NSM

NIS-direktivet for norske virksomheter

Innlegg for Digi Rogaland

16.10.2024

UGRADERT

NSM

Agenda

1. Det digitale risikobildet og bakgrunnen for NIS-direktivet
2. Status for regelverksutviklingen i Norge
3. Sentrale krav og plikter med vekt på NIS2
4. Viktige endringer fra NIS1 til NIS2
5. Kort om forholdet til andre regelverk
6. Noen spørsmål virksomheter bør drøfte internt for å forberede seg

NSM

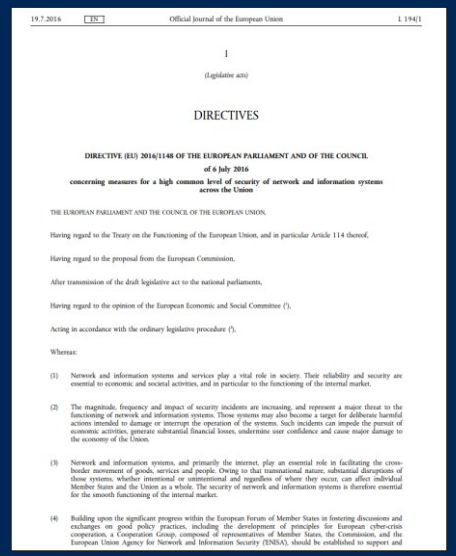
Endring og utvikling i det digitale risikobildet

- Digitaliseringen gjør oss effektive, men også sårbare
- Økt utnyttelse av nulldagssårbarheter
- Nye sektorer rammes
- Alle ledd i angrepskjeden profesjonaliseres

Kort om formålet med NIS-direktivet

- Alle samfunnsviktige tjenester er avhengige av digitale tjenester og digital infrastruktur
- Stille tydeligere og mer harmoniserte krav til digital sikkerhet i virksomheter som leverer samfunnsviktige tjenester i EU/EØS
- Grunnlag for å identifisere virksomheter som leverer samfunnsviktige tjenester
- Bidra til bedre situasjonsforståelse ved hendelser og økt samarbeid mellom myndigheter i Europa

Status for regelverksutviklingen



19.7.2016 EN Official Journal of the European Union L 194/1

1

(Legislative acts)

DIRECTIVES

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 6 July 2016
concerning measures for a high common level of security of network and information systems across the Union

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Acting in accordance with the ordinary legislative procedure (2),

Whereas:

(1) Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market.

(2) The magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union.

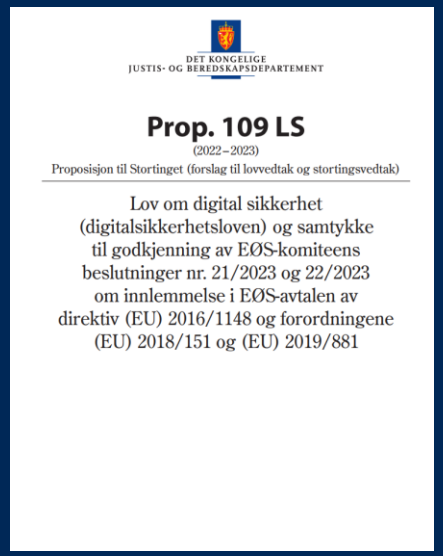
(3) Network and information systems, and primarily the internet, play an essential role in facilitating the cross-border movement of goods, services and people. Owing to that transnational nature, substantial disruptions of those systems, whether intentional or unintentional and regardless of where they occur, can affect individual Member States and the Union as a whole. The security of network and information systems is therefore essential for the smooth functioning of the internal market.

(4) Building upon the significant progress within the European Forum of Member States in fostering discussions and exchanges on good policy practices, including the development of principles for European cyber-crisis cooperation, a Cooperation Group, composed of representatives of Member States, the Commission, and the European Union Agency for Network and Information Security (ENISA), should be established to support and

NOU Norges offentlige utredninger 2018: 14

IKT-sikkerhet i alle ledd

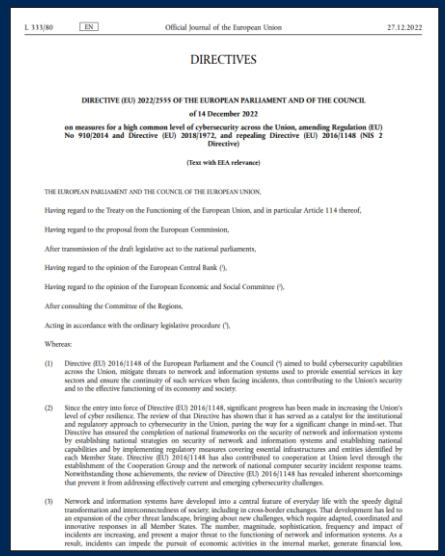
Organisering og regulering av nasjonal IKT-sikkerhet



DET KONGELIGE
JUSTIS- OG BEREDSKAPSDEPARTEMENT

Prop. 109 LS
(2022–2023)
Proposisjon til Stortinget (forslag til lovvedtak og stortingsvedtak)

Lov om digital sikkerhet (digitalsikkerhetsloven) og samtykke til godkjenning av EØS-komiteens beslutninger nr. 21/2023 og 22/2023 om innlemmelse i EØS-avtalen av direktiv (EU) 2016/1148 og forordningene (EU) 2018/151 og (EU) 2019/881



L 333/80 EN Official Journal of the European Union 27.12.2022

DIRECTIVES

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)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Central Bank (1),

Having regard to the opinion of the European Economic and Social Committee (2),

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) Directive (EU) 2016/1148 of the European Parliament and the Council (4) aimed to build cybersecurity capabilities across the Union, mitigate threats to network and information systems used to provide essential services in key sectors and ensure the continuity of such services when facing incidents, thus contributing to the Union's security and to the effective functioning of its economy and society.

(2) Since the entry into force of Directive (EU) 2016/1148, significant progress has been made in increasing the Union's level of cyber resilience. The review of that Directive has shown that it has served as a catalyst for the institutional and regulatory approach to cybersecurity in the Union, paving the way for a significant change in mind-set. That Directive has ensured the completion of national frameworks on the security of network and information systems by establishing national strategies on security of network and information systems and establishing national capabilities and by implementing regulatory measures covering essential infrastructures and entities identified by each Member State. Directive (EU) 2016/1148 has also contributed to cooperation at Union level through the establishment of the Cooperation Group and the network of national computer security incident response teams. Notwithstanding those achievements, the review of Directive (EU) 2016/1148 has revealed inherent shortcomings that prevent it from addressing effectively current and emerging cybersecurity challenges.

(3) Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, including in cross-border exchanges. That development has led to an expansion of the cyber threat landscape, bringing about new challenges, which require adapted, coordinated and innovative responses in all Member States. The number, magnitude, sophistication, frequency and impact of incidents are increasing, and present a major threat to the functioning of network and information systems. As a result, incidents can impede the pursuit of economic activities in the internal market, generate financial loss,

NIS 1 (2016)

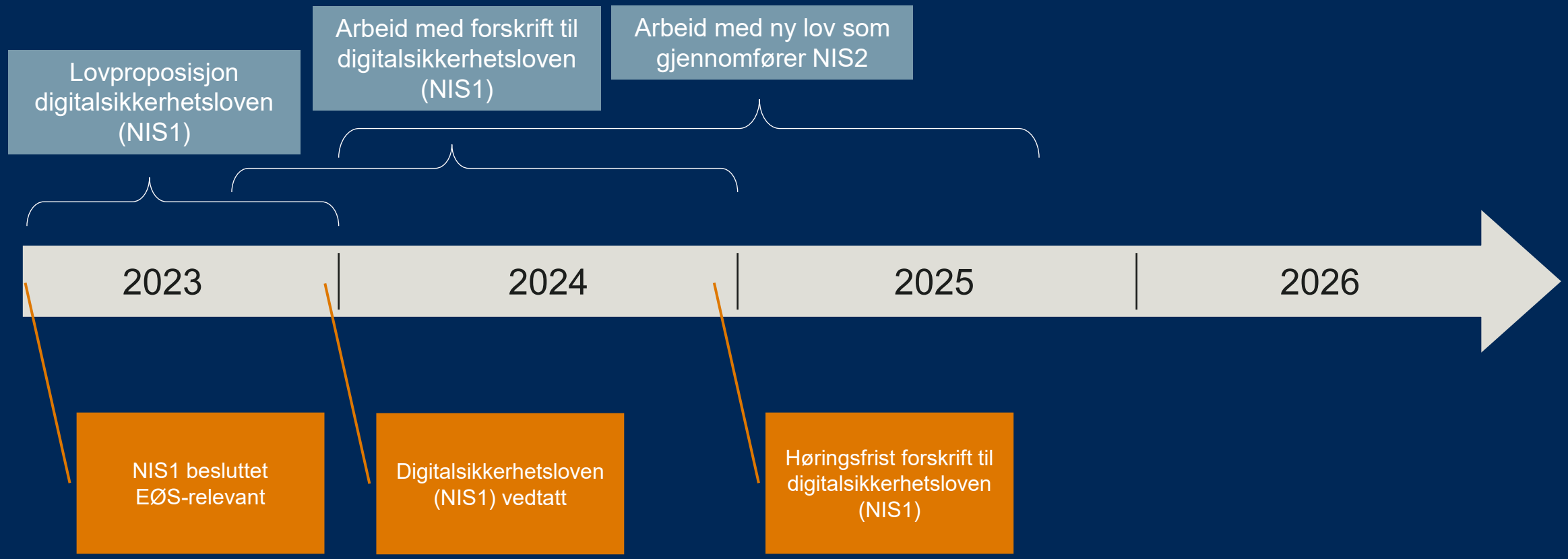
Høring - utkast til ny lov (2018-2019)

Prop. 109 LS (2022-2023) Lov om digital sikkerhet

NIS 2 (2022)

Ny lovproposisjon NIS2

Status for regelverksutviklingen



NSM

Overordnede krav i NIS

Hvert land skal sørge for et økt nivå av digital sikkerhet ved å:

1. Pålegge virksomheter plikt til å iverksette tiltak for digital sikkerhet
2. Pålegge virksomheter varslingsplikt til myndighetene ved alvorlige IKT-sikkerhetshendelser som er egnet til å ramme samfunnsviktige tjenester
3. Utarbeide en nasjonal strategi for digital sikkerhet
4. Etablere eller utpeke kompetente myndigheter for digital sikkerhet
5. Etablere eller utpeke et nasjonalt kontaktpunkt
6. Etablere eller utpeke responsmiljøer (CSIRTs)

NIS2 artikkel 21 – «Cybersecurity risk-management measures»

- Iverksette hensiktsmessige og proporsjonale tiltak for å håndtere risiko knyttet til nettverk og informasjonssystemer
- Teknologiske, fysiske, personellmessige og organisatoriske tiltak
- Skal ta hensyn til beste praksis, internasjonale/europeiske standarder, og kostnader, for å sikre at tiltakene er tilpasset den identifiserte risikoen knyttet til nettverk og informasjonssystemer
- Proporsjonalitet vurderes ut fra virksomhetens eksponering, størrelse og betydning, og sannsynligheten for uønskede hendelser
- «All hazards approach»

NSM

NIS2 artikkel 21 (forts.)

Det forebyggende sikkerhetsarbeidet i virksomheten skal blant annet dekke:

- Informasjonssikkerhetspolicy for virksomheten og retningslinjer for risikovurderinger
- Planer for hendelseshåndtering
- Planer for driftskontinuitet, inkludert backup og gjenoppretting
- Sikkerhet i leverandørkjeder
- Sikkerhet i anskaffelser, utvikling og vedlikehold av informasjonssystemer, inkludert deling av informasjon om sårbarheter
- Retningslinjer og rutiner for å vurdere effekten av sikkerhetstiltak
- Grunnleggende informasjonssikkerhetstiltak og opplæring av personell
- Retningslinjer og rutiner for tilgangskontroll og personellsikkerhet
- Retningslinjer og rutiner for bruk av kryptering der dette er hensiktsmessig
- Retningslinjer og rutiner for bruk av flerfaktorautentisering og kontinuerlig autentisering, og sikre tale-, meldings- og videotjenester, der dette er hensiktsmessig

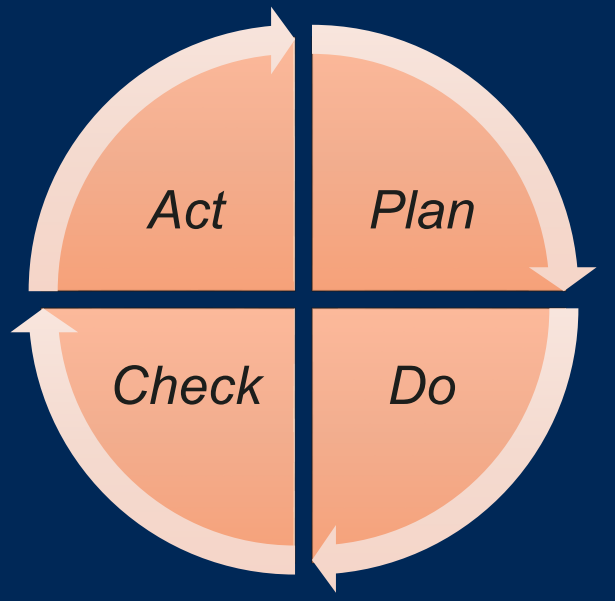
NSM

NIS2 artikkel 20 – «Governance»

- NIS2 tydeliggjør at virksomhetens øverste ledelse har ansvaret for det forebyggende sikkerhetsarbeidet
- Ledelsen skal godkjenne sikkerhetstiltakene
- Ledelsen skal følge opp og sørge for at tiltakene iverksettes
- Opplæring/kurs for å ha tilstrekkelig grunnlag for å identifisere risikoområder, vurdere hvordan risikohåndteringen i virksomheten virker, og forstå betydningen for virksomhetens tjenesteleveranser

NSM


Virksomhetsstyring
Sikkerhetsstyring
Styringsaktiviteter
Sikkerhetstiltak


Act
Plan
Check
Do

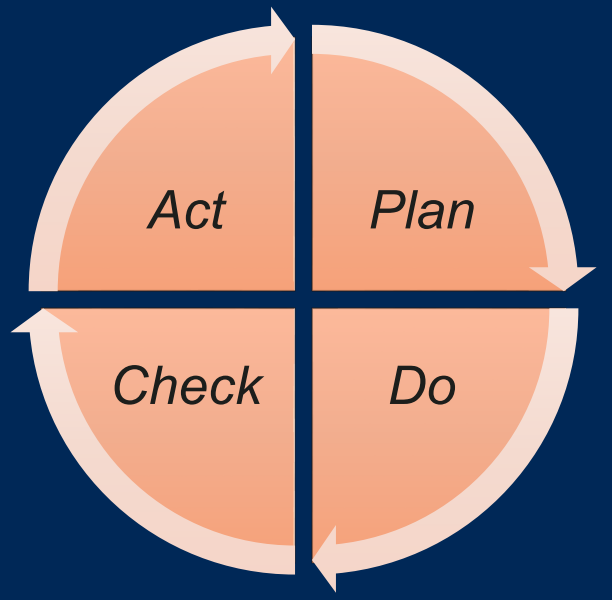
NSM

Virksomhetsstyring

Sikkerhetsstyring

Styringsaktiviteter

Sikkerhetstiltak



Kartlegging, risikovurdering, risikohåndtering, forankring i ledelsen, måling, evaluering, rapportering, kommunikasjon

Organisatoriske – teknologiske – fysiske – personellmessige

Forebygge – oppdage – håndtere - gjenopprette

NSM

Virkeområde – NIS1

Tilbydere av *samfunnsviktige tjenester* innen:

- Energi – elektrisitet, olje og gass
- Transport – luftfart, jernbane, sjø, veg
- Helse - helsetjenester
- Bank og finansmarkedsinfrastruktur
- Drikkevannsforsyning
- Digital infrastruktur – samtrafikkpunkter (IXP), navneservertjenester (DNS), forvalter av toppnivådomener (TLD)

Tilbydere av *digitale tjenester* omfatter etter NIS 1 skytjenester, nettbaserte markedsplasser og søkemotorer

NSM

Utvidet virkeområde – NIS2, vedlegg I

Kritiske sektorer:

- Energi – elektrisitet, olje og gass, oppvarming, hydrogen
- Transport – luftfart, jernbane, sjø, veg
- Helse – helsetjenester, laboratorier, R&D
- Bank- og finansmarkedsinfrastruktur
- Drikkevannsforsyning
- Digital infrastruktur – elektronisk kommunikasjon, datasentertjenester, skytjenester, tillitstjenester, samtrafikkpunkter (IXP), navneservertjenester (DNS), forvalter av toppnivådomener (TLD)
- Avløpsvann
- Administrerte IKT-tjenester
  - Leverandør av administrerte IKT-tjenester
  - Leverandør av administrerte sikkerhetstjenester
- Offentlig forvaltning – sentral og regional
- Romsektoren – bakkebasert infrastruktur

NSM

Utvidet virkeområde – NIS2, vedlegg II

Andre *viktige* sektorer:

- Produksjon og distribusjon av kjemikalier
- Produksjon og distribusjon av matvarer/næringsmidler
- Produksjon og distribusjon av visse typer varer, herunder medisinsk utstyr, IKT-utstyr, elektronikk, maskiner, motorkjøretøy og andre transportmidler
- Forskning
- Avfallshåndtering
- Post- og kurértjenester
- Tilbydere av digitale tjenester – søkemotorer, nettbaserte markedsplasser og sosiale medier-plattformer

Terskelverdier som utgangspunkt – hovedregel (NIS2)

Sektor (NIS2)	Store virksomheter (>= 250 ansatte)	Mellomstore virksomheter (50-249 ansatte)	Små virksomheter
Vedlegg I	KRITISKE	VIKTIGE	*Ikke omfattet*
Vedlegg II	VIKTIGE		*Ikke omfattet*

- I tillegg kommer terskler knyttet til omsetning for hhv. mellomstore og store virksomheter
- Følger etablert definisjon av mellomstore og store virksomheter i EU

NSM

Terskelverdier som utgangspunkt – noen spesielle unntak (NIS2)

Sektor (NIS2)	Type virksomhet	Store virksomheter	Mellomstore virksomheter	Små virksomheter
Digital infrastruktur	Kvalifiserte tillitstjenester	KRITISKE	KRITISKE	KRITISKE
	DSN-tjenestetilbydere, unntatt rotnavnetjenere	KRITISKE	KRITISKE	KRITISKE
	Toppnivådomeneregistrering	KRITISKE	KRITISKE	KRITISKE
	Tilbydere av elektronisk kommunikasjon	KRITISKE	KRITISKE	VIKTIGE
	Ikke-kvalifiserte tillitstjenester	KRITISKE	VIKTIGE	VIKTIGE
Offentlig forvaltning	Sentral offentlig forvaltning, unntatt nasjonal og offentlig sikkerhet, forsvar, domstoler, nasjonalforsamlinger, sentralbanker	KRITISKE	KRITISKE	KRITISKE
	Regional offentlig forvaltning, opp til det enkelte land om lokal offentlig forvaltning skal omfattes ut fra en risikovurdering	VIKTIGE	VIKTIGE	VIKTIGE

- Innen bank og finansmarkedsinfrastruktur er DORA-forordningen *lex specialis*
- Virksomheter identifisert som kritiske etter CER-direktivet omfattes også av kravene i NIS2

NSM

Varslingsplikten (NIS2 Art. 23) - når skal virksomheten varsle?

- Virksomheter skal varsle om betydelige hendelser som rammer nettverk og informasjonssystemer, som er egnet til å påvirke tjenesteleveransen
- "All hazards" – ikke avgrenset til tilsiktede handlinger, ikke avgrenset til cyberdomenet

Det legges opp til følgende frister for varsling:

- "Early warning" uten unødig opphold og varsel senest innen 24 timer
- Statusoppdatering innen 72 timer
- Utdypende hendelsesrapport innen én måned

- Virksomheten skal også varsle kunder/brukere om alvorlige hendelser

NSM

Hvem skal virksomheten varsle til?

- Direktivet legger opp til kontinuitet
- Lov om digital sikkerhet legger opp til å benytte eksisterende myndighetsstruktur i størst mulig grad
- Departementene kan utpeke kompetente myndigheter i sektorene som skal føre tilsyn og gi veiledning tilpasset sektorens egenart – eksisterende sektortilsyn
- Sektormyndigheter / sektortilsyn og sektorresponsmiljøer forventes å ha sentrale roller som «førstelinje»
- NSM forventes å ha en mer koordinerende rolle, både som responsmiljø, tilsynsmyndighet og innen rådgivning/veiledning

NSM

Viktige endringer i NIS2 – kort oppsummert

- Betydelig utvidelse av virkeområdet – flere sektorer omfattes, og flere typer virksomheter innen hver sektor
- Ny tilnærming til hvordan virksomheter blir underlagt regelverket
  - fra nasjonal identifisering til europeiske terskelverdier som utgangspunkt
- Nye kategorier for virkeområdet - fra *samfunnsviktige* og *digitale* tjenestetilbydere (NIS 1) til *kritiske* og andre *viktige* virksomheter (NIS2)
- Ytterligere og mer konkrete sikkerhetskrav og varslingskrav
- Kobling til CER-direktivet

NSM

Forholdet til sektorregelverk

- Noen av kravene er delvis ivaretatt i gjeldende sektorregelverk i dag
- Krav i ulike sektorregelverk varierer
  - Stilles i varierende grad konkrete krav til digital sikkerhet
  - Krav om varsling til myndighet ved uønskede hendelser varierer
  - Tilsyn med og kompetanse innen digital sikkerhet varierer
- Der krav i sektorregelverk minst tilsvarer kravene som følger av ny lov om digital sikkerhet, medfører ny lov ikke store endringer for virksomhetene
- Dersom det *ikke* stilles tilstrekkelige krav til digital sikkerhet eller krav om varsling i sektorregelverk, så vil slike krav følge av ny lov, eventuelt gjennom tilpasninger i sektorregelverk

NIS og lov om digital sikkerhet kan forstås som en «grunnplanke» for digital sikkerhet som bidrar til å løfte sikkerhetsnivået på tvers av viktige tjenesteleverandører i ulike sektorer

NSM

Forholdet til lov om nasjonal sikkerhet (sikkerhetsloven)

- NIS må ikke forveksles med sikkerhetsloven
  - ulike formål – NIS handler ikke om nasjonale sikkerhetsinteresser
  - forskjellige virkeområder – ulik tilnærming til hvordan virksomheter blir underlagt regelverket
  - NIS er avgrenset til nettverk og informasjonssystemer
  - forskjellige tilsynsregimer
  - ulikt risikobilde
- I tilfeller som omhandler nasjonale sikkerhetsinteresser gjelder sikkerhetsloven
  - Informasjonssystemer som inngår i skjermingsverdig infrastruktur
  - Informasjonssystemer som er klassifisert i henhold til sikkerhetsloven
  - Sikkerhetsgraderte informasjonssystemer
  - Grunnleggende nasjonale funksjoner
- Godt forebyggende sikkerhetsarbeid i virksomhetene bygger likevel på en del gjenkjennelige sikkerhetsprinsipper

NSM

Kort om forholdet til andre europeiske regelverk

En rekke regelverk på vei med betydning for digital sikkerhet og samfunnssikkerheten i bredt:

- DORA – *lex specialis* for bank- og finansmarkedssektoren
- Cyber Security Act (CSA) – frivillig sertifisering av IKT-produkter og –tjenester
- Critical Entities Resilience-direktivet (CER)
- Cyber Resilience Act (CRA) – sikkerhet i produkter koblet til nett
- Cyber Solidarity Act (CSOA) – regionale «Cyber Hubs»

NSM

Noen spørsmål virksomheter bør drøfte

- Har vår virksomhet definert mål, strategier og policy for digital sikkerhet?
- Har vi god oversikt over informasjonssystemer som er viktige for våre kritiske aktiviteter?
- Kjenner vi konsekvensene for vår virksomhet dersom data og informasjonssystemer blir utilgjengelige, endres eller blir kjent for uvedkommende? Har vi gjennomført gode risikovurderinger av våre informasjonssystemer?
- Har vi iverksatt hensiktsmessige sikkerhetstiltak som er tilpasset vårt risikobilde? Bygger disse tiltakene på anerkjente standarder og rammeverk for digital sikkerhet?
- Hvilke kritiske avhengigheter har vi i våre leverandørkjeder? Hvilke leverandører er vi avhengige av for at våre informasjonssystemer skal være sikre?
- Har vi en god plan for hendelseshåndtering? Når oppdaterte vi den?
- Er vårt arbeid med forebyggende digital sikkerhet og vår sikkerhetsorganisasjon forankret i ledelsen? Rapporteres det på mål og strategier for digital sikkerhet?

Svarene kan gi en indikasjon på virksomhetens modenhet.
Svarene kan også synliggjøre områder hos ledelsen eller i organisasjonen som bør prioriteres.

NSM

Hjelp oss å bygge nasjonalt situasjonsbilde

Telefon (24/7): 02497

E-post cyberhendelser: cert@ncsc.no
E-post sikkerhetstruende virksomhet og hendelser: varsel@nsm.no