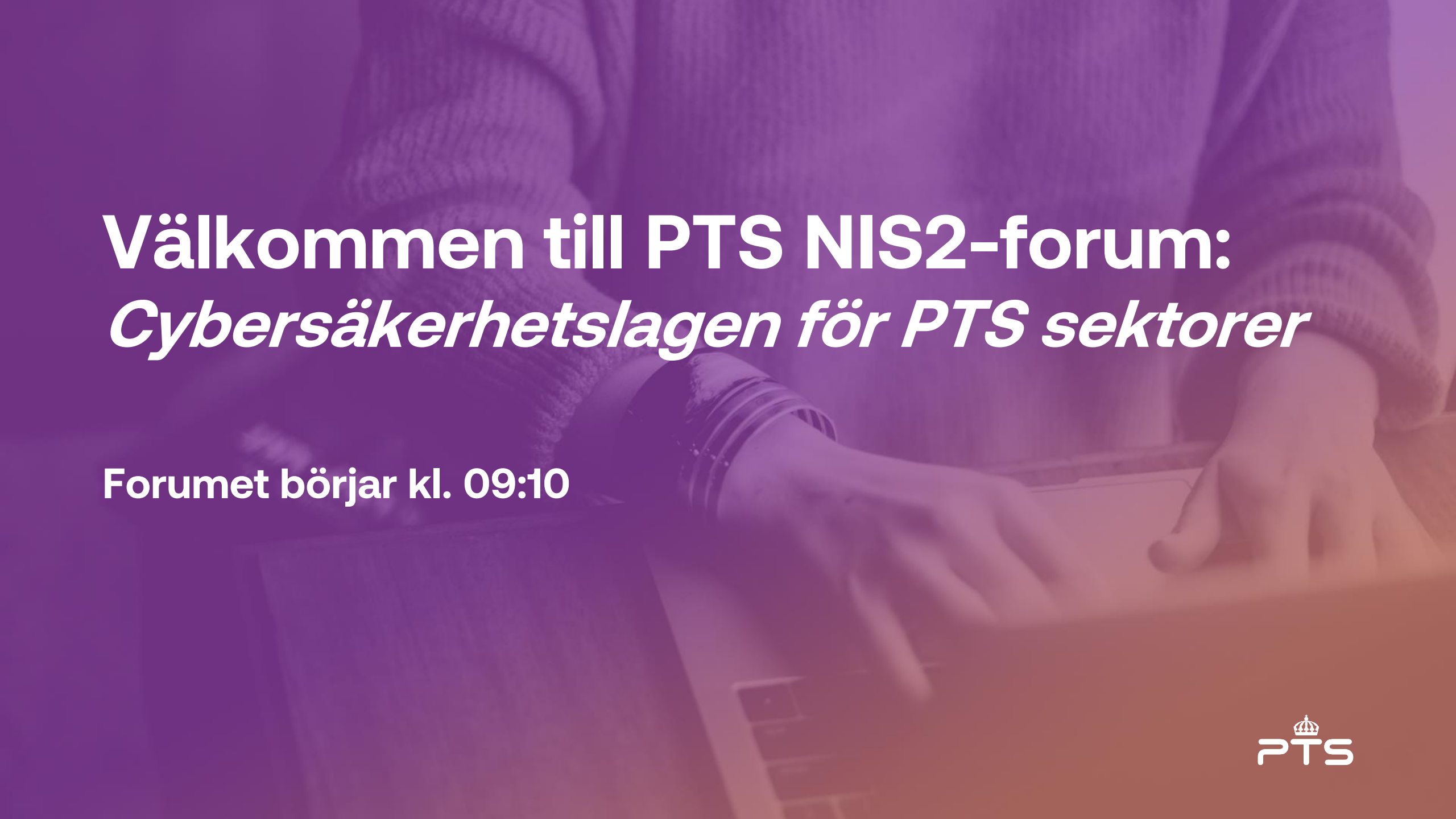
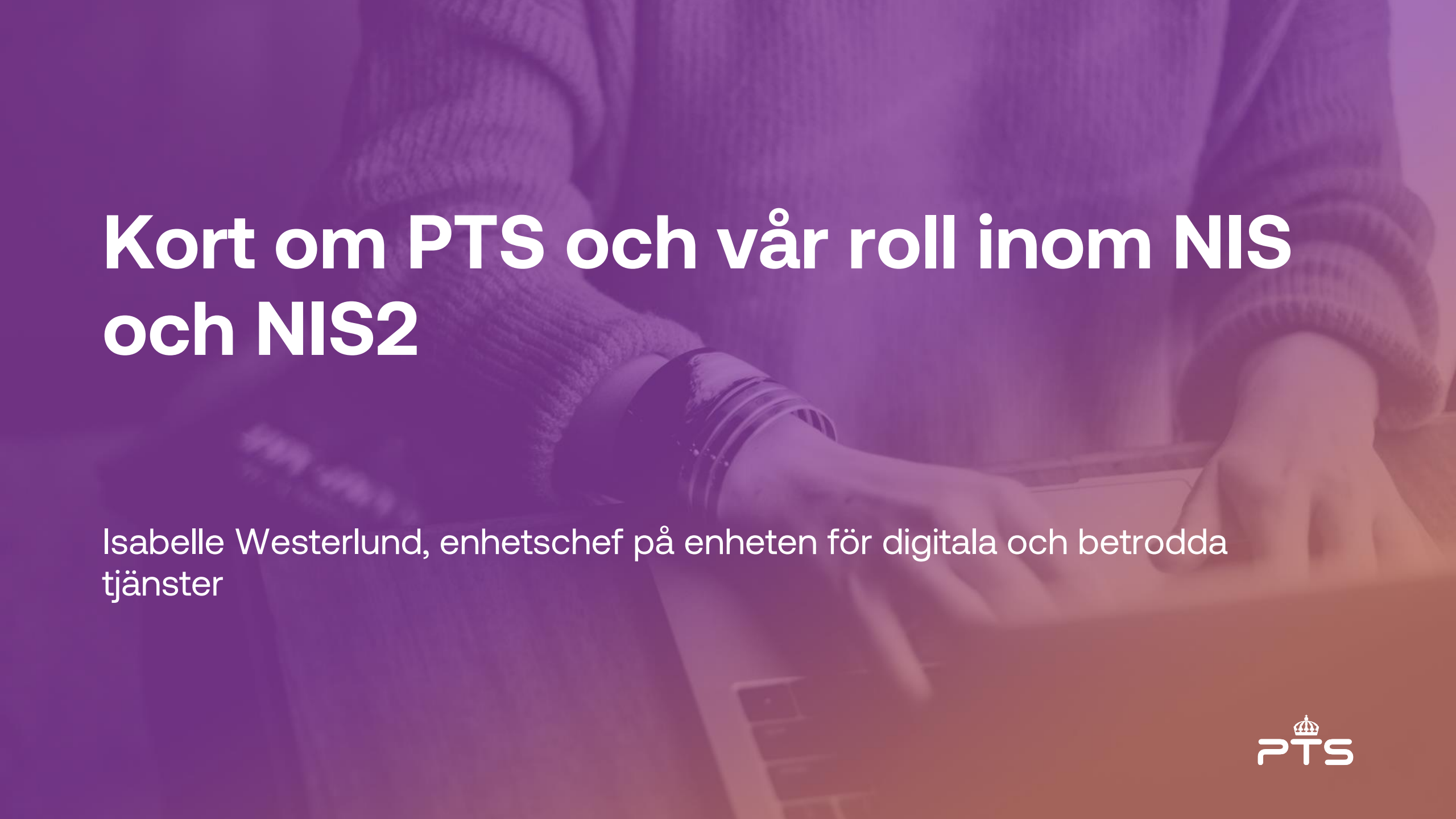


Välkommen till PTS NIS2-forum:
Cybersäkerhetslagen för PTS sektorer

Forumet börjar kl. 09:10

Dagens agenda

- 09.10-09.15 Välkomna!
- 09.15-09.25 PTS NIS2-arbete
- 09.25-10.15 Vilka regler gäller?
- 10.15-10.40 NIS2 i praktiken
- **10.40-11.10 Paus: Fika och mingel**
- 11.10-11.35 PTS panelsamtal
- 11.35-11.55 Verksamhetsutövare – viktig, väsentlig, registrering
- 11.55-12.00 Avslut – vad händer nu?



Kort om PTS och vår roll inom NIS och NIS2

Isabelle Westerlund, enhetschef på enheten för digitala och betrodda tjänster

Kort om PTS

- Post- och telestyrelsen (PTS) är en statlig myndighet som lyder under Finansdepartementet.
- Vår generaldirektör sedan 2017 heter Dan Sjöblom.
- Vi bedriver verksamhet i Stockholm, Kiruna och Malmö.
- På myndigheten arbetar cirka 420 medarbetare.
- Vår verksamhet finansieras till stor del av avgifter som tas ut av företag och personer med tillstånd. Övriga verksamheten finansieras genom 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, av NIS-lagen och av 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**

PTS kommande ansvar enligt cybersäkerhetslagen (förslag)

- Digital infrastruktur
- Förvaltning av IKT-tjänster (mellan företag)
- Rymden
- Post- och budtjänster
- Digitala leverantörer

Vad gör vi inom NIS ?

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

Vilka regler gäller?
– vad gäller nu – vad händer sen

Maria Wiberg, jurist, jur.dr EU-rätt

Frågor som tas upp

- Varför ändrar vi i EU-reglerna gällande cybersäkerhet?
- Hur förhåller sig NIS2-direktivet till direktivet om kritiska verksamheters motståndskraft (CER-direktivet)?
- Hur ser ”regelkartan” ut för olika verksamhetsutövare?
- Hur påverkas verksamhetsutövare nu när direktiven blivit tillämpliga (från 18 oktober 2024) men Sverige inte har någon lagstiftning på plats?

Varför ett NIS-direktiv?

Säkerhet i nät- och informationssystem

NIS-direktivet antogs 2016

- För att bygga upp cybersäkerheten i unionen

MEN

Krävs bättre säkerhet i fler sektorer

NIS2

Fler sektorer omfattas

NIS var för oprecist – skillnader uppstod mellan medlemsstaterna – kostsamt för verksamhetsutövare

NIS2

Mer detaljer och specificeringar

- Specificerade verksamheter
- Uppdelning i viktiga och väsentliga
- Alla verksamhetsutövare ska anmäla sig
- Bättre samarbete mellan myndigheter och medlemsstater

Olika regler i medlemsstaterna gällande bl.a.

- säkerhets- och incidentrapportering
- tillsyn och efterlevnadskontroll

NIS2

- Harmonisering av regler för incidenter och rapportering
- Harmonisering av tillsyn och efterlevnadskontroll,
- Sanktioner tydliggörs

Varför ett NIS-direktiv?

Säkerhet i nät- och informationssystem

NIS-direktivet antogs 2016

- För att bygga upp cybersäkerheten i unionen

MEN

NIS2-direktivet
Tillämpligt från och med 18 oktober 2024

Krävs bättre säkerhet i fler sektorer

NIS2

Fler sektorer omfattas

NIS var för oprecist – skillnader uppstod mellan medlemsstaterna – kostsamt för verksamhetsutövare

NIS2

- M… …fficeringar
- …rksamheter
- …ning i viktiga och väsentliga
- Alla verksamhetsutövare ska anmäla sig
- Bättre samarbete mellan myndigheter och medlemsstater

Olika regler i medlemsstaterna gällande bl.a.

- säkerhets- och incidentrapportering
- tillsyn och efterlevnadskontroll

NIS2

- Harmonisering av regler för incidenter och rapportering
- Harmonisering av tillsyn och efterlevnadskontroll,
- Sanktioner tydliggörs

Varför ett NIS-direktiv?

Säkerhet i nät- och informationssystem

NIS-direktivet antogs 2016

- För att bygga upp cybersäkerheten i unionen

MEN

Förslag SOU 2024:18
- **Cybersäkerhetslagen (CSL)**
- **Förordning om cybersäkerhet**

Även ändringar i bl.a.
- Lagen om elektronisk kommunikation
- Förordning om elektronisk kommunikation
- Lagen om nationella toppdomäner

Krävs bättre säkerhet i fler sektorer

NIS2

Fler sektorer omfattas

NIS var för oprecist – skillnader uppstod mellan medlemsstater för verksamhetsutövare

…ar
…ter
…äsentliga
…ka anmäla sig
…yndigheter och

…gällande bl.a.

…ncidentrapportering
…och efterlevnadskontroll

NIS2

- Harmonisering av regler för incidenter och rapportering
- Harmonisering av tillsyn och efterlevnadskontroll,
- Sanktioner tydliggörs

CER-direktivet – fokus på fysisk säkerhet

Direktiv från 2008 om klassificering av infrastruktur i **energi- och transportsektorerna** som kritisk infrastruktur där störningar kunde få betydande **gränsöverskridande konsekvenser**

Utvärdering 2019 – **skyddsåtgärderna var inte tillräckliga** – fler sektorer är **sammankopplade och gränsöverskridande**

CER-direktivet ger

Tydligare regler om kritiska entiteters motståndskraft

- Fler sektorer
- Tydliggör kritiska verksamhetsutövares roll och uppgifter

CER-direktivet – fokus på fysisk säkerhet

Direktiv från 2008 om klassificering av infrastruktur i **energi- och transportsektorerna** som kritisk infrastruktur där störningar k… betydande **gränsöverskridan…**

CER-di… **…a entiteters**

Utvärdering 2019 – … **tillräckliga** – fler sek… **och gränsöverskrid…** …rksamhetsutövares roll

CER-direktivet
Tillämpligt från och med 18 oktober 2024

Sektorn **digital infrastruktur är undantagen** från CER - NIS2 ger tillräcklig säkerhetsnivå – men medlemsstaterna ska peka ut kritiska verksamheter … gifter

CER-direktivet – fokus på fysisk säkerhet

Direktiv från 2008 om klassificering av
infrastruktur i **energi- och transportsektorerna**
som kritisk infrastruktur där störning
betydande **gränsöverskrid**

CER

ters

Utvärder
tillräcklig
och gräns

samhetsutövares roll

Förslag SOU 2024:64

- **Lag om motståndskraft hos kritiska verksamhetsutövare (LOM)**
- **Förordning om motståndskraft hos kritiska verksamhetsutövare**

Gällande nationella och EU-regler

Bestämmelser som inte gäller nu

LEK – lagen om elektronisk kommunikation
- Förordning om elektronisk kommunikation
  - Nationella föreskrifter

Grundas på direktivet om inrättande av en europeisk kodex för elektronisk kommunikation

NIS-lagen – lagen om informationssäkerhet för samhällsviktiga och digitala tjänster
- Förordning om informationssäkerhet för samhällsviktiga och digitala tjänster
  - Nationella föreskrifter

Grundas på NIS-direktivet från 2016

Cybersäkerhetslagen
Ändringar av bestämmelser i bl.a. LEK
Förordning
Föreskrifter (ex. från PTS)
Genomför NIS2-direktivet

eIDAS ”pekar” på uppfyllelse av NIS2-direktivet gällande incidenter och riskhanteringsåtgärd

Cybersäkerhetslagen

eIDAS-förordningen
Lagen (2016:561) om kompletterande bestämmelser till EU:s förordning om elektronisk identifiering

NIS-genomförande-förordning – upphörde att gälla 6 november 2024

NIS 2-genomförandeförordning – gäller från 7 november 2024

Proposition?

Sen – 2025

18 oktober 2024 | 7 november 2024 | Våren 2025

Lag om motståndskraft hos kritiska verksamhetsutövare
Förordning
Föreskrifter
Genomför CER-direktivet
(**digital infrastruktur undantaget**) – gäller fullt ut för sektorn rymden

Gällande nationella och EU-regler

Bestämmelser som inte gäller nu

LEK – lagen om elektronisk kommunikation
- Förordning om elektronisk kommunikation
- Nationella föreskrifter

Grundas på direktivet om inrättande av en europeisk kodex för elektronisk kommunikation

NIS-lagen – lagen om informationssäkerhet för samhällsviktiga och digitala tjänster
- Förordning om informationssäkerhet för samhällsviktiga och digitala tjänster

Grundas på NIS-direktivet från 2016

NIS2-direktivet behöver ”beaktas” när man tolkar de nationella reglerna

eIDAS ”pekar” på uppfyllelse av NIS2-direktivet gällande incidenter och riskhanteringsåtgärd

eIDAS-förordningen

Lagen (2016:561) om kompletterande bestämmelser till EU:s förordning om elektronisk identifiering

NIS-genomförande-förordning – upphörde att gälla 6 november 2024

NIS 2-genomförandeförordning – gäller från 7 november 2024

Cybersäkerhetslagen
Ändringar av bestämmelser i bl.a. LEK
Förordning
Föreskrifter (ex. från PTS)
Genomför NIS2-direktivet

Cybersäkerhetslagen

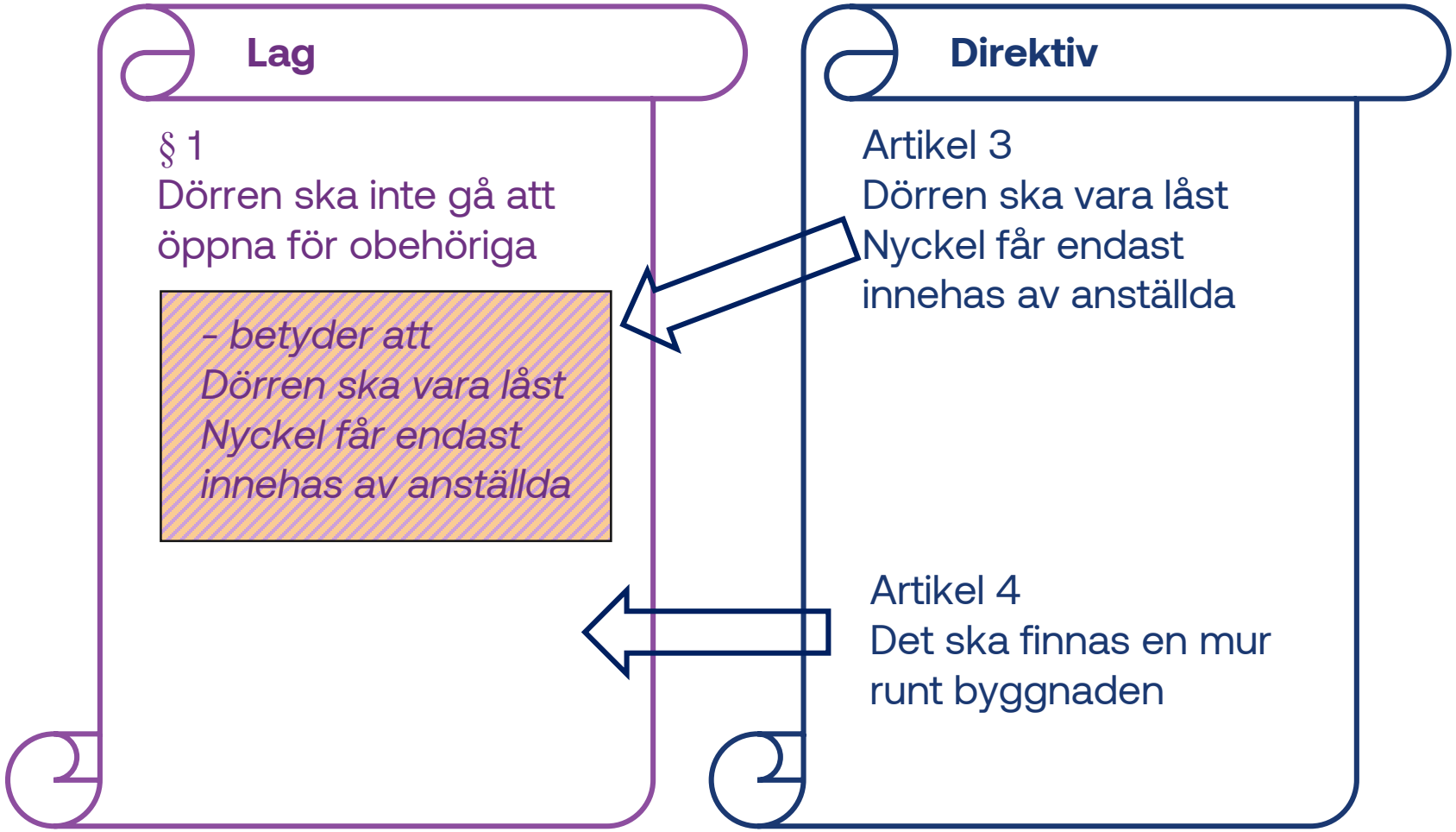
Proposition?

Sen – 2025

18 oktober 2024 **7 november 2024** **Våren 2025**

Lag om motståndskraft hos kritiska verksamhetsutövare
Förordning
Föreskrifter
Genomför CER-direktivet
(**digital infrastruktur undantaget**) – gäller fullt ut för sektorn rymden

Vad innebär att man ska ”beakta/tolka i ljuset av”?



Vad innebär att man ska ”beakta/tolka i ljuset av”?

PTS Sektorer (förslag)

- Digital infrastruktur
- Digitala leverantörer
- Förvaltning av IKT-tjänster
- Digital infrastruktur
- Rymden
- Post och budtjänster

NIS2

Verksamhetsutövare	NIS-regelverket	Nationella föreskrifter	NIS-Genom-förande-förordning	NIS2-Genom-förande-förordning	LEK	eIDAS-förordning	CER

PTS Sektorer (förslag)

- Digital infrastruktur
- Digitala leverantörer
- Förvaltning av IKT-tjänster
- Digital infrastruktur
- Rymden
- Post och budtjänster

NIS2

Verksamhetsutövare	NIS-regelverket	Nationella föreskrifter	NIS-Genom-förande-förordning	NIS2-Genom-förande-förordning	LEK	eIDAS-förordning	CER
Allmänna elektroniska kommunikationsnät							
Allmänt tillgängliga kommunikationstjänster							
DNS-tjänster							
Registreringsenheter för toppdomäner							
Molntjänster							
Sökmotorer							
Marknadsplatser online							
Plattformar för sociala tjänster							
Utlokaliserade driftstjänster							
Utlokaliserade säkerhetstjänster							
Datacentraler							
Nätverk för lev av innehåll							
Betrodda tjänster							
Internetknutpunkter							
Rymden (markbaserad infrastr.)							
Post- och budtjänster							

NIS2 och kommande CSL

LOM

PTS Sektorer (förslag)

- Digital infrastruktur
- Digitala leverantörer
- Förvaltning av IKT-tjänster
- Digital infrastruktur
- Rymden
- Post och budtjänster

Verksamhetsutövare	NIS-regelverket	Nationella föreskrifter	NIS-Genom-förande-förordning	NIS2-Genom-förande-förordning	LEK		eIDAS-förordning	CER
Allmänna elektroniska kommunikationsnät		Säkerhetsföreskrifter ”Beakta” NIS2			Säkerhet ”Beakta” NIS2			Utses
Allmänt tillgängliga kommunikationstjänster		Säkerhetsföreskrifter ”Beakta” NIS2			Säkerhet ”Beakta” NIS2			Utses

Korresponderande skyldigheter tolkas i ljuset av NIS2

Opåverkade bestämmelser

Bestämmelser som inte gäller nu

PTS Sektorer (förslag)

- Digital infrastruktur
- Digitala leverantörer
- Förvaltning av IKT-tjänster
- Digital infrastruktur
- Rymden
- Post och budtjänster

NIS2

Verksamhetsutövare	NIS-regelverket	Nationella föreskrifter	NIS-Genom-förande-förordning	NIS2-Genom-förande-förordning	LEK	eIDAS-förordning	CER
Allmänna elektroniska kommunikationsnät		Säkerhetsföreskrifter ”Beakta” NIS2			Säkerhet ”Beakta” NIS2		Utses
Allmänt tillgängliga kommunikationstjänster		Säkerhetsföreskrifter ”Beakta” NIS2			Säkerhet ”Beakta” NIS2		Utses
DNS-tjänster	”Beakta” NIS2	NIS-föreskrifter ”Beakta” NIS2					Utses
Registreringsenheter för toppdomäner	”Beakta” NIS2	NIS-föreskrifter ”Beakta” NIS2					Utses

Korresponderande skyldigheter tolkas i ljuset av NIS2

Bestämmelser som inte gäller nu

PTS Sektorer (förslag)

- Digital infrastruktur
- Digitala leverantörer
- Förvaltning av IKT-tjänster
- Digital infrastruktur
- Rymden
- Post och budtjänster

NIS2

Verksamhetsutövare	NIS-regelverket	Nationella föreskrifter	NIS-Genom-förande-förordning	NIS2-Genom-förande-förordning	LEK	eIDAS-förordning	CER
Allmänna elektroniska kommunikationsnät		Säkerhetsföreskrifter ”Beakta” NIS2			Säkerhet ”Beakta” NIS2		Utses
Allmänt tillgängliga kommunikationstjänster		Säkerhetsföreskrifter ”Beakta” NIS2			Säkerhet ”Beakta” NIS2		Utses
DNS-tjänster	”Beakta” NIS2	NIS-föreskrifter ”Beakta” NIS2					Utses
Registreringsenheter för toppdomäner	”Beakta” NIS2	NIS-föreskrifter ”Beakta” NIS2					Utses
Molntjänster	”Beakta” NIS2						Utses
Sökmotorer	”Beakta” NIS2						
Marknadsplatser online	”Beakta” NIS2						

Korresponderande skyldigheter tolkas i ljuset av NIS2

Direkt tillämpliga

Bestämmelser som inte gäller nu

NIS2

PTS Sektorer (förslag)

- Digital infrastruktur
- Digitala leverantörer
- Förvaltning av IKT-tjänster
- Digital infrastruktur
- Rymden
- Post och budtjänster

Verksamhetsutövare	**NIS-regelverket**	**Nationella föreskrifter**	**NIS-** Genom-förande-förordning	**NIS2-** Genom-förande-förordning	**LEK**	**eIDAS-förordning**	**CER**
Allmänna elektroniska kommunikationsnät		Säkerhetsföreskrifter ”Beakta” NIS2			Säkerhet ”Beakta” NIS2		Utses
Allmänt tillgängliga kommunikationstjänster		Säkerhetsföreskrifter ”Beakta” NIS2			Säkerhet ”Beakta” NIS2		Utses
DNS-tjänster	”Beakta” NIS2	NIS-föreskrifter ”Beakta” NIS2					Utses
Registreringsenheter för toppdomäner	”Beakta” NIS2	NIS-föreskrifter ”Beakta” NIS2					Utses
Molntjänster	”Beakta” NIS2						Utses
Sökmotorer	”Beakta” NIS2						
Marknadsplatser online	”Beakta” NIS2						
Plattformar för sociala tjänster							
Utlokaliserade driftstjänster							
Utlokaliserade säkerhetstjänster							
Datacentraler							Utses
Nätverk för lev av innehåll							Utses

Bestämmelser som inte gäller nu

NIS2

PTS Sektorer (förslag)

- Digital infrastruktur
- Digitala leverantörer
- Förvaltning av IKT-tjänster
- Digital infrastruktur
- Rymden
- Post och budtjänster

Verksamhetsutövare	NIS-regelverket	Nationella föreskrifter	NIS-Genom-förande-förordning	NIS2-Genom-förande-förordning	LEK	eIDAS-förordning	CER
Allmänna elektroniska kommunikationsnät		Säkerhetsföreskrifter ”Beakta” NIS2			Säkerhet ”beakta”		Utses
Allmänt tillgängliga kommunikationstjänster		Säkerhetsföreskrifter ”Beakta” NIS2			Säkerhet ”beakta”		Utses
DNS-tjänster	”Beakta” NIS2	NIS-föreskrifter ”Beakta” NIS2					Utses
Registreringsenheter för toppdomäner	”Beakta” NIS2	NIS-föreskrifter ”Beakta” NIS2					Utses
Molntjänster	”Beakta” NIS2						Utses
Sökmotorer	”Beakta” NIS2						
Marknadsplatser online	”Beakta” NIS2						
Plattformar för sociala tjänster							
Utlokaliserade driftstjänster							
Utlokaliserade säkerhetstjänster							
Datacentraler							Utses
Nätverk för lev av innehåll							Utses
Betrodda tjänster				Krav eIDAS			Utses

Direkt tillämplig

Kraven i eIDAS-förordningen ”pekar” på riskhanteringsåtgärder, som tydliggörs genom genomförandeförordningen

Bestämmelser som inte gäller nu

NIS2

PTS Sektorer (förslag)

PTS Sektorer (förslag)	Verksamhetsutövare	NIS-regelverket	Nationella föreskrifter	NIS-Genom-förande-förordning	NIS2-Genom-förande-förordning	LEK	eIDAS-förordning	CER
Digital infrastruktur	**Allmänna elektroniska kommunikationsnät**		Säkerhetsföreskrifter ”Beakta” NIS2			Säkerhet ”beakta”		Utses
	Allmänt tillgängliga kommunikationstjänster		Säkerhetsföreskrifter ”Beakta” NIS2			Säkerhet ”beakta”		Utses
	DNS-tjänster	”Beakta” NIS2	NIS-föreskrifter ”Beakta” NIS2					Utses
	Registreringsenheter för toppdomäner	”Beakta” NIS2	NIS-föreskrifter ”Beakta” NIS2					Utses
	Molntjänster	”Beakta” NIS2						Utses
Digitala leverantörer	Sökmotorer	”Beakta” NIS2						
	Marknadsplatser online	”Beakta” NIS2						
	Plattformar för sociala tjänster							
Förvaltning av IKT-tjänster	**Utlokaliserade driftstjänster**							
	Utlokaliserade säkerhetstjänster							
Digital infrastruktur	**Datacentraler**							Utses
	Nätverk för lev av innehåll							Utses
	Betrodda tjänster				Krav eIDAS			Utses
	Internetknutpunkter	NIS-direktivet	Säkerhetsföreskrifter ”Beakta” NIS2			Säkerhet ”beakta”		Utses
Rymden								
Post och budtjänster								

Omfattas av NIS-direktivet men regleras i LEK – därav tolkas LEK i enlighet med NIS2

Bestämmelser som inte gäller nu

NIS2

PTS Sektorer (förslag)	Verksamhetsutövare	NIS-regelverket	Nationella föreskrifter	NIS-Genom-förande-förordning	NIS2-Genom-förande-förordning	LEK	eIDAS-förordning	CER
Digital infrastruktur	**Allmänna elektroniska kommunikationsnät**		Säkerhetsföreskrifter ”Beakta” NIS2			Säkerhet ”beakta”		Utses
	Allmänt tillgängliga kommunikationstjänster		Säkerhetsföreskrifter ”Beakta” NIS2			Säkerhet ”beakta”		Utses
	DNS-tjänster	”Beakta” NIS2	NIS-föreskrifter ”Beakta” NIS2					Utses
	Registreringsenheter för toppdomäner	”Beakta” NIS2	NIS-föreskrifter ”Beakta” NIS2					Utses
	Molntjänster	”Beakta” NIS2						Utses
Digitala leverantörer	Sökmotorer	”Beakta” NIS2						
	Marknadsplatser online	”Beakta” NIS2						
	Plattformar för sociala tjänster							
Förvaltning av IKT-tjänster	**Utlokaliserade driftstjänster**							
	Utlokaliserade säkerhetstjänster							
Digital infrastruktur	**Datacentraler**							Utses
	Nätverk för lev av innehåll							Utses
	Betrodda tjänster				Krav eIDAS			Utses
	Internetknutpunkter	NIS-direktivet	Säkerhetsföreskrifter ”Beakta” NIS2			Säkerhet ”beakta”		Utses
Rymden	**Rymden (markbaserad infrastr.)**							**Fullt ut**
Post och budtjänster	**Post- och budtjänster**							

Sektorn rymden omfattas fullt ut

Tack!

Maria Wiberg, jurist, jur.dr EU-rätt

Introduktion genomförandeakter

Anders Franzén, civilingenjör

Vad är en genomförandeakt?

- Kommissionen beslutar om
  - Direktiv
  - Förordningar
- Ibland behövs mer enhetliga och detaljerade villkor → genomförandeakter
- Ungefär som föreskrifter

Genomförandeakter i NIS2

- NIS2 är ett direktiv → nationell lag för att implementera
- I NIS2-direktivet står det att kommissionen ska ta fram två genomförandeakter som ska
  - fastställa de tekniska och metodologiska specifikationerna för riskhanteringsåtgärder
  - närmare ange när en incident ska anses vara betydande och därmed rapporteras
- I praktiken blev det **en (1)** genomförandeakt
  - vilka incidenter som är betydande beskrivs i artiklar
  - riskhanteringsåtgärderna ligger i en bilaga
- Genomförandeakterna i NIS2 är en genomförandeförordning = direkt tillämpliga

Följande sektorer omfattas av genomförandeförordning

- Digital infrastruktur
  - IXP
  - DNS
  - Moln
  - Datacenter
  - CDN
  - Betrodda tjänster
  - Telekom, dvs operatörer
- IKT-tjänster
  - Utlokaliserade drifttjänster
  - Utlokaliserade säkerhetstjänster
- Digitala leverantörer
  - Marknadsplatser
  - Sökmotorer
  - Sociala nätverkstjänster
- Rymden
- Post- och budtjänster

Process för framtagande av genomförandeförordning

- Kommittéförfarande
- Utkast skickades ut i slutet av juni
- Lades samtidigt ut publikt under en 4-veckorsperiod
- Tre möten med representanter från alla medlemsländer
- Sista mötet ett beslutsmöte då genomförandeakterna antogs
- Skulle börja gälla 18 oktober men i praktiken blev det 7 november
- Kommissionens genomförandeförordning 2024/2690

Disposition av genomförandeförordningen

- 43 skäl som ger mer detaljerad förklaring till innehållet
- Art. 3-14 definierar en **betydande incident**, dvs när en incident ska rapporteras
- Uppdelat på horisontella och vertikala trösklar
  - Artikel 3-4 är horisontella trösklar
  - Artikel 5-14 är vertikala trösklar dvs specifika trösklar för respektive sektor
- Bilagan innehåller de riskhanteringsåtgärder som ska vidtas

Horisontella trösklar, artikel 3 och 4

- Har orsakat skada över € 500 000 eller 5% av omsättning
- Företagshemlighet kan eller har försvunnit
- Orsakat eller kan orsaka dödsfall, eller betydande skada på hälsa
- Framgångsrik obehörig åtkomst till nätverk- och informationssystem
- En incident har inträffat
  - minst två gånger inom sex månader,
  - har samma grundorsak **och**
  - kan tillsammans orsaka skada enligt första punkten

Vertikala trösklar för respektive sektor

- Helt otillgänglig mellan 0 och 30 minuter eller för mer än 5 % av användarna
- Svarstiden över 10 sekunder för vissa
- Tillgängligheten är begränsad för 5 % eller 1 miljon av användarna
- Riktighet, konfidentialitet eller autenticitet påverkad i olika utsträckning och beroende på om det är avsiktligt eller av misstag

Bilaga - riskhanteringsåtgärder

- Art. 21.2 i NIS2-direktivet
- Koppling till svenska föreskrifter?
- Förbättringspotential i den svenska översättningen
- Strategier mm ska ses över med planerade intervall eller när någon har hänt förutom 1.1.2, 2.1.4, 10.1.3 där det ska göras årligen samt dokumenteras

Några intressanta skäl

- Skäl 4, 5, 6
  - Proportionalitetsprincipen
- Skäl 7,
  - ENISA har tagit fram vägledning som nu är ute på remiss
- Skäl 31,
  - Tidsfristen börjar löpa from. att verksamhetsutövaren får kännedom om händelsen
- Skäl 36
  - Ta hänsyn till alla ekonomiska förluster som incidenten orsakat vid beräkning

Riskhanteringsåtgärder

- Kapitel 1, strategi för säkerhet i nätverk- och informationssystem
- **Kapitel 2, strategi för riskhantering**
- Kapitel 3, incidenthantering
- Kapitel 4, driftskontinuitet och krishantering
- **Kapitel 5, säkerhet i leveranskedjan**
- Kapitel 6, säkerhet vid förvärv, förändringshantering, säkerhetstestning, patchning, nätverkssäkerhet, sårbarhetshantering
- Kapitel 7, strategier för att bedöma effektiviteten i riskhanteringsåtgärder
- Kapitel 8, cyberhygien
- Kapitel 9, kryptering
- **Kapitel 10, personalsäkerhet**
- Kapitel 11, åtkomstkontroll
- Kapitel 12, hantering av tillgångar
- **Kapitel 13, fysisk säkerhet**

Kapitel 2 - strategi för riskhantering

- Ta fram ett ramverk för riskhantering
  - Bedöma risker, allriskansats
  - Analysera hot, sannolikhet, konsekvenser
  - Implementera en riskhanteringsplan
  - Identifiera ansvariga
  - Dokumentera
  - Godkännande av ledningen
- Övervaka efterlevnaden av strategin
- Oberoende granskning

Kapitel 5 - säkerhet i leveranskedjan

- Ta fram strategi för säkerhet i leveranskedjan
- Ha kriterier för vilka leverantörer man ska ingå avtal med
- Genom SLA eller avtal säkerställa ett antal krav på leverantörer
- Följa upp strategin genom att
  - Övervaka rapportering från SLA
  - Granska incidenter från leverantörer
- Ha ett register över alla leverantörer

Kapitel 10 - personalsäkerhet

- Säkerställa att anställda och leverantörer förstår vilka säkerhetsuppgifter de är ansvariga för
- Användare och ledningen agerar i enlighet med sin roller
- Se över tilldelningen av roller och uppdatera minst en gång per år, avsnitt 1.2
- Genomföra bakgrundskontroller om det är lämpligt
- Rutin för avslutad eller ändrad anställning
- Disciplinära förfaranden vid överträdelser

Kapitel 13 - fysisk säkerhet

- Skydd mot strömavbrott och andra försörjningstjänster
- Överväga redundans i försörjningstjänster
- Övervaka och testa skydden
- Förhindra eller begränsa fysiska hot, både avsiktlig och miljömässiga
- Förhindra och övervaka obehörigt fysiskt tillträde

Sammanfattning genomförandeförordning

- Två delar, incidenttrösklar och riskhanteringsåtgärder
- Genomförandeförordningen gäller för vissa sektorer men har betydelse för alla

Länkar

- NIS2-direktivet
- Kommissionens genomförandeförordning 2024/2690
- ENISA:s vägledning till genomförandeförordning

Frågor från er

NIS2 i praktiken – var ska vi börja?

Erika Hersaeus, senior cybersäkerhetshandläggare

Innehåll

1. **Centralt uttryck - säkerhet i nätverks- och informationssystem**
2. **NIS2 i praktiken - var ska vi börja? Tips på metodstöd och tillvägagångssätt.**
3. **Riskhanteringsåtgärder** som kan vara **lämpliga att börja med**.
4. **Vad tillsynsobjekt ofta missar?** Tips till tillsynsobjekt att beakta i riskhanteringsarbetet!
5. **Vanliga orsaker till inträffade incidenter av betydande omfattning i telekom** – värdefulla insikter för fler?

Säkerhet i nätverks- och informationssystem och deras fysiska miljö

Definitionen av säkerhet

”säkerhet i nätverks- och informationssystem”: **nätverks- och informationssystems förmåga** att med en viss tillförlitlighetsnivå **motstå händelser** som **kan undergräva tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten** hos

- *lagrade*,
- *överförda eller*
- *behandlade uppgifter eller*
- *hos de tjänster som erbjuds genom eller*
- *är tillgängliga via dessa nätverks- och informationssystem*.

T R A K ska upprätthållas

1. Tillgänglighet
2. Riktighet
3. Autenticitet
4. Konfidentialitet

i era nätverks- och informationssystem.

Var ska vi börja?

Några utgångspunkter

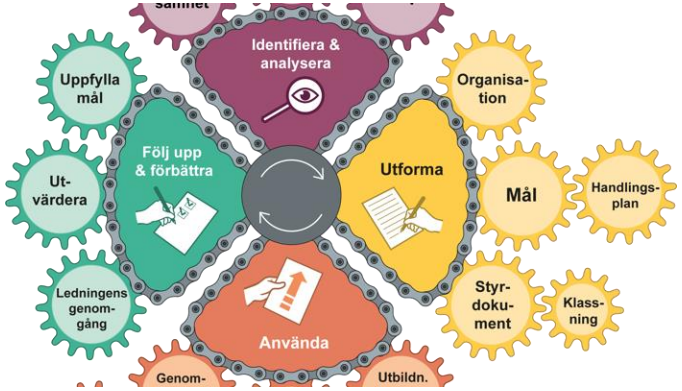
- Alla regler i genomförandeförordningen behöver efterlevas av dem som omfattas av den.
  - För vissa tillkommer sektorsspecifika föreskrifter.
- Det finns flera sätt man kan efterfölja reglerna på.
- Denna presentation ger förslag på hur man kan börja.
- Inget krav att man gör i enlighet med presentationen.
- Börja med att efterleva de mest grundläggande riskhanteringsområdena och strategierna, förfaranden inom dessa områden.
- Utvärdera och anpassa arbetet - löpande och över tid.

Exempel på hur man kan ta sig an efterlevnaden av NIS2

- Nyttja MSB:s metodstöd för att uppnå ett systematiskt och riskbaserat säkerhetsarbete, t.ex.:
  - Mognadsdialogen
  - Systematiskt riskbaserat arbetssätt

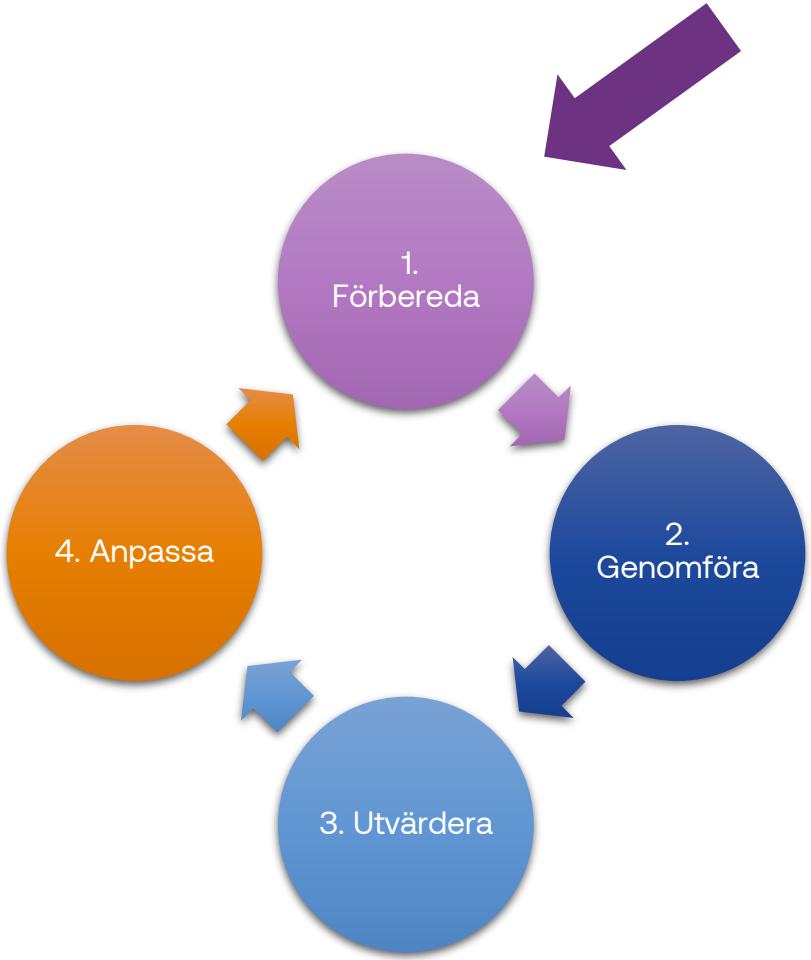
- Nyttja ENISAS:s vägledning till genomförandeakterna (155 sidor)

- Certifiera er verksamhet enligt ISO-27000



Hur börjar vi? (1/2)

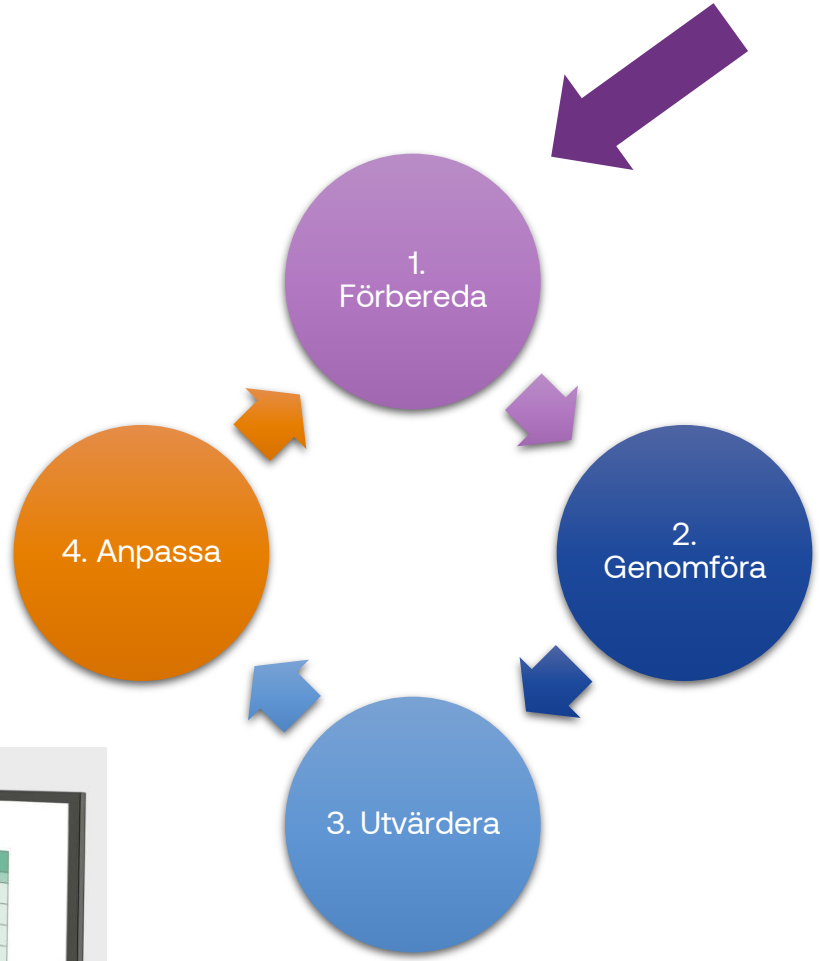
1. **Tillsätt resurser** till arbetet med att efterleva reglerna.
2. **Koordinera** och **fördela arbetet**.
   - Säkerhetsarbete är inte en enpersonsarbete!
   - CISO samverkar med berörda ansvariga (ledning, olika säkerhets-, process-, tjänst-, informationssystem-, nätverksansvariga, m.fl.)
3. **Läs** NIS2: Commission implementing regulation on critical entities and networks
   a) Bilagan om riskhanteringsåtgärder 28 sidor, 13 kapitel
   b) NIS2 Directive - Commission implementing Regulation C(2024) – betydande incidenter



Hur börjar vi? (2/2)

4. Gör **en nulägesbild** över inom vilka **riskhanteringsområden** som ni **behöver utveckla** ert arbete inom. Det kan ske t.ex. med hjälp av:

- ENISA:s vägledning
- MSB:s metodstöd för systematiskt riskbaserat informationssäkerhetsarbete
- Mognadsdialogen
- Eget verktyg/arbetssätt

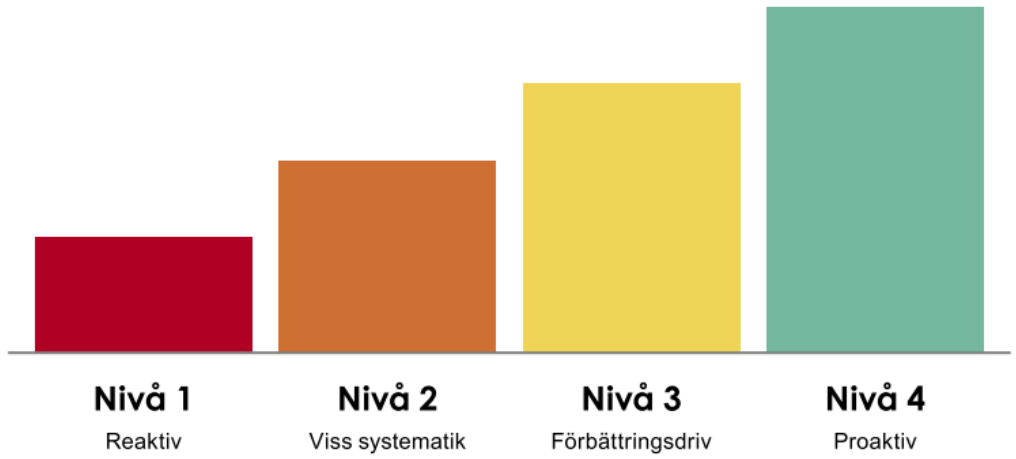


Exempel på verktyg – MSB:s Mognadsdialogen

MSB:s Mognadsdialogen - ett verktyg för att skapa samsyn om aktuellt säkerhetsarbete och utvecklingsområden

- Ger en **nulägesbild** av organisationens **systematiska säkerhetsarbete** och **utvecklingsområden**.
- Nuläget skapas genom att **i dialog jämföra sig med fördefinierade mognadsbeskrivningar enligt fyra olika mognadsnivåer.**
- **Centrala delar** av organisationens **informationssäkerhetsarbete utvärderas** baserat på **ISO/IEC 27000-serien** – s.k. perspektiv.
- **Passar de flesta organisationer**.

Figur 1. Fyra mognadsnivåer



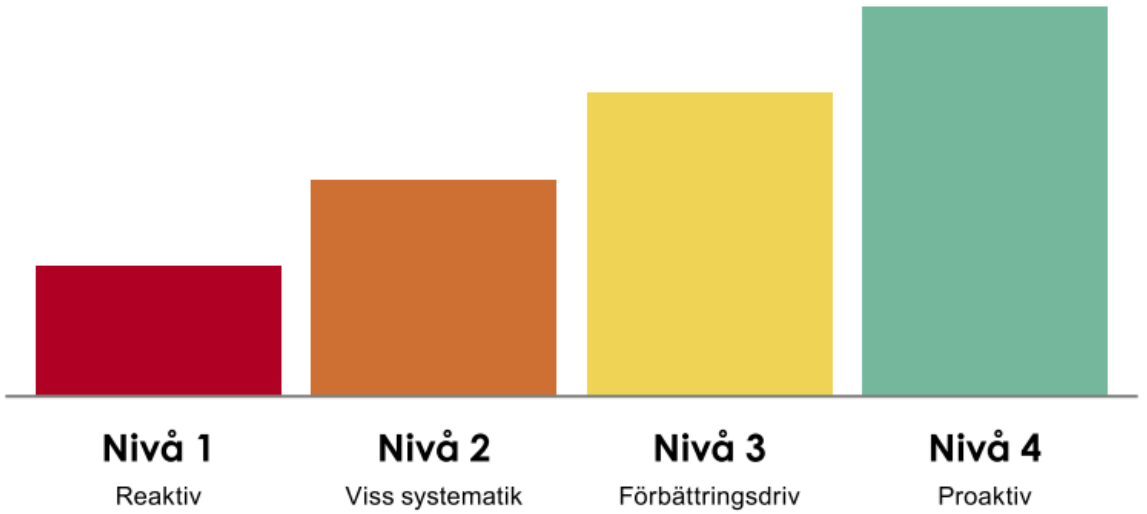
Fokus på följande frågor

1. **Arbetssätt** – Hur gör vi, har vi etablerade och medvetet valda arbetssätt?
2. **Tillämpning** – I vilken omfattning använder vi arbetssätten, gör vi som vi säger att vi ska göra?
3. **Resultat –** Vilka resultat leder våra arbetssätt till? Kan resultaten härledas till arbetssätten?
4. **Följa upp, lärande och förbättring** – Hur utvärderar vi arbetssätten och hur förbättrar vi dem?

Perspektiven som ingår är

1. Riskhantering
2. Informationsklassning
3. Incidenthantering
4. Upphandling
5. Kompetens
6. Uppföljning

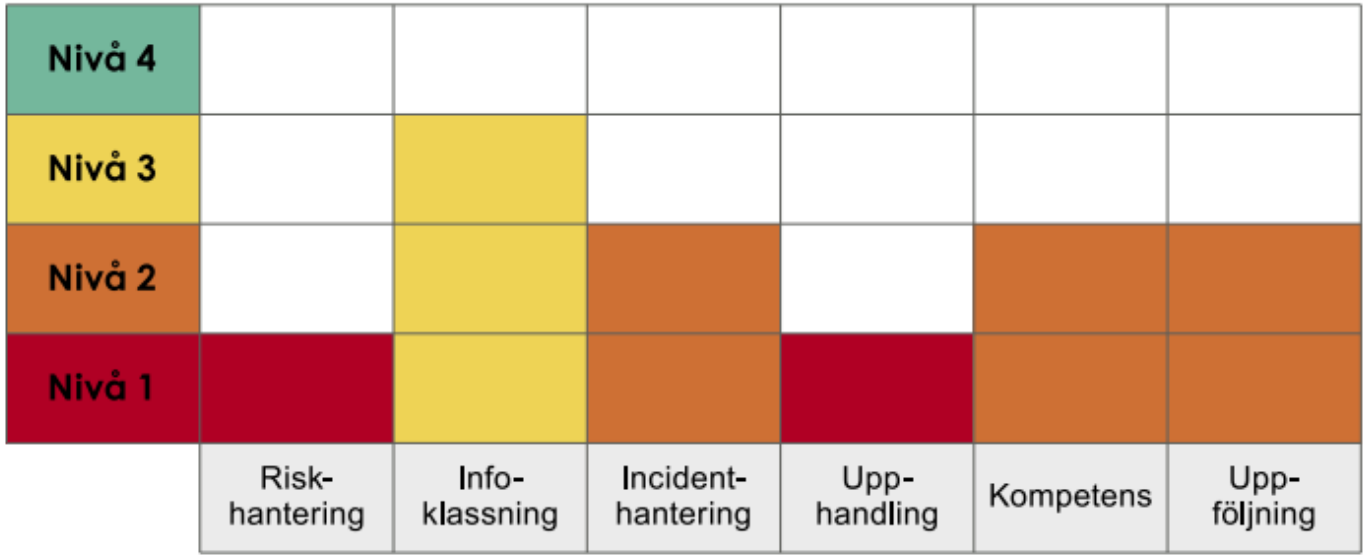
Figur 1. Fyra mognadsnivåer



När passar Mognadsdialogen att utföra?

- Det lättöverskådliga resultatet kan med fördel användas vid **ledningens genomgång**.
- Mognadsdialogen kan göras **vid ett enstaka tillfälle eller återkommande** som ett arbetssätt för att följa utvecklingen över tid.
- För mer info, se Mognadsdialogen

Figur 4. Exempelbild av hur resultatet kan se ut för respektive perspektiv.



Vilka bör vara med vid Mognadsdialogen?

- Förslag 1: **Ledningsgrupp**
- Genom att **ledningen aktivt medverkar** kan **förståelsen och engagemanget för** att **bedriva ett systematiskt informationssäkerhetsarbete öka.** Det är **en fördel genom att resultatet, nuläget och vägen framåt blir väl förankrat i hela ledningen**, vilket spar tid och kan snabba upp utvecklingstakten. En avgörande förutsättning är att ledningen har tid.
- Förslag 2: **En mindre väl sammansatt grupp** som **kan bidra till att ge en helhetsbild av organisationen**. T.ex. **chefer** och **specialister** som har ansvar över eller berörs av nätverks- och informationssystemen, funktioner inom säkerhet, NOC, SOC, abuse, changemangement, samt **gärna personer från kärnverksamheten**

Vilken eller vilka strategier ska man börja med?

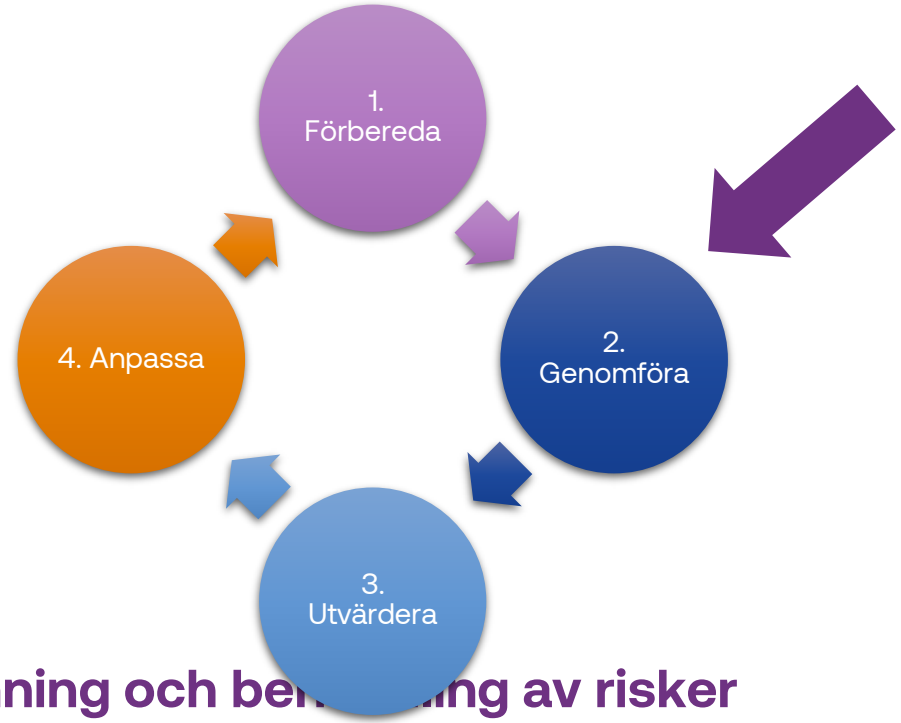
- Strategin om säkerhet i nätverks- och informationssystem, kapitel 1
- Ramverk för riskhantering, kapitel 2
- Strategi för incidenthantering, kapitel 3
- Driftkontinuitet och krishantering, kapitel 4
- Säkerhet i leveranskedja, kapitel 5
- Strategi för att bedöma effektivitet i riskhanteringsåtgärder, kapitel 7
- Hantering av tillgångar, kapitel 12
- Åtkomstkontroll, kapitel 11

Kapitel 1 - strategi för säkerhet i nätverks- och informationssystem, art 21.2 a

- Ta fram en **strategi** för säkerhet i nätverks- och informationssystem
- Tillhandahålla tillräckliga **resurser** för genomförandet
- Se till att anställda och underleverantörer **känner till** strategin
- Se till att **ledningen godkänner** strategin
- Strategin ska **uppdateras** minst årligen
- Ta fram **roller** och **ansvarsområden**

Kapitel 2 - Riskhantering och ramverk för riskhantering

- **Integrerad del** i organisationen
  - **Koordinerade aktiviteter** för att **styra och hantera** en organisation **utifrån risk**
  - **Systematiskt** och **strukturerat**
- Beakta **ALLRISK-perspektivet**
- **Iterativ process, ständig förbättring**
- **Följa en riskhanteringsmetod**
- **Fastställa förfaranden för identifiering, analys, bedömning och be[illegible]ing av risker (riskhanteringsprocess för cybersäkerhet)**
- **Fastställa risktoleransnivån i enlighet med entitetens riskbenägenhet**
- **Fastställa och upprätthålla relevanta riskkriterier**



Vad missar aktörer ofta i tillsyn?

- Att **identifiera** och **analysera samtliga relevanta hot** mot **”säkerheten i nätverks- och informationssystem”** –> **allriskperspektivet!**

Hot mot säkerheten i nätverks- och informationssystem *kan ha olika ursprung ->*

Därför ska riskhanteringsåtgärder för cybersäkerhet bygga på

ALLRISKPERSPEKTIVET

ALLRISKPERSPEKTIVET i RISKANALYSERNA

- *Stöld, brand, översvämning, naturfenomen*
- *telekommunikations- eller elavbrott*
- *obehörig fysisk åtkomst,*
- *systemfel, mänskliga misstag*
- *avsiktligt skadliga handlingar, sabotage*
- *skada eller störning på en väsentlig eller viktig entitets information och informationsbehandlingsresurser, som kan undergräva* **tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten** *hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem*

ALLRISKPERSPEKTIVET i RISKANALYSERNA även

- Ransomewareattacker
- Wiperattacker
- Överbelastningsattacker
- Avlyssning
- Förvanskning av uppgifter
- Informationsstöld
- Mfl.

Vad missar aktörer ofta i tillsyn? (2/2)

- ✓Att analysera **konsekvenserna** av identifierade hot **utifrån samtliga säkerhetsaspekter T R A K ->** inte bara Tillgänglighet, utan även för **Riktighet, Autenticitet och Konfidentialitet!**
- ✓Att uppdatera riskanalyser efter **inträffade omvärldshändelser, inträffade incidenter, förändringar i nätverk- och informationssystem (återföra från andra processer till ”riskhanteringsarbetet”)!**
- ✓Att **riskanalyser och riskbedömning** är en **integrerad del och genomförs regelbundet för att bedöma behov av åtgärder!**

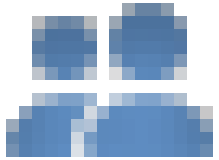
Vanliga orsaker till incidenter med betydande påverkan inom telekom - värdefulla insikter för fler?

- Två av de **vanligaste orsakerna** till inträffade incidenter med betydande påverkan är:
  - **systemfel** och **antagonsiska angrepp (22 st, 7 st)**.

- Närmare orsak till **systemfelen**:
  - felaktig uppdatering av mjukvara, 6st
  - hårdvarufel, 6st
  - mjukvarubugg, 5st
  - överbelastning, 2 st
  - Strömavbrott, 1 st
  - Felaktig uppdatering av hårdvara, 1 st

- Närmare orsak till **antagonistiska angrepp**:
  - DDoS-attack, 3st
  - skadlig programvara, 2 st
  - exploateringar av sårbarhet, 2 st
  - Övrigt 1 st

Sammanfattning



1. **Tillsätt resurser** till arbetet med att efterleva reglerna!
2. **Koordinera** och **fördela arbetet**.
   - Säkerhetsarbete är **inte** en enpersonsarbete!
   - CISO samverkar med berörda ansvariga (ledning, olika säkerhets-, process-, tjänst-, informationssystems-, nätverksansvariga, m.fl.)

3. Gör **en nulägesbild** över vilka **riskhanteringsområden** som ni **behöver utveckla** ert arbete inom. Nyttja t.ex:

- ENISA:s vägledning
- MSB:s metodstöd för systematiskt riskbaserat informationssäkerhetsarbete
- MSB:s Mognadsdialogen
- Eget verktyg/arbetssätt, genomförandeakterna

4. **Utbilda** inom samt **tillämpa riskhanteringsåtgärder**.

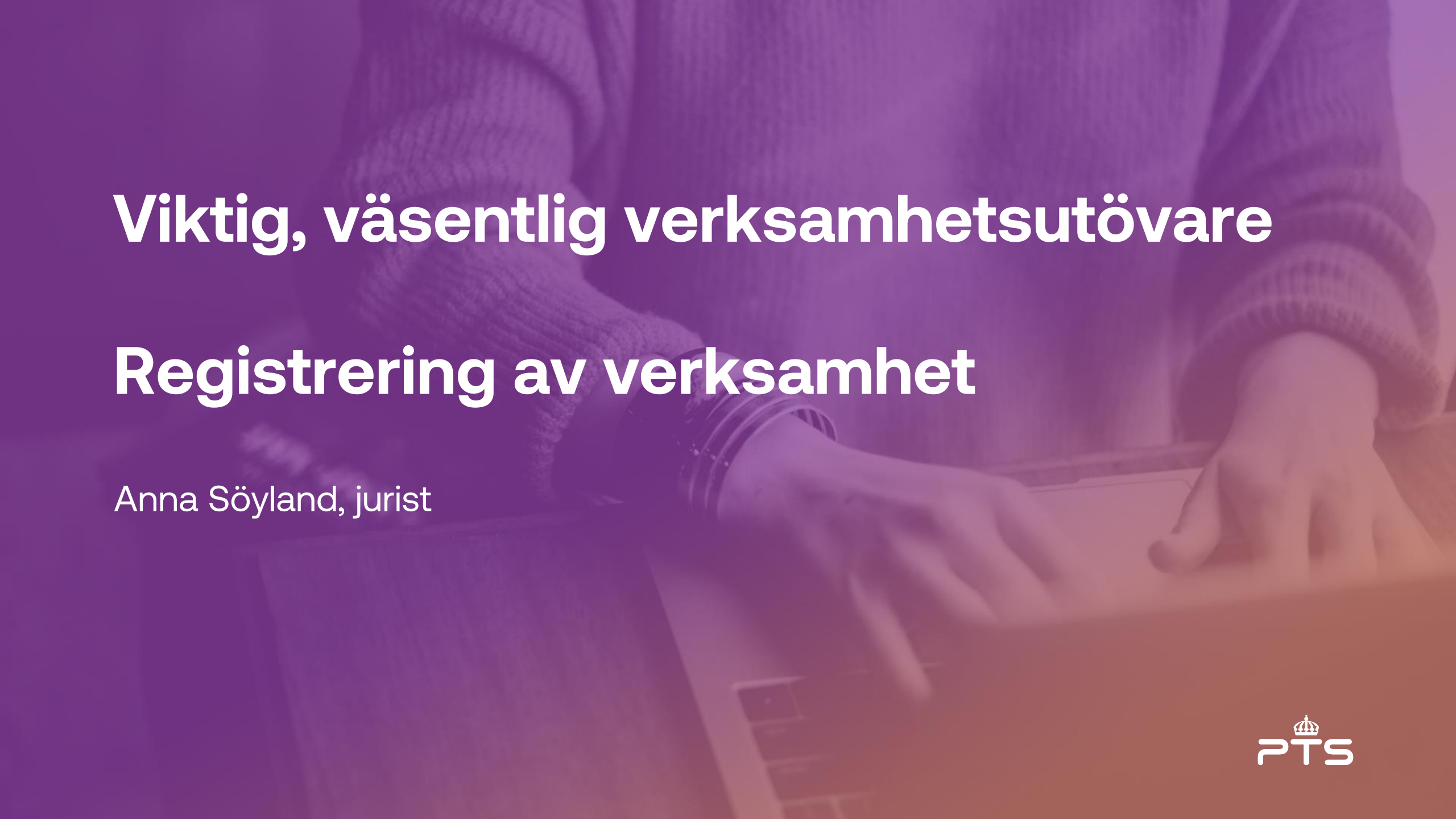
5. **Utvärdera riskhanteringsåtgärder**, **anpassa riskhanteringsåtgärderna**, **13 st.**

Frågor från er

Fika och mingel kl. 10:40 – 11:10

- Hur jobbar ni med att förbereda er för NIS2?
- Vad är era största utmaningar?
- Vad skulle ni behöva av PTS?
- Vad har ni för frågor och funderingar?

Skriv era frågor och reflektioner i chatten



Viktig, väsentlig verksamhetsutövare

Registrering av verksamhet

Anna Söyland, jurist

Viktig, väsentlig verksamhetsutövare

Beräkning och konsekvenser

Väsentlig eller viktig verksamhetsutövare?

- Storleksbaserat för att träffas av regelverket
- Även storleksbaserat för att bedöma: väsentlig eller viktig
- Tumregel:
  - **Bilaga II**: Viktig (stort/medelstort företag), ***eller*** omfattas inte (små/mikro)
  - **Bilaga I**:
    - Små/mikro = omfattas inte av CSL
    - Medelstort företag = viktig
    - Stort företag = väsentlig

  - OBS: fortfarande flera undantag, samt **beräkningsregler**

Väsentlig eller viktig?

- Påverkar inte: Riskhanteringsåtgärder, incidentrapportering
- Påverkar:
  - **Tillsyn**,
    - planlagd (väsentlig) eller händelsestyrd (viktig)
  - **Sanktioner**,
    - Väsentlig: upp till 2 procent av er totala globala årsomsättning närmast föregående räkenskapsår, eller €10 miljoner (vad som än är högst)

      Viktig: upp till 1,4 procent av er totala globala årsomsättning eller €7 miljoner (vad som än är högst)

Stor eller medel – beräkning

Stort företag:

≥ 250 anställda

eller

> €50 miljoner årsomsättning **och** > €43 miljoner årsbalansomslutning

Medelstort företag:

≥ 50 anställda

eller

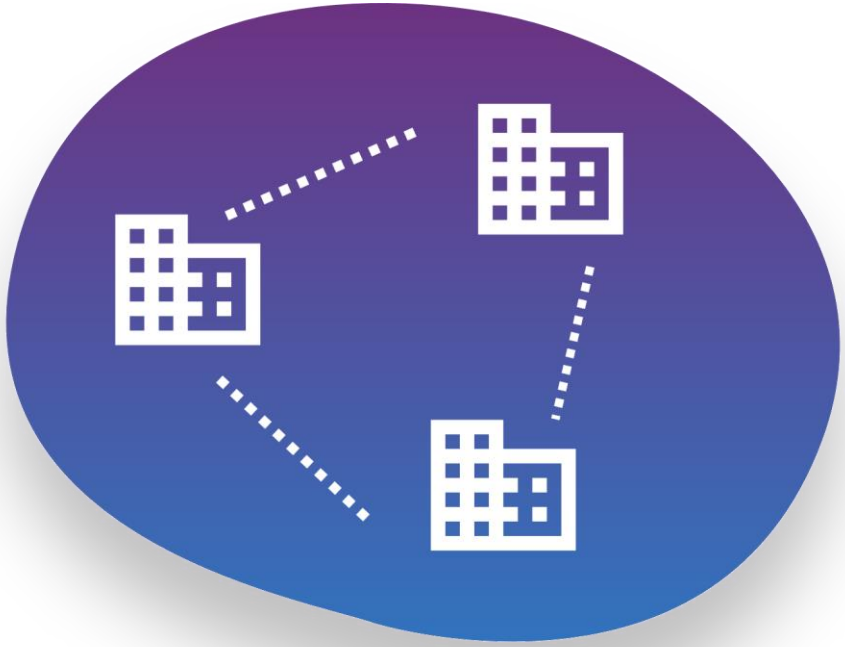
> €10 miljoner årsomsättning eller årsbalansomslutning

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

Vad gäller för koncerner?

Partnerföretag och **anknutna företag** måste beaktas när beräkningen görs.

Användarhandledning om definitionen av SMF-företag - Publications Office of the EU



Definitionen av SMF-företag

För att ta fram uppgifterna som det ska tas hänsyn till och bedömas i förhållande till tröskelvärdena måste du först avgöra om du är något av följande:

- Ett **fristående** företag (den överlägset vanligaste)
- Ett **partnerföretag**
- Ett **anknutet** företag

s. 15, Användarhandledning om definitionen av SMF-företag

Partnerföretag eller anknutet företag

- **Partnerföretag**

  (s. 18, Användarhandledning)

  - Företag som sluter betydande ekonomiska partnerskap med andra företag utan att det ena verkligen utövar en direkt eller indirekt kontroll över det andra.
  - Företag som varken är fristående eller anknutna till varandra.

- **Anknutet företag**

  (s. 21, Användarhandledning)

  - Företag som formar en koncern genom direkt eller indirekt kontroll av huvuddelen av rösterna eller genom att utöva ett bestämmande inflytande över ett företag.
  - Ett typexempel på ett anknutet företag är ett helägt dotterbolag.

”Ok, vi har räknat ut!
Vad gör vi nu?”

Registrering av verksamhet

Registrering

SOU 2024:18 Nya regler om cybersäkerhet s. 177:

”Utredningens förslag:
(...)
3. Verksamhetsutövare ska i en anmälan till tillsynsmyndigheten lämna uppgift om identitet, kontaktuppgift, IP-adressintervall, verksamhet och uppgift om i vilka länder verksamhet bedrivs (...).”

OBS: Ännu inte beslutat.

Det kommer finnas möjlighet att anmäla sin verksamhet när CSL träder i kraft.

Registrering – vanliga frågor

- **Hur vet vi om vi måste anmäla oss?**
  - PTS e-tjänst: **Omfattas vi av CSL?** / **Does CSL apply to us? (English)**
- **När kommer vi kunna anmäla oss?**
  - Det vet vi först när vi har en beslutad lag, men förmodligen till sommaren då CSL förväntas träda i kraft.
- **Vi har verksamhet i flera länder, var gör vi vår anmälan då?**
  - Det beror på vilken jurisdiktionsregel ni faller under.

Registrering – vanliga frågor

- **Vi träffas av flera sektorer – måste vi anmäla oss till flera tillsynsmyndigheter då?**
  - Om det som nu är föreslaget blir beslutat och träder i kraft, ja.
- **Vad händer om vi inte anmäler oss?**
  - Ni kan drabbas av sanktionsavgifter.
- **… Hur höga sanktionsavgifter?**
  - Det bedöms i varje enskilt fall.

Frågor från er

Vad händer nu?

- Cybersäkerhetslagen
- Läs igenom genomförandeförordningen
- Börja med förberedelser

- nis@pts.se

Tack för ert deltagande!

Frågor: nis@pts.se

Inspelning läggs ut inom några veckor på pts.se