
BRS
networks

NIS2 och cybersäkerhetslagen

Korta fakta om BRS Networks

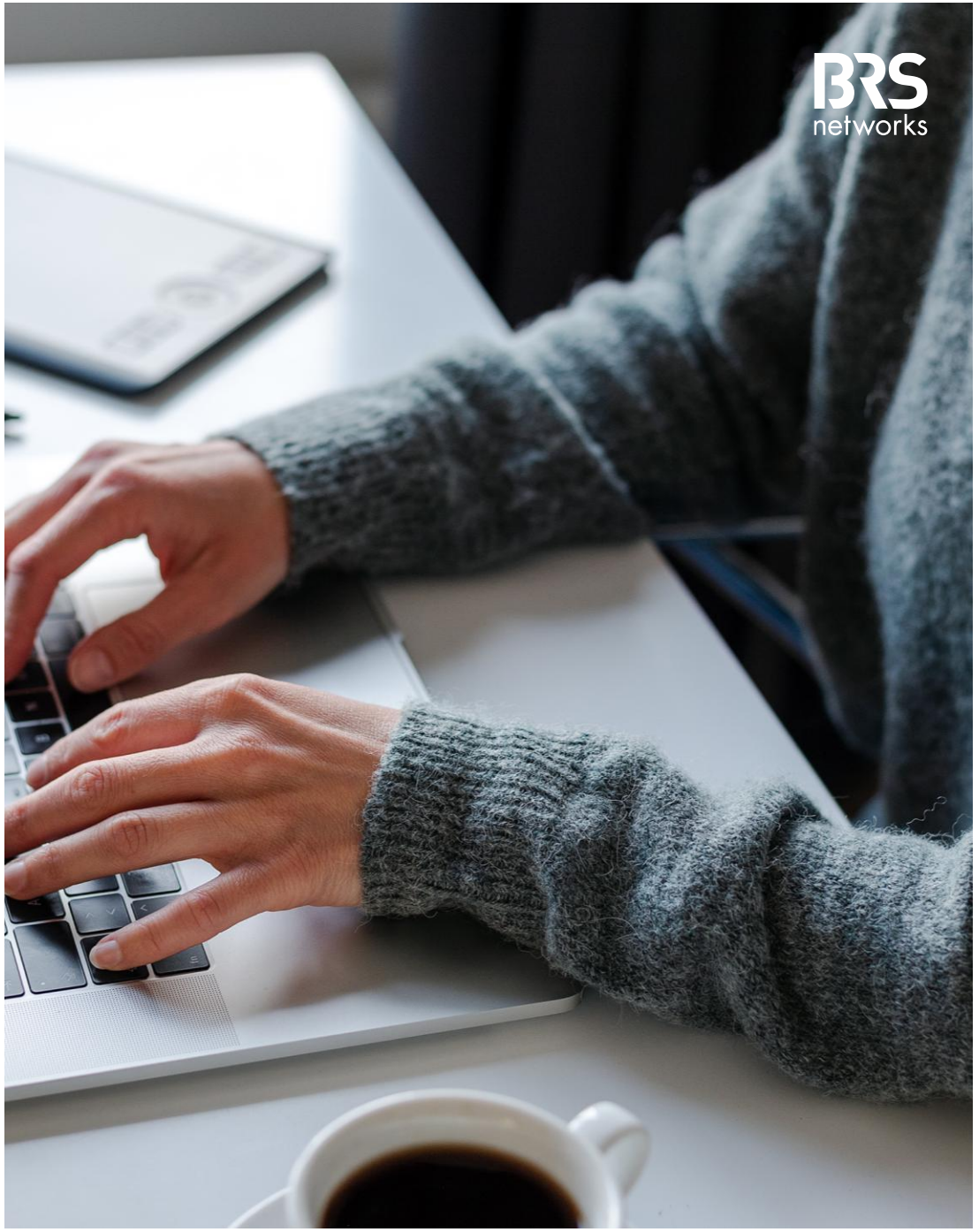
- Grundades 2011
- Huvudkontor i Visby
- Ca 80 medarbetare i koncernen
- Ägt av gotlänningar
- Koncernomsättning ca 150 mkr

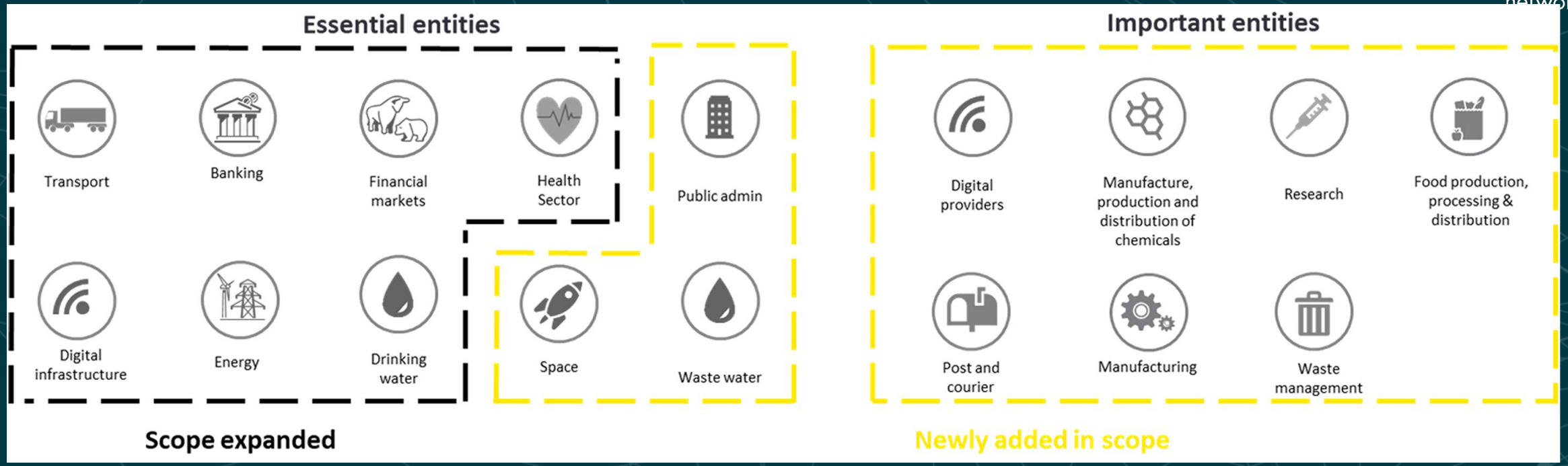
- Visby
- Kalmar/Öland
- Norrtälje
- Düsseldorf, DE
- Hannover, DE

NIS2

Syftet med NIS2 är att **höja den gemensamma nivån av cybersäkerhet** inom EU genom:

- Skärpta och tydligare krav på hur verksamheter ska arbeta med informations- och IT-säkerhet.
- Tydliga regler för **incidentrapportering** vid allvarliga cyberangrepp och IT-incidenter.
- Förstärkt **tillsyn** och sanktioner för aktörer som inte följer regelverket.





NIS2 har förenklat avgränsningen som de behöriga myndigheterna måste göra. En lista över sektorer har definierats och en grundregel är att alla stora (med över 250 anställda eller mer än 50 miljoner euro i omsättning) eller medelstora (med över 50 anställda eller mer än 10 miljoner euro i omsättning) företag från dessa sektorer kommer att inkluderas direkt i omfattningen.

Små eller mikroföretag är dock inte nödvändigtvis undantagna; medlemsstaterna kan utöka dessa krav om ett företag uppfyller specifika kriterier som indikerar en nyckelroll för samhället, ekonomin eller för särskilda sektorer eller typer av tjänster.

Säkerhetsåtgärdskrav

NIS2-direktivet ställer krav att entiteter som omfattas av direktivet ska vidta lämpliga och proportionella åtgärder kring säkerhetsarbetet. Detta för att hantera risker som hotar säkerheten i nätverks- och informationssystem som används för att tillhandahålla tjänsten.

Ytterligare anledningen till att det ska finnas säkerhetsåtgärdskrav är för att förhindra en incident i förstahand, men även vid en inträffad incident ska det påverka tillhandahållandet av tjänsten så lite som möjligt.

Vid bedömning av vad som är lämplig och proportionell åtgärd, ska det ta hänsyn till entitetens:

- Grad av riskexponering mot cybersäkerhet
- Storlek
- Sannolikheten att incidenter inträffar
- Vilken allvarlighetsgrad incidenten skulle inbegripa, både samhälleliga och ekonomiska konsekvenser.

Risk kring cybersäkerhet

Den reviderade direktivet ställer även krav på tio minimumåtgärder som ska vara inkluderade i verksamhetens arbete av riskhanteringen. Dessa åtgärder ska hantera riskerna och hot mot nätverks-och informationssystemen som används för att tillhandahålla verksamheten.

Om de 10 minimumåtgärderna inte är inkluderad i verksamhetens arbete med riskhanteringen kan det bland annat medföra sanktionsavgifter.

Man kan inte heller ”avtala bort” riskerna genom att peka på att en leverantör borde ha ansvarat.

Därav är det obligatorisk att entiteter som NIS2 omfattas inför följande åtgärder…

1 - 5

- Riskbedömningar och säkerhetspolicyer för informationssystem
- Policyer och procedurer för att utvärdera effektiviteten av säkerhetsåtgärder
- Policyer och procedurer för användning av kryptografi
- En plan för hantering av säkerhetsincidenter
- Säkerhet kring upphandling av system samt utveckling och drift av system

6 - 10

- Säkerhetsprocedurer för anställda med tillgång till känslig eller viktig data
- En plan för att hantera affärsverksamhet under och efter en säkerhetsincident
- Användning av multifaktorautentisering
- Säkerhet kring leveranskedjor och relationen mellan företaget och direktleverantören
- Cybersäkerhetsutbildning och praxis för grundläggande datorsäkerhet

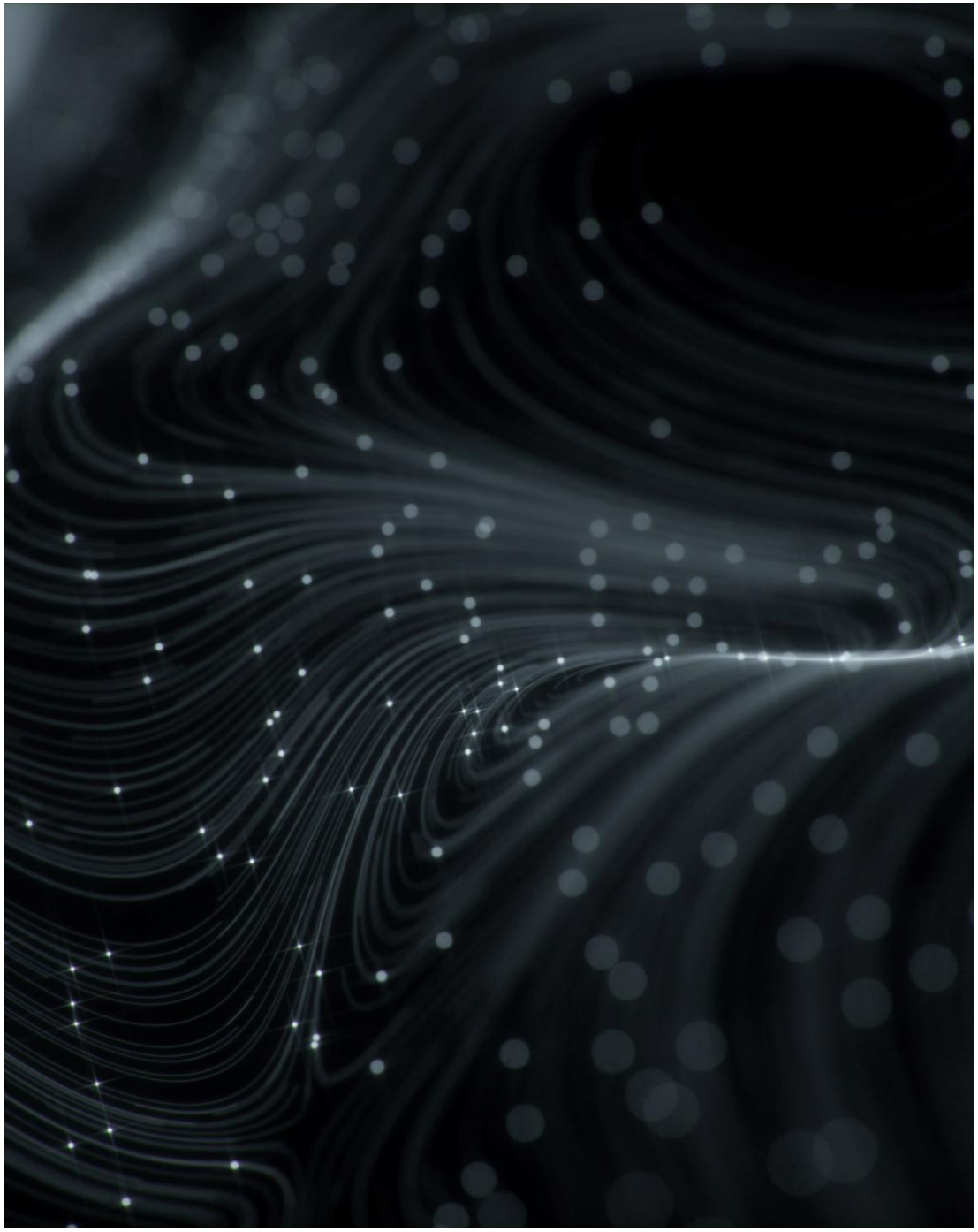
Nya rapporteringskrav

Om du råkar ut för en säkerhetsincident måste du meddela rätt personer. NIS2-direktivet ger tydliga instruktioner för hur organisationer ska rapportera säkerhetsincidenter.

- **Inom 24 timmar:** Skicka en tidig varning till CSIRT-enheten eller den nationella myndigheten. Ange om incidenten tros vara skadlig eller olaglig och om den kan få gränsöverskridande konsekvenser.

- **Inom 72 timmar:** Lämna in en incidentanmälan som uppdaterar den tidiga varningen med en bedömning av incidentens allvarlighetsgrad, konsekvenser och eventuella tecken på intrång.

- **Inom 1 månad:** Lämna in en slutrapport med en detaljerad beskrivning av incidenten, dess allvarlighetsgrad och inverkan, orsaker, vidtagna och pågående riskreducerande åtgärder samt den internationella inverkan.



Rent konkret då?

- Kraven kommer införas i svensk lag i slutet av 2025
- Man behöver ha ett systematiskt arbete

- Exempel på företag på Gotland som omfattas direkt
- - Destination Gotland
- - GEAB
- - BRS Networks

- Ställer även krav när man är leverantör till en kund
- - Säkerhetsnivå och systematiskt arbete
- - Incidentrapportering
- - SLA:er

- Vite
- Upp till 10 MEUR eller 2% av omsättningen

Summering

Högre krav på robusthet och systematik

- Analysera och jämför befintliga säkerhetsåtgärder mot de nya kraven med en GAP-analys
- Skärp rutinerna kring incidentrapportering
- Engagera styrelse och företagsledning
- Kontinuerlig riskanalys och systematiska processer för att skydda verksamheten
- Säkra leverantörskedjan

Kontakt: per.jordeglans@brsnetworks.se