikkerhetsovervåkn



NIS2 DIRECTIVE

Article 21

Cybersecurity risk-management measures

1. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

SECURENOK®