Information om NIS2 för PTS sektorer

Anders Franzén och Åsa Gihl

NIS 2 Direktiv

- Minimiregler för riskhanteringsåtgärder
- Effektivt samarbete
- Förteckning över sektorer och verksamheter
- Effektiva rättsmedel och efterlevnadskontroller, t ex högre sanktionsavgifter
- Fler sektorer och tjänster
- Uttalat ansvar för ledningsorganen

NIS2 Direktiv

- Åtgärda brister i differentieringen av leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster
- Enhetliga kriterier för entiteter som omfattas
- **CER**-direktivet pekar ut kritiska entiteter – öka motståndskraft

Ny uppdelning i entiteter

- En fysisk eller juridisk person som bildats och erkänts som sådan enligt nationell rätt där den etablerats och som i eget namn får utöva rättigheter och ha skyldigheter.

- Register över entiteter

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

Digital infrastruktur

- Leverantörer av internetknutpunkter (IXP)
- Leverantörer av DNS-tjänster (rotservrar undantagna)
- Registreringsenheter för toppdomäner
- Leverantörer av molntjänster
- Leverantörer av datacentraltjänster
- Leverantörer av nätverk för leverans av innehåll (CDN)
- Tillhandahållare av betrodda tjänster (eIDAS)
- Tillhandahållare av allmänna elektroniska kommunikationsnät
- Tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster

Förvaltning av IKT-tjänster

- Leverantörer av hanterade tjänster (managed services)
- Leverantörer av hanterade säkerhetstjänster

Vilka aktörer omfattas av NIS 2 – 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

Digitala leverantörer

- Leverantörer av marknadsplatser online
- Leverantörer av plattformar för sociala nätverkstjänster
- Leverantörer av sökmotorer

Definitioner i NIS2 artikel 6

- Leverantör av DNS tjänster
  - ✓ *allmänna rekursiva tjänster för att lösa domännamnsfrågan till internetslutanvändare, eller*
  - ✓ *auktoritativa tjänster för att lösa domännamnsfrågor för användning av tredje part, med undantag för rotnamnsservrar*
- Entitet som erbjuder domännamnsregistreringstjänster
  - ✓ *en registrar som verkar på uppdrag av en registreringsenhet eller ett ombud för en registreringsenhet, såsom återförsäljare och leverantörer av integritetsregistreringstjänster och proxyregistreringstjänster*

Forts. definitioner i NIS2 artikel 6

- Registreringsenhet för toppdomäner eller TLD registreringsenhet

✓ *administrationen av toppdomänen*

- ❖ *registreringen av domännamn under toppdomänen*

✓ *tekniska driften av toppdomänen*

- ❖ *drift av dess namnservrar*
- ❖ *underhåll av dess databaser*
- ❖ *distribution av zonfiler för toppdomänen mellan namnservrar,*

Oberoende av huruvida någon aspekt av denna drift utförs av enheten själv eller har utkontrakterats, dock inte situationer där toppdomäner används av en registreringsenhet endast för dess eget bruk.

Forts. definitioner i NIS2 artikel 6 MoIntjänster

- MoIntjänst

- *administration på **begäran** och*
- *bred **fjärråtkomst** till en*
- ***skalbar** och*
- ***elastisk** pool av gemensamma **beräkningstjänster**, inbegripet när sådana resurser är distribuerade på flera platser.*
- *(förtydliganden i skäl 33) Möjliggör administration av beställtjänster.*

Forts. definitioner i NIS2 artikel 6 Skäl 33

- **Beräkningsresurser;**
  - nätverk,
  - servrar eller annan infrastruktur,
  - operativsystem, programvaror, lagring, applikationer och tjänster
- **Tjänstemodeller**
  - Infrastruktur som en tjänst,
  - plattform som en tjänst,
  - program som en tjänst och
  - nätverk som en tjänst.
- **Distribueringsmodellerna**
  - privata moln,
  - gemensamt moln,
  - offentligt moln och
  - hybridmoln.

Definitioner i NIS2 artikel 6 Datacentraltjänster

- Datacentraltjänst

  -strukturer, eller grupper av strukturer

  -avsedda för centraliserad inkvartering, sammankoppling och drift av it- och nätutrustning som

  -tillhandahåller datalagrings-, databehandlings- och dataöverföringstjänster samt

  -alla anläggningar och infrastrukturer för kraftdistribution och miljökontroll.

Bör inte vara tillämplig på interna datacentraler som ägs och drivs av den berörda entiteten för egen räkning (skäl 35)

Definition av företag

Typ av företag	Antal sysselsatta	Omsättning
Mikroföretag	< 10 personer	< €2M
Små företag	< 50 personer	< €10M
Medelstora företag	< 250 personer	< €50M

Båda villkoren ska vara uppfyllda för att klassas som en viss typ av företag, Kommissionens förslag om definitionen av mikroföretag samt små och medelstora företag (2003/361/EG)

Vilken storlek krävs för att omfattas av NIS2?

- Alla offentliga och privata aktörer som betecknas som medelstora företag eller större **men** med ett antal undantag…
- Oavsett storlek omfattas följande:
  - Allmänna elektroniska kommunikationsnät- och tjänster
  - Betrodda tjänster
  - Registreringsenheter för toppdomäner och leverantörer av DNS-tjänster
  - Om aktören är den enda i en medlemsstat och den är kritisk
  - Vissa offentliga förvaltningsentiteter

Väsentliga entiteter

- Aktörer inom digital infrastruktur som överstiger trösklarna för medelstora företag, dvs 250 anställda eller fler
  - IXP, datacenter, CDN, molntjänster,
- Oavsett storlek
  - Registreringsenheter för toppdomäner
  - Leverantörer av DNS-tjänster
  - Kvalificerade betrodda tjänster
- Allmänna elektroniska kommunikationsnät- och tjänster som är medelstora företag eller större, dvs 50 anställda eller fler
- De som inte betraktas som väsentliga entiteter är viktiga vilket innebär att…

Följande är viktiga entiteter inom digital infrastruktur och digitala tjänster

- Allmänna elektroniska kommunikationsnät- och tjänster, färre än 50 anställda
- IXP, 50 <= anställda < 250
- Molntjänster, 50 <= anställda < 250
- Datacentraltjänster, 50 <= anställda < 250
- CDN, 50 <= anställda < 250
- Icke kvalificerade betrodda tjänster oavsett storlek
- Marknadsplatser, endast viktiga, 50 anställda eller fler
- Plattformar för sociala nätverkstjänster, endast viktiga, 50 anställda eller fler
- Sökmotorer, endast viktiga, 50 anställda eller fler

I tabellform

Aktör	Viktig	Väsentlig
TLD, DNS, kvalificerade betrodda tjänster oavsett storlek		X
Allmänna elektroniska kommunikationsnät- och tjänster, 50 eller fler		X
Allmänna elektroniska kommunikationsnät- och tjänster, färre än 50	X	
IXP, datacenter, CDN, molntjänster, 250 eller fler		X
IXP, datacenter, CDN, molntjänster, färre än 250 men 50 eller fler	X	
Marknadsplatser, sociala plattformar, sökmotorer, 50 eller fler	X	
Icke kvalificerade betrodda tjänster oavsett storlek	X	

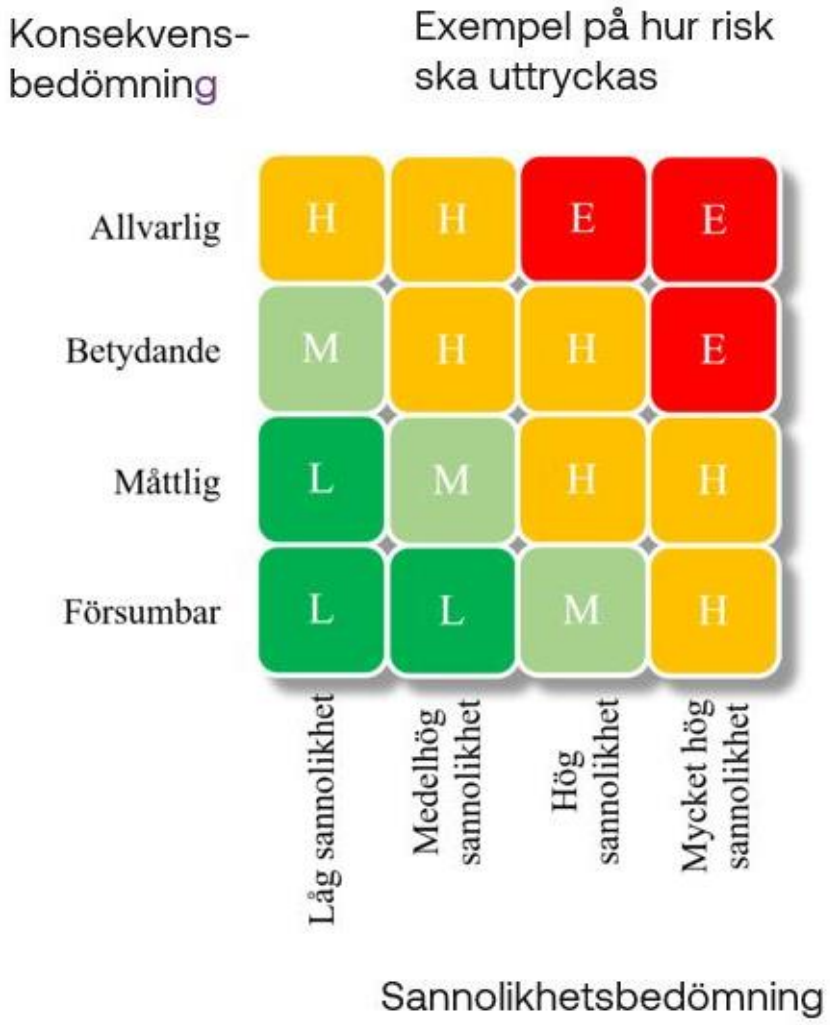
Riskhanteringsåtgärder (säkerhetsåtgärder) artikel 21

- **Väsentliga** och **viktiga** entiteter ska vidta lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverk- och informationssystem.
- Samma som tidigare men sedan har man angett mer specifikt vad som avses och det ska baseras på en **allriskansats**

Definitioner i NIS2 artikel 6 risk

- Risk

Risk för förlust eller störning orsakad av en incident, som ska uttryckas som en kombination av omfattningen av förlusten eller störningen och sannolikheten för att en sådan incident inträffar.



Riskhanteringsåtgärder ska minst inbegripa

- Strategier för riskanalys och informationssystemens säkerhet
- Incidenthantering
- Driftskontinuitet som exempelvis hantering av säkerhetskopiering
- Säkerhet i leveranskedjan
- Säkerhet vid förvärv
- Strategier och förfaranden för att bedöma riskhanteringsåtgärderna
- Grundläggande praxis för cyberhygien och utbildning
- Strategier för användning av krypto
- Personalsäkerhet, strategier för åtkomstkontroll
- Användning av multifaktorautentisering och säkrade kommunikationer

Genomförandeakt för riskhanteringsåtgärder

- 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

Rapporteringsskyldighet – artikel 23

- Samma för väsentliga och viktiga
- **Betydande incident**
- Underrätta mottagarna av tjänster om åtgärder de kan vidta som svar på **betydande cyberhot**
- Gränsöverskridande verkningar
- Om lämpligt underrätta om betydande incidenter och cyberhot

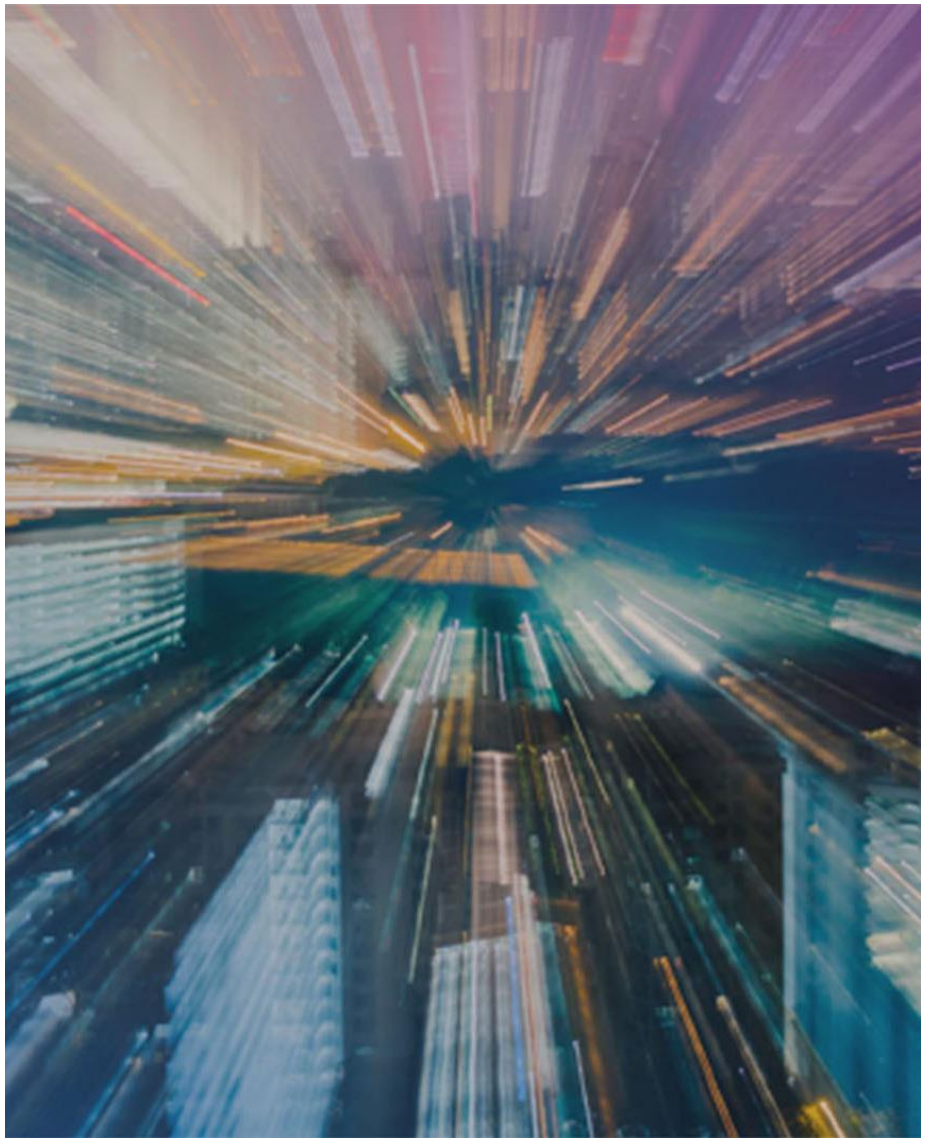
Betydande incident

- Undergräver tillgänglighet, autenticiteten, riktigheten eller konfidentialiteten

OCH

a)Har orsakat eller kan orsaka allvarliga driftsstörningar för tjänsterna eller ekonomiska förluster för entiteten.

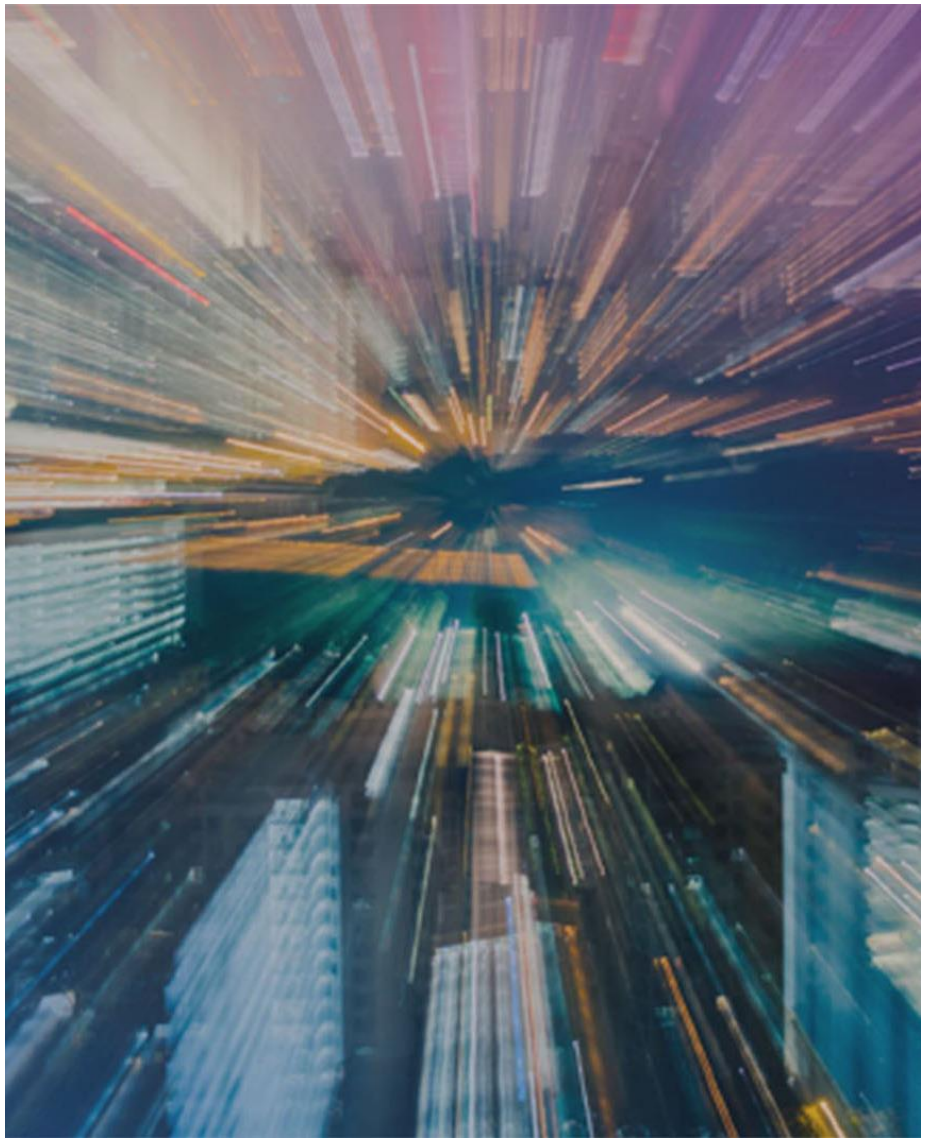
  - drabbade nätverks- och informationssystemen betydelse
  - Allvar och tekniska egenskaper hos cyberhot
  - Underliggande sårbarheter



Forts. betydande incident

b)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



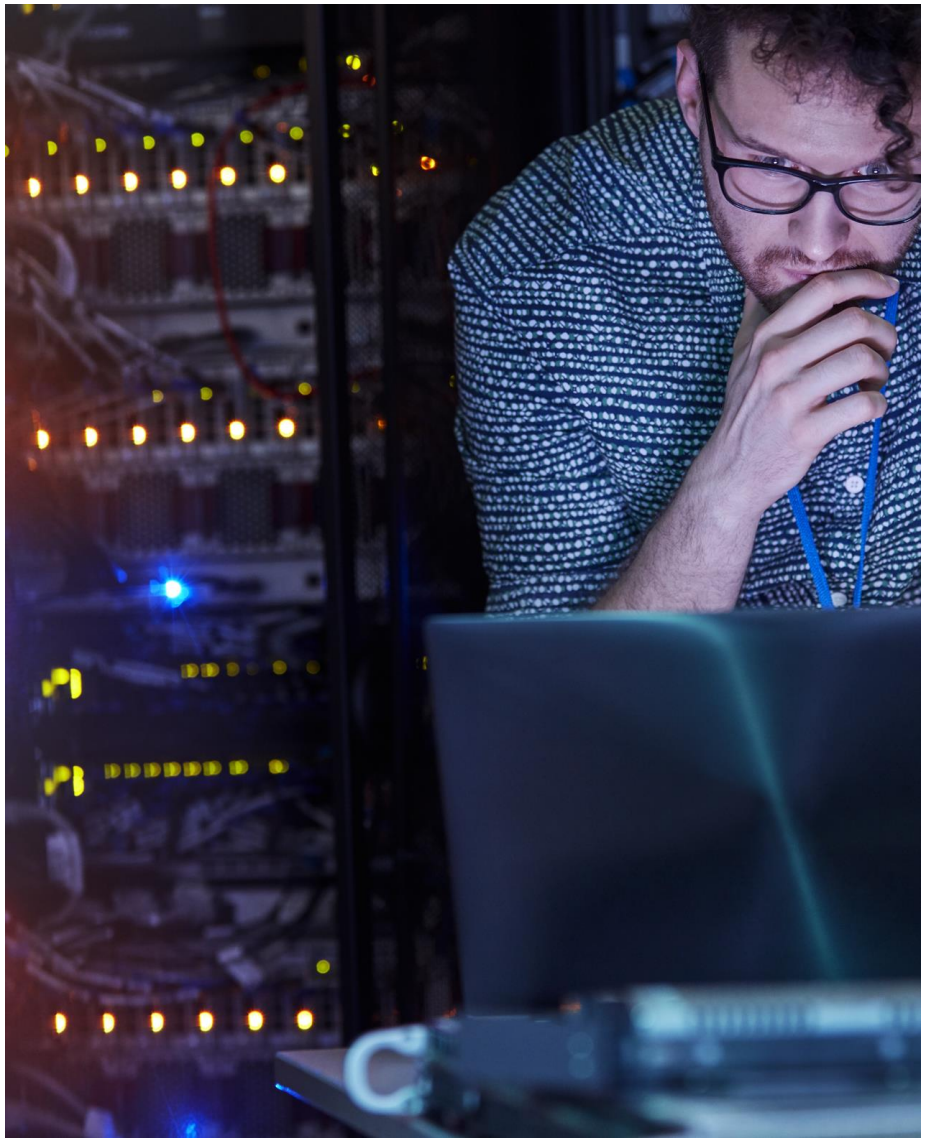
Frivillig underrättelse

- Tillbud (engelska ”Near miss”)
- Incidenter
- Cyberhot

En frivillig underrättelse får inte leda till att den underrättande entiteten åläggs ytterligare skyldigheter som den inte skulle ha blivit föremål för om den inte hade lämnat in underrättelsen.

Definitioner i NIS2 artikel 6 cyberhot och betydande cyberhot

- Cyberhot
- ***omständighet, händelse eller handling***
- ***skada, störa , negativt sätt påverka***
- ***nätverks- och informationssystem, användare***
- Betydande cyberhot
- ***tekniska egenskaper, allvarlig påverkan***
- ***betydande materiell eller immateriell skada.***



Tider för rapportering

Tidig varning 24 timmar
(idag 6 timmar)

- Olagliga eller avsiktligt skadliga handlingar
- Gränsöverskridande

72 timmar incidentanmälan
(idag 24 timmar)

- Inledande beömning
- Allvarlighetsgrad
- Konsekvenser
- Angreppsindikatorer

Slutrapport 1 månad
(Idag 3 veckor)

- Allvarlighetsgrad
- Typ av hot eller grundorsak
- Begränsande åtgärder
- Gränsöverskridande

Forts. tider för rapportering

- CSIRT/Behörig myndighet ska om möjligt återkoppla inom 24 timmar efter mottagande
  - Återkoppla till underrättande entiteten
  - På begäran ge vägledning eller operativa råd om möjliga begränsande åtgärder

- Behörig myndighet kan begära en delrapport

Jurisdiktion (artikel 26) digital infrastruktur digitala leverantörer

- Gränsöverskridande karaktär
- Huvudsakligt etableringsställe i unionen
  - Där beslut om cybersäkerhet fattas
  - Där cybersäkerhetsoperationer utförs
  - Där flest anställda i unionen
- Om ej etablerad i unionen
  - Utse företrädare där tjänsterna erbjuds

Register över entiteter (artikel 27 samt artikel 3.3)

- Medlemsstaterna ska upprätta en förteckning över väsentliga och viktiga entiteter samt tillhandahållare av domänregistreringstjänster
- Förteckningen ska minst innehålla:
  - Entitetens namn
  - Sektor (t.ex. digital infrastruktur)
  - Adress och kontaktuppgifter
  - De medlemsstater där man erbjuder tjänster
  - IP-adressintervall
- Uppgifterna ska vara lämnade till behörig myndighet senast 17 januari 2025
- Ändringar ska meddelas inom 3 månader

Register fortsättning

- Enisa ska dessutom skapa och upprätthålla ett register över entiteter inom digital infrastruktur, förvaltning av IKT-tjänster och digitala leverantörer, **förutom IXP men inklusive registrarer**
- Detta register är baserat på de uppgifter medlemsstaterna samlar in

Databas över domännamn (artikel 28)

- Registreringsenhet för toppdomänen och registrarer ska samla in och upprätthålla uppgifter kring domännamn
- Följande uppgifter krävs:
  - Domännamn
  - Registreringsdatum
  - Namn, e-postadress och telefonnummer
  - E-post och telefonnummer till den som administrerar domänen
- Det ska säkerställas att informationen är korrekt
- Informationen ska offentliggöras förutom personuppgifter
- Ingen ytterligare information utöver det som anges i 6 § i toppdomänlagen (2006:24) förutom registreringsdatum

Typ av tillsyn, artikel 31-33

Väsentlig

- Säkerställa att NIS2 efterlevs

Viktig

- Vid bevis om underlåtenhet att fullgöra krav i NIS2

Tillsynsåtgärder, artikel 32-33

Väsentlig

- Inspektioner
- Säkerhetsrevisioner
- Säkerhetsskanning
- Handlingar och information
- Bevis
- Ad-hoc revisioner

Viktig

- Inspektioner
- Säkerhetsrevisioner
- Säkerhetsskanning
- Handlingar och information
- Bevis

Efterlevnadskontroll artikel 32-33

Väsentlig

- Utfärda varningar
- Bindande instruktioner
- Upphöra med beteende
- Ålägga att vidta åtgärder och informera användare
- Sanktionsavgifter
- Övervakningsansvarig

Viktig

- Utfärda varningar
- Bindande instruktioner
- Upphöra med beteende
- Ålägga att vidta åtgärder och informera användare
- Sanktionsavgifter

Efterlevnadskontroller som är ineffektiva, artikel 32

Väsentlig

- Tillfälligt upphäva en certifiering eller auktorisation
- Begära tillfälligt förbud att utöva ledningsfunktioner i entitet.

Omständigheter att beakta vid utfärdande av efterlevnadskontroller , artikel 34

Väsentlig och Viktig
• Överträdelsen allvar och betydelsen av de bestämmelser som överträtts. • Överträdelsens varaktighet • Tidigare överträdelser • Materiella´och immateriella skador • Uppsåt och oaktsamhet • Om åtgärder vidtagits för att förhindra och begränsa materiella och immateriella skador • Samarbetet med de behöriga myndigheterna

Sanktionsavgifter och viten (artikel 34)

- Sanktionsavgifter ska påföras entiteter vid överträdelser av artikel 21 (riskhanteringsåtgärder) och artikel 23 (rapporteringsskyldigheter)
  - Väsentliga entiteter, högst €10M eller högst 2 % av omsättningen
  - Viktiga entiteter, högst €7M eller högst 1,4 % av omsättningen
- Sanktionsavgifterna ska vara effektiva, proportionella och avskräckande
- Medlemsstaterna får föreskriva befogenhet att förelägga viten