Vad betyder NIS2 i praktiken?
KommITS Västerås

2023-10-24

Sveriges Kommuner och Regioner

Vad är NIS?

- NIS = Resiliens i nätverk och informationssystem
  - Resiliens i NIS = Förmåga att motstå och återhämta sig från incidenter
- Gäller för samhällsviktiga tjänster
- Reglerat i lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
  - Europaparlamentet och rådet direktivet (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela den europeiska unionen

Arbetet med NIS2 pågår…

- NIS2 direktivet beslutades den 14 december 2022
- Genomförande av direktivet som svensk lag pågår
  - Den svenska utredningen väntas vara klar februari 2024
    - Utredningen inkluderar även införandet av CER-direktivet i svensk rätt
  - Senast den 17 oktober 2024 måste medlemsstaterna anta och offentliggöra de bestämmelser som är nödvändiga för att följa detta direktiv
- Hur NIS2 faktiskt kommer att implementeras är inte helt klart…
  - Den höga graden av harmonisering innebär att EU dock inte lämnat så stort utrymme till medlemsstaterna att bestämma hur saker ska göras

Nytt med NIS2

- Högre grad av harmonisering inom EU
  - Vem som omfattas
  - Krav på riskanalyser och säkerhetskrav
  - Tillsyn och sanktioner
- NIS2 träffar fler sektorer än NIS
- Krav på ledningens deltagande i cybersäkerhetsarbetet
- Från begreppet tjänsteleverantörer till viktiga/väsentliga entiteter

Vem kommer att omfattas?

- En entitet som tillhandahåller en samhällsviktig tjänst inom vissa sektorer och som är av viss storlek.
  - Gäller både privata och offentliga entiteter
- Sektor och storlek är avgörande

Storlek

Företags-kategori	Personalstyrka: Arbetskrafts-enheter/år (UTA)	Årsomsättning	Balans-omslutning	
Medelstora	< 250	≤ € 50 milj.	≤ € 43 milj.	Huvud-regel
Små	< 50	≤ € 10 milj.	≤ € 10 milj.	Undantag
Mikro	< 10	≤ € 2 milj.	≤ € 2 milj.	

Sektorer ur ett kommunperspektiv

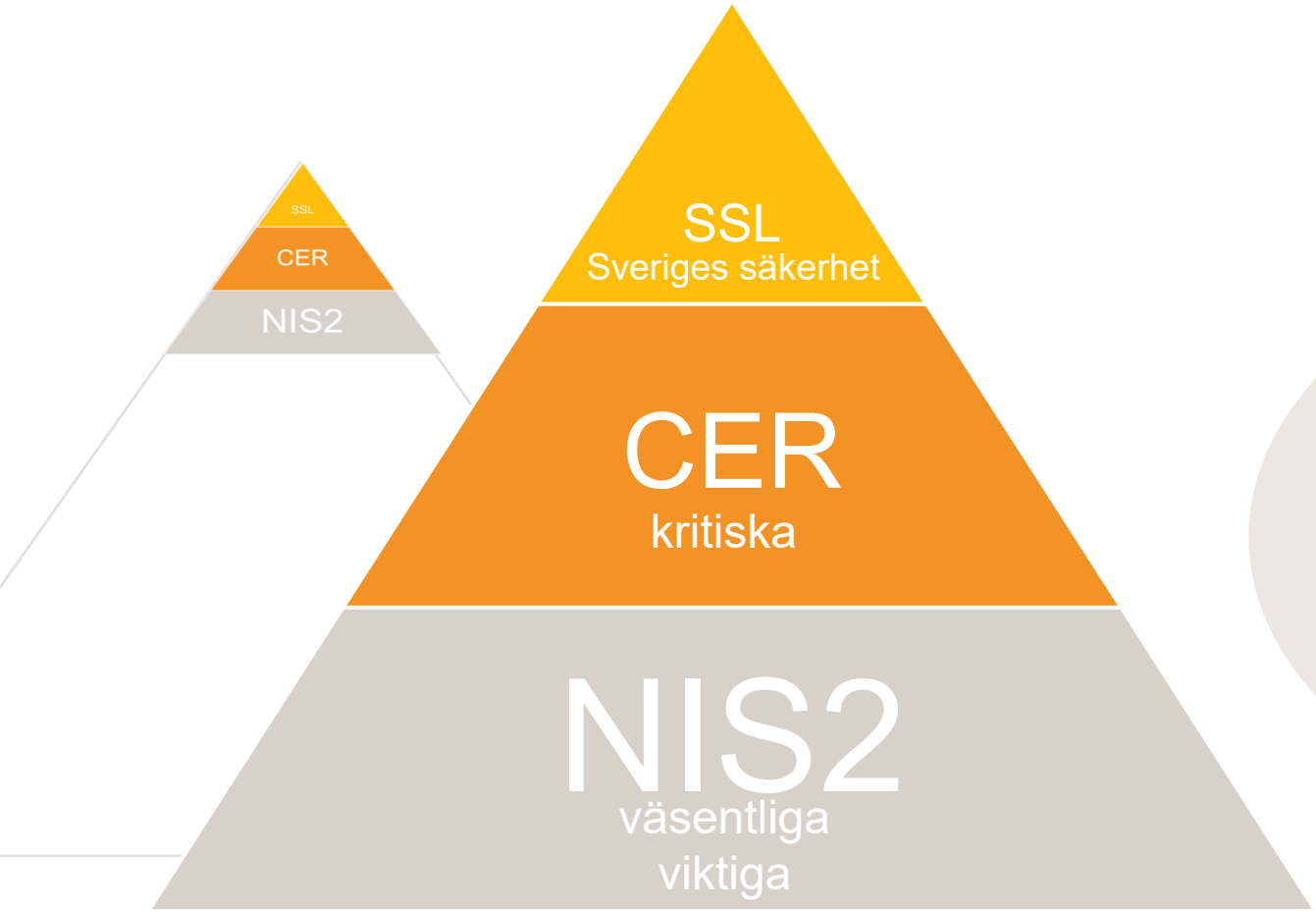
- **Avfallshantering**
- **Avloppsvatten**
- Dricksvatten
- Digital infrastruktur
  - Leverantör av DNS-tjänster
  - **Tillhandahållare av betrodda tjänster**
  - […]

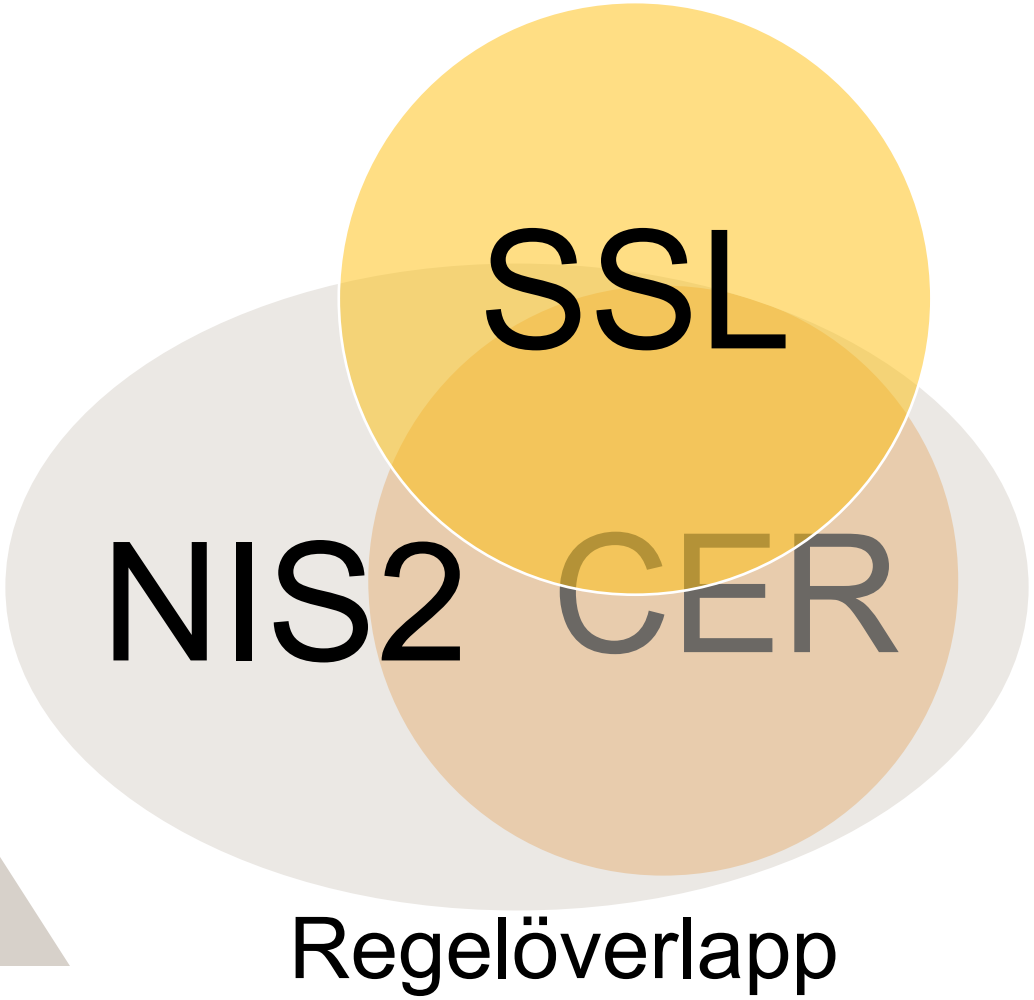
= nytt i NIS2

- Energi
  - Elektricitet
  - **Fjärrvärme och -kyla**
  - Olja
  - Gas
  - **Vätgas**
- Hälso- och sjukvård
- Offentlig förvaltning som en entitet
  - På regional nivå
    - Oklart var gränsen går till lokal nivå?

Sveriges Kommuner och Regioner

NIS2, CER, Säkerhetskyddlagen





Regelöverlapp

Sveriges Kommuner och Regioner

Ytterligare en samling med krav?

– I grunden är det krav på ett riskbaserat och systematiskt arbetssätt

– Artikel 21.1

> *Medlemsstaterna ska säkerställa att väsentliga och viktiga entiteter vidtar **lämpliga** och proportionella **tekniska**, driftsrelaterade och **organisatoriska åtgärder** för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och för att förhindra eller minimera incidenters påverkan på mottagarna av deras tjänster och på andra tjänster.*

Specifika åtgärder i art 20.2

– Riskhantering
– Systemsäkerhet
– Incidenthantering
– Driftskontinuitet
– Säkerhet i leveranskedjor
– Säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem

Sveriges Kommuner och Regioner

Specifika åtgärder i art 20.2

- Förmåga att bedöma effektiviteten i vidtagna åtgärder
- Cyberhygien och utbildning i cybersäkerhet
- Användning av kryptografi och kryptering
- Personalsäkerhet, åtkomstkontroll och tillgångsförvaltning
- Användning av lösningar för multifaktorautentisering eller kontinuerlig autentisering, säkrade röst-, video- och textkommunikationer och säkrade nödkommunikationssystem

Tekniska och metodologiska specifikationer

- Senast den 17 oktober 2024 ska det finnas detaljerade krav för:
  - leverantörer av DNS-tjänster och registreringsenheter för toppdomäner
  - leverantörer av molntjänster och datacentraltjänster
  - leverantörer av nätverk för leverans av innehåll (ex stadsnät)
  - leverantörer av hanterade tjänster
  - leverantörer av hanterade säkerhetstjänster
  - leverantörer av marknadsplatser online
  - sökmotorer och för plattformar för sociala nätverkstjänster
  - kvalificerade tillhandahållare av betrodda tjänster (ex underskriftstjänst)

Sanktionsavgifter i art 34

- Medlemsstaterna ska säkerställa att de administrativa sanktionsavgifter som påförs för överträdelser är effektiva, proportionella och avskräckande...
- Väsentliga entiteter högst € 10M eller högst 2 % av den totala globala årsomsättningen.
- Viktiga entiteter högst € 7M eller högst 1,4 % av den totala globala årsomsättningen

Sveriges Kommuner och Regioner

Inspiration och stöd

- Ledningssystem för informationssäkerhet (LIS)
- KLASSA
  - Uppdaterad kravkatalog för NIS mm tillgängliggörs inom kort
  - Modul för metodstöd i riskhantering under utveckling
- SKR / Offentliga fastigheter ”Trygg och säker informationshantering”
  - Vägledning om NIS, CER och säkerhetsskydd samt riskhantering
- Säpos vägledning för informationssäkerhet (B/H)
- Föreskrifter NIS
  - Uppdateras av MSB och sektorsmyndigheter efter februari 2024