NSM

NIS-direktivet og ny lov om digital sikkerhet – hva betyr dette for norske virksomheter?

Nettverk for informasjonssikkerhet (NIFS)

06.03.2024

UGRADERT

NSM

Agenda

1. Bakgrunn og formål med NIS-direktivet
2. Innholdet i NIS-direktivet – krav, plikter, virkeområde, roller
3. NIS blir til ny lov om digital sikkerhet - status for lovarbeidet i Norge
4. Forholdet til andre regelverk
5. Noen overordnede råd til virksomheter

Bakgrunn og formål med NIS-direktivet

NSM

Hva er NIS-direktivet?

NIS er: Direktivet for et høyt felles sikkerhetsnivå i nettverk og informasjonssystemer, eller «nettverks- og informasjonssikkerhetsdirektivet»

En mulig «problembeskrivelse» identifisert på EU-nivå:

- Alle samfunnsviktige tjenester er i dag avhengige av digitale tjenester og digital infrastruktur
- … men det er ikke iverksatt tilstrekkelige beskyttelsestiltak for nettverk og informasjonssystemer
- … som ligger til grunn for samfunnsviktige tjenester i EU/EØS
- … og tilnærmingen til beskyttelsestiltak er for fragmentert på tvers av land.

NIS-direktivet er et sentralt regulatorisk virkemiddel i EUs overordnede cybersikkerhetsstrategi

Hva er NIS-direktivet? (forts.)

- Regelverk som skal sørge for et høyt felles nivå av digital sikkerhet i samfunnsviktige virksomheter og tjenester i EU/EØS
- Sørge for økt grad av harmonisering på tvers av land
- Legger vekt på tjenestekontinuitet, men omfatter alle aspekter ved sikkerhet i nettverk og informasjonssystemer
- Innføres i Norge gjennom ny lov om digital sikkerhet (i første omgang)

NSM

Noen overordnede mål

- Bidra til å bygge sikkerhetskultur i virksomheter som leverer samfunnsviktige tjenester
- Holde virksomhetens ledelse ansvarlig med hensyn til det forebyggende sikkerhetsarbeidet
- Sørge for at virksomheter gjennomfører risikovurderinger og iverksetter og kontrollerer sikkerhetstiltak for å øke motstandsdyktigheten
- Forbedre og ivareta tverrsektoriell, nasjonal situasjonsforståelse ved hendelser
- Bidra til bedre samarbeid og informasjonsdeling på tvers av sektorer og på tvers av land

Innholdet i NIS-direktivet:
Krav, plikter, virkeområde, roller

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. Sikre at kompetente myndigheter har nødvendige ressurser og faglig kompetanse til å føre tilsyn med digital sikkerhet
6. Etablere eller utpeke et nasjonalt kontaktpunkt
7. Etablere eller utpeke et nasjonalt hendelseshåndteringsmiljø

NIS2 artikkel 21 – «Cybersecurity risk management measures»

- Iverksette hensiktsmessige og proporsjonale tiltak for å håndtere risiko knyttet til nettverk og informasjonssystemer
- Tekniske, operasjonelle 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

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 og vurdere hvordan risikohåndteringen i virksomheten virker, og forstå betydningen for virksomhetens tjenesteleveranser

NSM

Virkeområde – NIS1

Samfunnsviktige tjenestetilbydere innen:

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

Digitale tjenestetilbydere omfatter etter NIS1 skytjenester, nettbaserte markedsplasser og søkemotorer

NSM

Utvidet virkeområde – NIS2

Kritiske virksomheter innen:

- Energi – strømforsyning, olje og gass, oppvarming, hydrogen
- Transport – luftfart, jernbane, sjø, veg
- Helse
- Bank- og finansmarkedsinfrastruktur
- Drikkevannsforsyning
- Digital infrastruktur – elektronisk kommunikasjon, datasentertjenester, skytjenester, tillitstjenester, samtrafikkpunkter (IXP), navneservertjenester (DNS), forvalter av toppnivådomener (TLD)
- Avløpsvann
- ICT service management
  - Managed service providers
  - Managed security service providers
- Offentlig forvaltning – sentral og regional
- Romsektoren – bakkebasert infrastruktur

NSM

Utvidet virkeområde – NIS2 (forts.)

Viktige virksomheter innen:

- Produksjon og distribusjon av kjemikalier
- Produksjon og distribusjon av matvarer/næringsmidler
- Produksjon og distribusjon av medisinsk utstyr, IKT-utstyr, elektronikk, maskiner, motorkjøretøy og andre transportmidler
- Forskning
- Post- og kurértjenester
- Digitale tjenestetilbydere – søkemotorer, nettbaserte markedsplasser og sosiale medier-plattformer

NSM

Varslingsplikten - når skal virksomheten varsle?

- Virksomheter skal varsle om hendelser som rammer nettverk og informasjonssystemer
- “All hazards” – ikke avgrenset til tilsiktede handlinger, ikke avgrenset til cyberdomenet

Det legges opp til følgende frister for varsling:

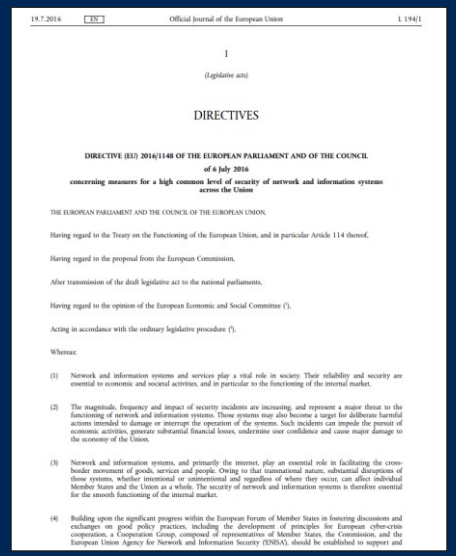
- “Early warning” uten unødig opphold og varsel senest innen 24 timer
- Statusoppdatering innen 72 timer
- Utdypende hendelsesrapport innen én måned

Hvem skal virksomheten varsle til?

- Direktivet legger opp til kontinuitet, der det allerede varsles om hendelser og føres tilsyn med digital sikkerhet i dag
- Lovproposisjonen til lov om digital sikkerhet legger opp til å benytte eksisterende myndighetsstruktur i størst mulig grad
- Sektormyndigheter / sektortilsyn ventes å få en sentral rolle
- Departementene kan utpeke kompetente myndigheter i sektorene som skal føre tilsyn og gi veiledning tilpasset sektorens egenart
- Informasjon om alvorlige hendelser må også nå frem til NSM som nasjonalt kontaktpunkt, også for å bidra til tverrsektoriell situasjonsforståelse

Lovarbeidet

Lovarbeidet



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

I

(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.

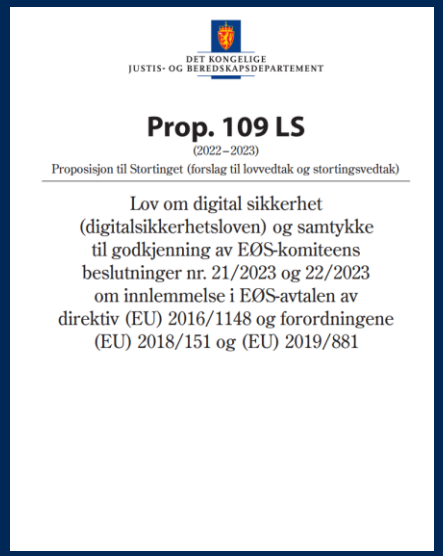
(3) Network and information systems, and primarily the internet, play an essential role in facilitating the cross-border movement of goods, services and people. Owing to that transnational nature, substantial disruptions of those systems, whether intentional or unintentional and regardless of where they 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

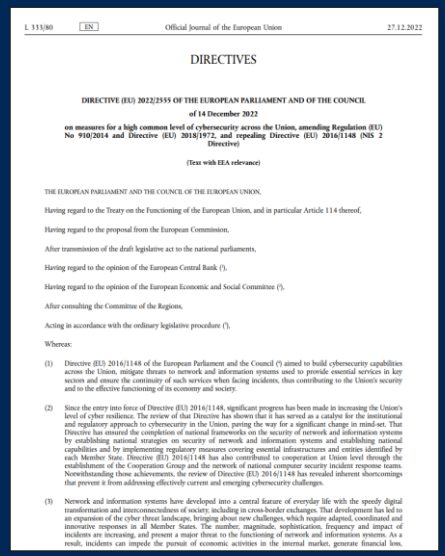
Organisering og regulering av nasjonal IKT-sikkerhet



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)

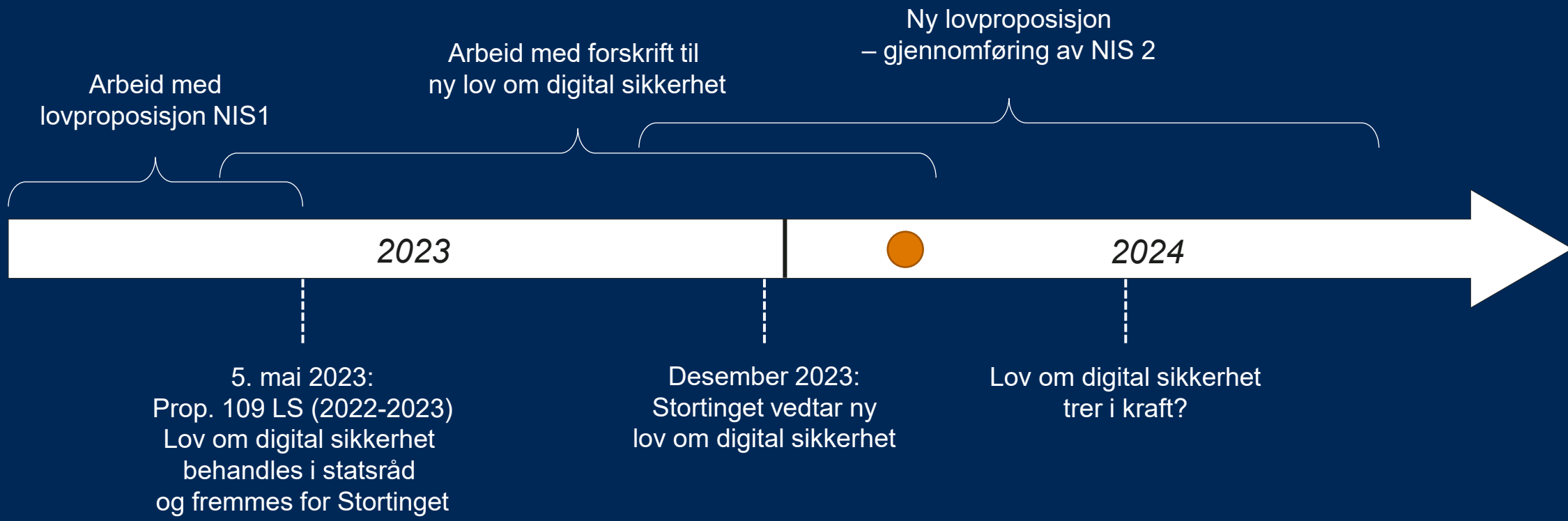
Høring - utkast til ny lov (2018-2019)

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

NIS 2 (2022)

Ny lovproposisjon NIS2

Status for lovarbeidet



NIS1-direktivet innføres i norsk rett gjennom ny lov om digital sikkerhet.
Det pågår lovarbeid for å forberede nødvendige endringer etter NIS2.

Forholdet til andre regelverk

NSM

Forholdet til sektorregelverk

- Noen av kravene er delvis ivaretatt i gjeldende sektorregelverk i dag
- Krav i ulike sektorregelverk varierer
  - Stilles i varierende grad krav til digital sikkerhet
  - Krav om varsling til myndighetene ved uønskede hendelser varierer
  - Tilsyn med og kompetanse innen digital sikkerhet varierer i ulike sektorer
- Der krav i sektorregelverk minst tilsvarer kravene som følger av ny lov om digital sikkerhet, medfører ny lov ikke store endringer for virksomheten
- 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 sektorregelverket
- Ny lov bidrar til å identifisere og lukke «gap»

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

NSM

Forholdet til sikkerhetsloven

- Finnes ingen tverrsektoriell lov som fullt ut dekker NIS-direktivet i dag
- NIS må ikke forveksles med sikkerhetsloven
  - ulike formål – NIS omhandler ikke nasjonal sikkerhet
  - forskjellige virkeområder – ulik tilnærming til hvilke virksomheter som omfattes
  - NIS er avgrenset til nettverk og informasjonssystemer
  - forskjellige tilsynsregimer
  - ulikt risikobilde
- I tilfeller som omhandler nasjonale sikkerhetsinteresser gjelder sikkerhetsloven
  - Skjermingsverdige verdier
  - Grunnleggende nasjonale funksjoner
- Godt forebyggende sikkerhetsarbeid i virksomhetene bygger likevel på en del gjenkjennelige sikkerhetsprinsipper

NSM

NIS virker sammen med andre EU-regelverk

CER-direktivet – Critical Entities Resilience Directive

- Overlappende virkeområde
- Virksomheter identifisert som kritiske etter CER-direktivet, omfattes av NIS2
- Krav til digital sikkerhet reguleres i NIS2

CSA – Cyber Security Act

- Etablering av et europeisk rammeverk for frivillig sertifisering av IKT-produkter og -tjenester
- NIS2 (artikkel 24) åpner for å stille krav om sertifiserte IKT-produkter eller –tjenester i anskaffelser/innkjøp

DORA – Digital Operational Resilience Act

- *Lex specialis* som regulerer digital sikkerhet i finanssektoren
- Forordning, ikke direktiv

Legges opp til samarbeid mellom kompetente myndigheter etter NIS, CER og DORA

Noen overordnede råd til virksomheter

NSM

Overordnet veiledning

Virksomhetene bør:

- Sørge for å ha etablert et ledelsessystem for sikkerhetsstyring, som:
  - inngår i virksomhetens overordnede ledelsessystem
  - gjennomgås av virksomhetens øverste ledelse
  - Dokumenteres
- Holde oversikt over nettverk og informasjonssystemer i virksomheten, inkludert avhengigheter til leverandører
- Systematisk vurdere risiko knyttet til nettverk og informasjonssystemer
- Iverksette sikkerhetstiltak som er tilpasset risiko, basert på beste praksis og anerkjente standarder og sikkerhetsrammeverk, og vurdere effekten av disse tiltakene
- Etablere rutiner for å ivareta plikten til å melde fra om alvorlige hendelser som rammer nettverk og informasjonssystemer i virksomheten

NSM

Noen nøkkelspørsmål virksomheter bør drøfte

- Vil vår virksomhet være ansett som «kritisk» eller «viktig» i forbindelse med NIS? Vil vi være omfattet av virkeområdet til ny lov om digital sikkerhet?
- Hvor moden er vår virksomhet og vår bransje med tanke på digital sikkerhet?
- Hvilke kritiske avhengigheter har vi i våre leverandørkjeder, særlig med tanke på informasjonssystemer? Hvilke underleverandører er vi avhengige av for at våre informasjonssystemer skal være sikre?
- Når gjennomførte vi sist 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?
- Har vi en god plan for hendelseshåndtering? Når ble den sist oppdatert?
- Er vårt arbeid med forebyggende digital sikkerhet godt forankret i ledelsen og kommunisert i virksomheten?