Omfattas vi av NIS2 och CSL?

Ett webbinarium med PTS
2024-05-22

Dagens agenda

9:30 PTS som myndighet

9:40 Grundläggande om cybersäkerhetslagen

10:30 Paus

10:45 Presentation av PTS självskattningsverktyg för identifiering

11:30 Avslut

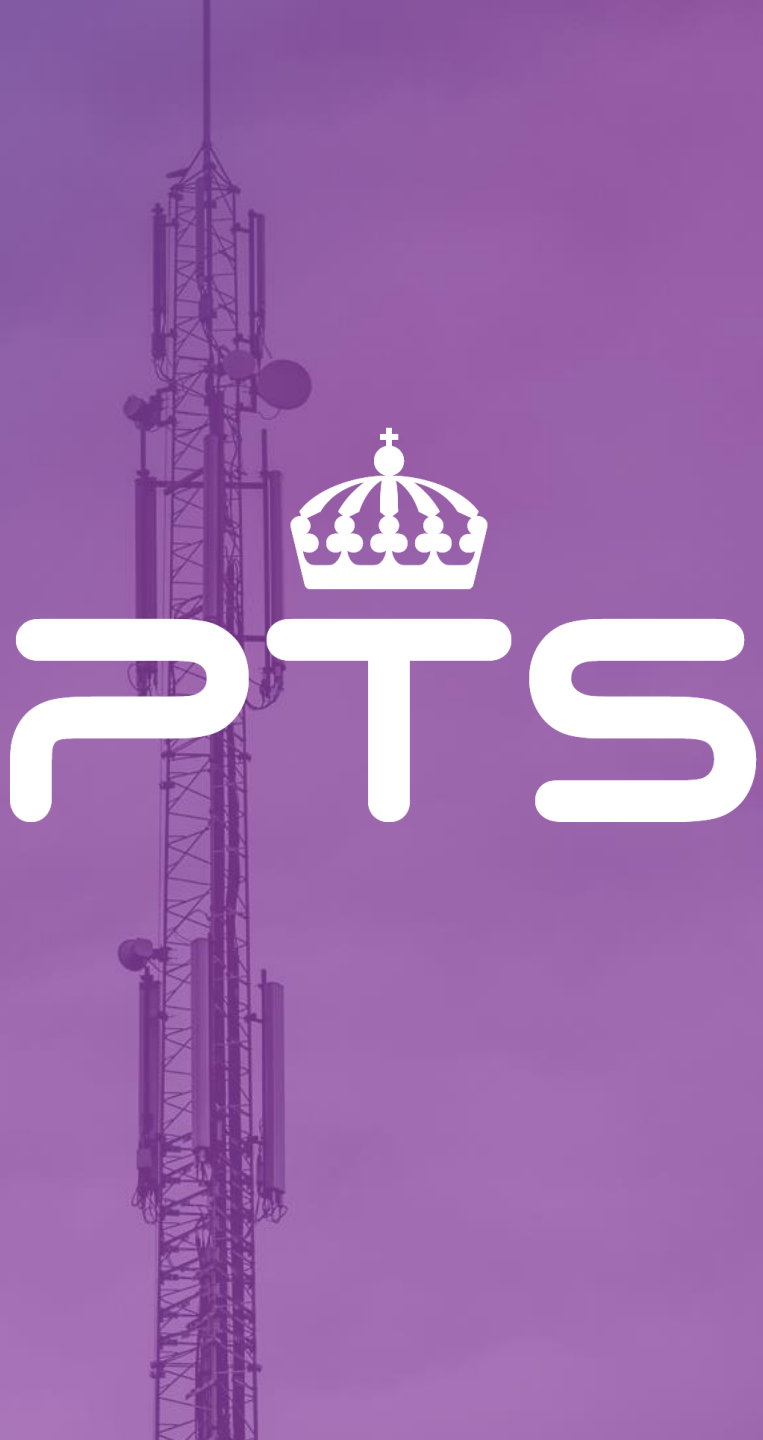
Kort om PTS och vår roll inom NIS

Enhetschef Isabelle Westerlund

Enheten för digitala och betrodda tjänster

Kort om PTS

- Statlig myndighet som lyder under Finansdepartementet.
- Generaldirektör Dan Sjöblom.
- Verksamhet i Stockholm, Kiruna och Malmö.
- 420 medarbetare.
- Vår verksamhet finansieras genom
  - avgifter som tas ut av företag och personer med tillstånd.
  - anslag från statsbudgeten.
- Myndigheten bildades 1992.



Vad gör PTS?

- Tillsynsmyndighet med sektorsansvar inom elektronisk kommunikation och post.
- **NIS,** PTS ansvar framgår bl.a. av
  - PTS instruktion
  - NIS-lagen
  - Förordningen om informationssäkerhet för samhällsviktiga och digitala tjänster.

PTS ansvar enligt den nuvarande NIS-lagen

Samhällsviktiga tjänster

- Energi
- Transport
- Bankverksamhet
- Finansmarknadsinfrastruktur
- Hälso- och sjukvård
- Leverans och distribution av dricksvatten
- **Digital infrastruktur**

Digitala tjänster

- **Internetbaserade marknadsplatser**
- **Internetbaserade sökmotorer**
- **Molntjänster**

Vad gör PTS inom NIS ?

- Tar fram föreskrifter om säkerhetsåtgärder
- Tar emot incidentrapporter
- Bedriver tillsyn med stöd av reglerna
- Samverkar → delar erfarenheter och harmoniserar regler
  - Nationellt
  - Internationellt

Grundläggande om cybersäkerhetslagen

Åsa Gihl, data- och systemvetare

Anders Franzén, ingenjör

Vad ska vi prata om?

1. Vad är NIS?
2. Vilka omfattas av NIS2/CSL?
3. Vad innebär det för de som omfattas av NIS2/CSL
4. PTS roll och ansvar inom CSL
5. Föreskrifter och genomförandeakter
6. Nästa steg

Vad är NIS?

Bakgrund

- NIS-direktivet trädde i kraft 2016
- Vad är syftet?
  - En hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela Unionen
- Direktiv måste implementeras
  - Svensk **NIS-lag** 2018,
  - PTS föreskrifter 2021
- Krav på säkerhet i nätverks- och informationssystem
  - Tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten
  - Anmälan till tillsynsmyndighet
  - Incidentrapportering
- NIS-direktivet tog sikte på **samhällsviktiga tjänster** inom 7 sektorer

Varför NIS2?

- Öka harmonisering och öka samarbete
- Fler sektorer och tjänster anses viktiga för den inre marknaden (från 7 till 19 sektorer)
- Beslutades i december 2022
- Ska vara implementerat i nationell lag 18 oktober 2024

Nyheter med NIS2

- Nya sektorer och fler områden inom resp. sektor
- Detaljerade regler kring riskhanteringsåtgärder
- Gemensamma regler kring incidentrapportering
- Ledningens ansvar
- Nya tillsynsverktyg som:
  - Anmärkning
  - Säkerhetsrevisioner, säkerhetsskanningar, övervakningsansvarig
  - Förbud att utöva ledningsfunktion
- Högre sanktionsbelopp, upp till 10 miljoner euro eller 2% av omsättningen

Vilka omfattas av NIS2/CSL

Vilka aktörer omfattas av NIS2 - högkritiska sektorer (Bilaga 1. NIS2-direktivet)

1. Energi
2. Transporter
3. Bankverksamhet
4. Finansmarknadsinfrastruktur
5. Hälso- och sjukvårdssektorn
6. Dricksvatten
7. Avloppsvatten
8. **Digital infrastruktur**
9. **Förvaltning av IKT-tjänster (mellan företag)**
10. Offentlig förvaltning
11. **Rymden**

Vilka aktörer omfattas av NIS2 – andra kritiska sektorer (Bilaga 2. NIS2-direktivet)

1. **Post- och budtjänster**
2. Avfallshantering
3. Tillverkning, produktion och distribution av kemikalier
4. Produktion, bearbetning och distribution av livsmedel
5. Tillverkning, medicintekniska produkter, datorer, elektronikvaror, maskiner, motorfordon, mm
6. **Digitala leverantörer**
7. Forskning

Sektor	Verksamhet	Stora företag fler än 250 anställda	Medelstora företag fler än 50 och färre än 250 anställda	Små- och mikroföretag färre än 50 anställda
Digital infrastruktur	Leverantörer av DNS-tjänster (med undantag för operatörer av rotnamnsservrar)	Väsentlig	Väsentlig	Väsentlig
	Registreringsenheter för toppdomäner	Väsentlig	Väsentlig	Väsentlig
	Kvalificerade tillhandahållare av kvalificerade betrodda tjänster	Väsentlig	Väsentlig	Väsentlig
	Internetknutpunkter (IXP)	Väsentlig	Viktig	Omfattas ej av NIS2
	Leverantörer av molntjänster	Väsentlig	Viktig	Omfattas ej av NIS2
	Leverantörer av datacentraltjänster	Väsentlig	Viktig	Omfattas ej av NIS2
	Leverantörer av nätverk för leverans av innehåll	Väsentlig	Viktig	Omfattas ej av NIS2
	Icke-kvalificerade tillhandahållare av betrodda tjänster	Väsentlig	Viktig	Viktig
	Tillhandahållare av allmänna elektroniska kommunikationsnät	Väsentlig	Väsentlig	Viktig
	Tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster	Väsentlig	Väsentlig	Viktig
Förvaltning av IKT-tjänster	Leverantörer av hanterade tjänster	Väsentlig	Viktig	Omfattas ej av NIS2
	Leverantörer av hanterade säkerhetstjänster	Väsentlig	Viktig	Omfattas ej av NIS2
Rymden	Operatörer av markbaserad infrastruktur	Väsentlig	Viktig	Omfattas ej av NIS2
Post- och budtjänster	Post- och budtjänster	Viktig	Viktig	Omfattas ej av NIS2
Digitala leverantörer	Leverantörer av marknadsplatser online	Viktig	Viktig	Omfattas ej av NIS2
	Leverantörer av sökmotorer	Viktig	Viktig	Omfattas ej av NIS2
	Leverantörer av plattformar för sociala nätverkstjänster	Viktig	Viktig	Omfattas ej av NIS2

Väsentliga och viktiga verksamhetsutövare

NIS2 delar upp sina tillsynsobjekt i två olika kategorier

- **Väsentliga** entiteter / verksamhetsutövare
- **Viktiga** entiteter / verksamhetsutövare

Olika möjligheter till tillsyn (ex ante och ex post)

Olika sanktionsbelopp

- maxbelopp på 7 MEUR vs 10MEUR,
- alternativt 1,4 % av årsomsättning vs 2 % av årsomsättning)

Huvudsakligen **storleken som styr** vilken typ av verksamhet ni är

Vad innebär det att omfattas av NIS2?

Vad innebär det för de som omfattas?

- **Identifiera**
  sig som en NIS2 aktör
- **Utbildning**
  av ledning och anställda
- **Vidta riskhanteringsåtgärder**
  för att skydda nätverk- och informationssystem
- **Informationssäkerhetsarbete**
  Systematiskt och riskbaserat
- **Anmäla sig**
  till tillsynsmyndighet (i rätt EU medlemsland)
- **Incidentrapportera**
  betydande incidenter
- **Informera kunder**
  (vid behov) om betydande incidenter och cyberhot

Riskhanteringsåtgärder (säkerhetsåtgärder)

- 3 kap 1 § delbetänkande CSL (artikel 21 NIS2)
- Tekniska,
- Driftsrelaterade och
- Organisatoriska riskhanteringsåtgärder
- Skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter.
- Allriskperspektiv och en riskanalys som utvärderas och innefattar 9 angivna krav.

Riskhanteringsåtgärder i CSL

1. Incidenthantering
2. Kontinuitetshantering
3. Säkerhet i leveranskedjan
4. Säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem inklusive hantering av sårbarheter och sårbarhetsinformation
5. Strategier och förfaranden för användning av kryptografi och kryptering
6. Personalsäkerhet
7. Strategier för åtkomstkontroll och tillgångsförvaltning
8. Säkrade lösningar för kommunikation
9. Lösningar för autentisering

Incidentrapportering

- NIS-incidenter rapporteras till CERT-SE (MSB)
- Tidig varning inom 24 timmar
- Incidentanmälan inom 72 timmar
- Slutrapport inom en månad
- Vid behov informera kunder
  - Vid betydande incidenter och betydande cyberhot
- Tillsynsmyndighet kan förelägga verksamhetsutövare att informera kunder om betydande cyberhot
- Skillnad mot tidigare NIS och LEK
- Integritetsincidenter hanteras fortsatt enligt LEK

Vilka incidenter ska rapporteras?

En händelse som undergräver tillgänglighet, autenticiteten, riktigheten eller konfidentialiteten och som:

- Har orsakat eller kan orsaka allvarliga driftsstörningar för tjänsterna eller ekonomiska förluster för entiteten.
  - Drabbade nätverks- och informationssystemen betydelse
  - Allvar och tekniska egenskaper hos cyberhot
  - Underliggande sårbarheter

Vilka incidenter ska rapporteras?

En händelse som undergräver tillgänglighet, autenticiteten, riktigheten eller konfidentialiteten och som:

- Har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada
  - I vilken utrstäckning påverkas tjänsten
  - Hur länge pågår incidenten
  - Hur många drabbade

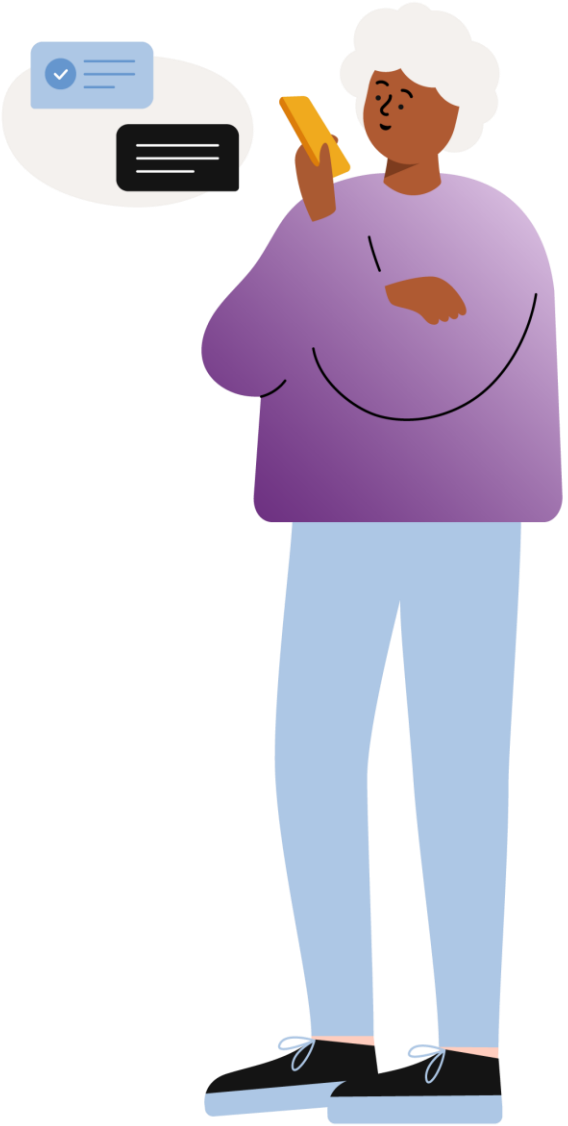
Incidentrapportering innehåll

Varningen ska ange: (24 timmar)

- om det finns misstanke om incidenten orsakats uppsåtligen och
- om den är gränsöverskridande

Incidentanmälan: (72 timmar)

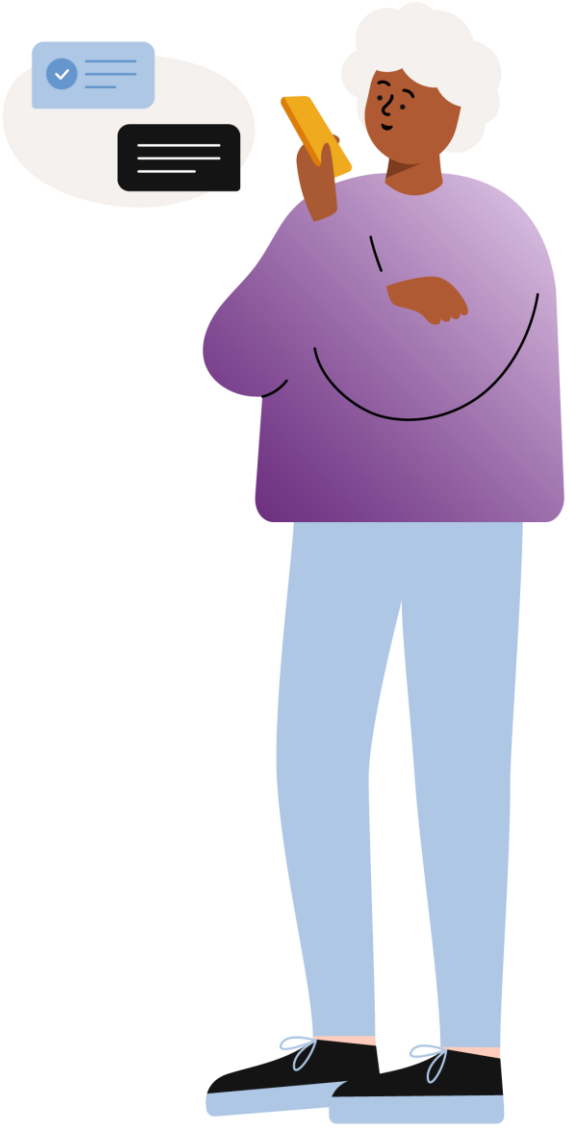
- inledande bedömning av hur allvarlig den betydande incidenten är,
- konsekvenserna av den och
- förekomsten av angreppsindikatorer.
- Vidare ska tidigare varning enligt 5 § uppdateras.



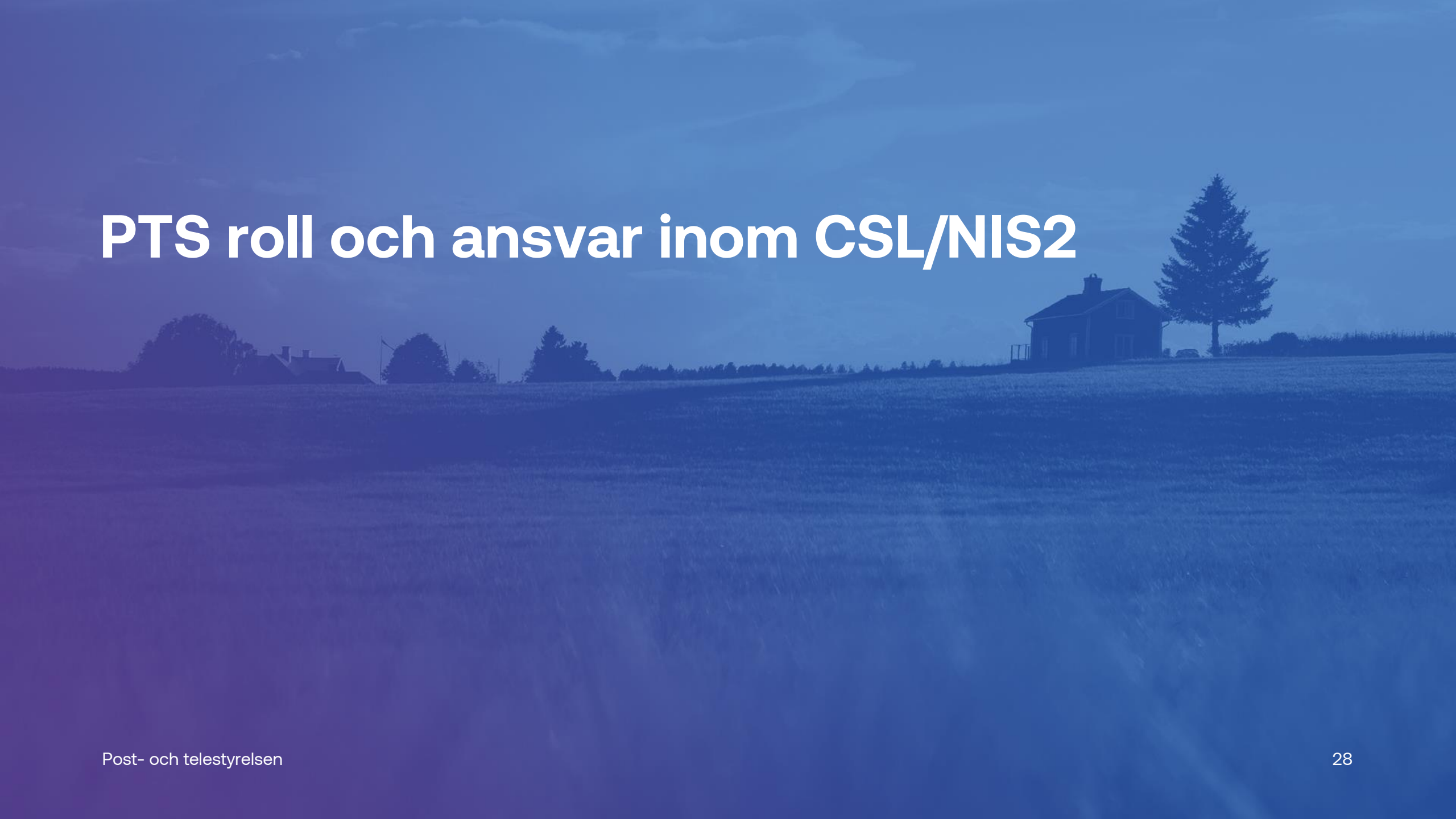
Incidentrapportering innehåll

Slutrapporten (4 veckor) ska innehålla en beskrivning av:

- Incidenten och dess konsekvenser,
- hur allvarlig incidenten bedöms vara,
- vad som sannolikt utlöst incidenten,
- åtgärderna för att begränsa incidenten, och
- incidentens möjliga gränsöverskridande effekter.



PTS roll och ansvar inom CSL/NIS2



PTS roll inom NIS2/cybersäkerhetslagen

- Tar emot anmälan
- Tar emot och utreder incidenter
- Genomför tillsyn
- Tar fram föreskrifter
- Deltar i samarbetsgrupper inom EU
- MSB har en samordningsroll

Föreskrifter och genomförandeakter

Föreskriftsrätt enligt delbetänkande CSL

- Om systematiskt och riskbaserat informationssäkerhetsarbete
  - Tillsynsmyndigheten
- Riskhanteringsåtgärder
  - Tillsynsmyndigheten
- Utbildning om riskhanteringsåtgärder
  - Tillsynsmyndigheten
- Vad som utgör en betydande incident och kring incidentrapporteringsregler
  - MSB

Genomförandeakt för riskhanteringsåtgärder och rapporteringsskyldigheter

- Senast den 17 oktober 2024 **ska** kommissionen anta genomförandeakter för att fastställa de tekniska och metodologiska specifikationerna för riskhanteringsåtgärderna
- Gäller för:
  - DNS-tjänster och registreringsenheter för toppdomäner
  - Molntjänster
  - Datacentraltjänster
  - CDN
  - Hanterade tjänster och hanterade säkerhetstjänster
  - Marknadsplatser online, sökmotorer och plattformar för sociala nätverkstjänster
  - Kvalificerade tillhandahållare av betrodda tjänster (ej för rapporteringsskyldigheter)

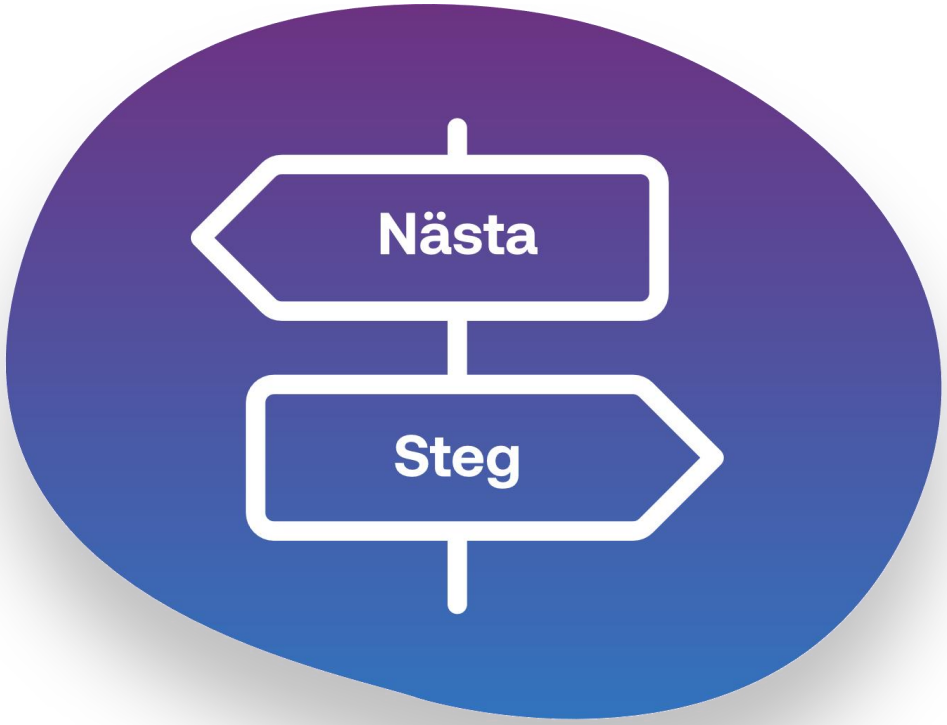
Cybersäkerhetslagen och CER-direktivet

- Nya lagen föreslås träda i kraft 1 januari 2025
- CER-direktivet under utredning
  - Ställer krav på fysisk säkerhet
  - Stora delar inom digital infrastruktur undantas från CER

Nästa steg

Nästa steg

- Följa upp proposition och fortsatta CER-utredningen
- Bevaka genomförandeakter
- Förbereda PTS internt med processer och IT-stöd
- Mer kommunikation under hösten
- Många saker oklara fortfarande




Frågor?

Paus till 10:45

Ny e-tjänst: *Omfattas vi av CSL?*

Anna Söyland, Jurist

Fanny Schönenberg, Jurist och UX-designer

Ny e-tjänst: Omfattas vi av CSL?

- Stöd för att hjälpa er utreda om ni omfattas av CSL
- Designad utifrån PTS sektoransvar
- Endast vägledande
- En typ av verksamhet i taget
- Lansering i slutet av juni

Demo: MoIntjänstföretaget MoInAB

- Software as a service-tjänster
- Sverige, Danmark och Tyskland
- Huvudkontor i Göteborg
- 350 anställda

Demo: Budtjänsten Kikis Expressbud AB

- Budtjänster
- Sverige, Danmark och Finland
- 25 anställda
- Årsomsättning under 10M €

Kikis Expressbud

Frågor?

Vad händer nu?

- ***Omfattas vi av CSL?*** lanseras i juni
- Förväntade justeringar av e-tjänsten
- Fler kommunikationsinsatser till hösten, se pts.se

- **nis@pts.se**

Tack för idag!

Kontakt: nis@pts.se