# Sammanfattning av förslag till cybersäkerhetslag för genomförande av NIS2-direktivet i Sverige

Maj 2024

pwc

# Bakgrund

Nedan text är en sammanfattning av den statliga utredningen (SOU 2024:18) med tillhörande lagförslag som har lämnats, med syfte att genomföra NIS2-direktivet i Sverige.

NIS-direktiven syftar till att skapa en hög gemensam säkerhet avseende informations- och it-säkerhet inom EU. Det första direktivet antogs 2016. Sedan dess har informations- och nätverkssystem blivit än mer centrala och nödvändiga för att såväl människors vardagsliv, näringsliv och grundläggande samhällsfunktioner ska fungera. Samtidigt har också hotbilden mot dessa system höjts, och incidenter har både ökat och blivit mer omfattande och sofistikerade.

Utifrån den bakgrunden antogs i slutet av 2022 ett nytt direktiv, NIS2, som ersätter det tidigare direktivet. NIS2 ställer tydligare krav på bland annat riskanalyser och olika säkerhetsåtgärder. Direktivet ställer även ökade krav på ledningens deltagande i organisationens cybersäkerhetsarbete. NIS2 innebär också att betydligt fler sektorer omfattas av lagstiftningen jämfört med NIS. De aktörer som omfattas av lagstiftningen kommer också göra det på ett mer ingripande sätt än tidigare. Sanktionerna blir även kraftfullare än idag i det fall kraven inte efterlevs.

Utredningen föreslår att den nuvarande lagen (lag om informationssäkerhet för digitala och samhällsviktiga tjänster) upphävs och ersätts av en ny lag; cybersäkerhetslagen. Förslaget till cybersäkerhetslag innebär ett genomförande av NIS2-direktivet, men innehåller även förslag som går längre än direktivet. Den nya cybersäkerhetslagen föreslås träda i kraft den 1 januari 2025. Observera att det inte finns någon övergångsregel utan den nya lagstiftningen börjar gälla i sin helhet från första dag.

# Vem omfattas?

## Sektorer

Antalet sektorer som omfattas har ökat från sju till 18. De sektorer som omfattas är nu:

- energi,
- transporter,
- bankverksamhet,
- finansmarknadsinfrastruktur,
- hälso- och sjukvårdssektorn,
- dricksvatten,
- avloppsvatten,
- digital infrastruktur,
- förvaltning av IKT-tjänster (mellan företag),
- offentlig förvaltning,
- rymden,
- post- och budtjänster,
- avfallshantering,
- tillverkning, produktion och distribution av kemikalier,
- produktion, bearbetning och distribution av livsmedel,
- tillverkning av vissa produkter exempelvis medicinteknik, datorer och transportmedel,
- digitala leverantörer samt
- forskning.

Avseende sektorn offentlig förvaltning föreslås att den ska inkludera i princip alla myndigheter, det vill säga både statliga myndigheter, regioner och kommuner.

## Från “tjänst” till “verksamhetsutövare”

Med nuvarande lagstiftning omfattas endast samhällsviktiga och digitala tjänster av NIS-reglerna. Det innebär att det inte är hela verksamheten inom ett bolag eller myndighet som behöver följa NIS-reglerna. Förslaget till ny lagstiftning innebär att det inte längre ska vara tjänster som omfattas av lagkraven, utan verksamhetsutövare. Verksamhetsutövare ska förstås som fysisk eller juridisk person som bedriver verksamhet.

Detta innebär att, enligt lagförslaget, om en verksamhetsutövare (det vill säga en juridisk person och i teorin även enskilda firmor) till någon del omfattas av NIS2-reglerna, ska hela verksamheten omfattas av regelverket.

## Ledningens ansvar

Det nya regelverket tydliggör även ansvaret för verksamhetsutövarnas ledningsfunktioner. I huvudsak avses styrelse, VD och vice VD. Dessa funktioner ska övervaka implementeringen av riskhanteringsåtgärder, följa upp dessa och säkerställa att åtgärder vidtas vid brister. För att understryka vikten av detta ansvar föreslås att personer med ledningsansvar hos en verksamhetsutövare ska kunna förbjudas att utöva ledningsfunktioner där.

# Vem omfattas?

## Storlekskravet

För enskilda verksamhetsutövare gäller som huvudregel ett storlekskrav med innebörd att verksamheten måste sysselsätta minst 50 personer och ha en årsomsättning som överstiger 10 miljoner euro för att omfattas av lagen. Detta innebär att huvudregeln också är att aktörer som inte når upp till dessa storlekskrav inte kommer att omfattas av NIS2-reglerna.

Det finns ett antal särregler som innebär att även mindre aktörer kan omfattas i vissa fall. Exempelvis om aktören är av särskild betydelse på regional eller nationell nivå, om en störning avseende den tjänst som aktören tillhandahåller kan få påverkan på människors liv och hälsa, aktören tillhandahåller allmänna elektroniska kommunikationsnät eller är en tillhandahållare av betrodda tjänster (exempel på betrodda tjänster är elektronisk legitimation eller certifikat för autentisering av webbplatser).

För myndigheter föreslås heller inget storlekskrav att gälla, utan de omfattas i princip alltid, i sin helhet, av de nya reglerna.

## Koncerner

För att avgöra om ett företag omfattas av NIS2-regelverket behöver man göra en storleksbedömning. Storleken mäts genom antalet anställda och omsättning/balansomslutning. Det är inte enbart det enskilda bolagets storlek som ska räknas in, utan även så kallade anknutna företag och partnerföretag. Definitionen av anknutna företag stämmer i allt väsentligt överens med aktiebolagslagens definition av koncern. Med partnerföretag avses företag som inte betecknas som anknutna, men som har en kapital- eller röstandel på minst 25 procent i ett annat företag eller om ett annat företag har samma kapital- eller röstandel i det företaget. Innebörden av detta blir att även företag som inte når upp till storlekskravet som egen juridisk person kan göra det på grund av sambandet med exempelvis ett moderbolag.

Samtidigt anger NIS2-direktivet att anknutna företag och partnerföretag inte behöver omfattas av regelverket om det kan anses oproportionerligt. Utifrån den regeln föreslår utredningen att det ska skapas möjligheter till undantag i den svenska lagstiftningen. Det föreslås att detta ska regleras i den kommande så kallade cybersäkerhetsförordningen, som regeringen föreslås kunna besluta om.

### Undantag

Vissa typer av verksamheter är undantagna NIS2-regelverket och det svenska lagförslaget. Det handlar i huvudsak om statliga myndigheter som bedriver säkerhetskänslig verksamhet eller brottsbekämpning.

# Riskhanteringsåtgärder

## Självbedömning och anmälningsplikt

En verksamhetsutövare som omfattas av lagen ska anmäla sig till sin tillsynsmyndighet (exempelvis ska Transportstyrelsen vara tillsynsmyndighet för sektorn transporter och Finansinspektionen för sektorerna bankverksamhet och finansmarknadsinfrastruktur) och lämna uppgifter om bland annat identitet, kontaktuppgift och verksamhet. Indirekt innebär det också krav på att alla organisationer behöver göra en bedömning om man omfattas eller ej.

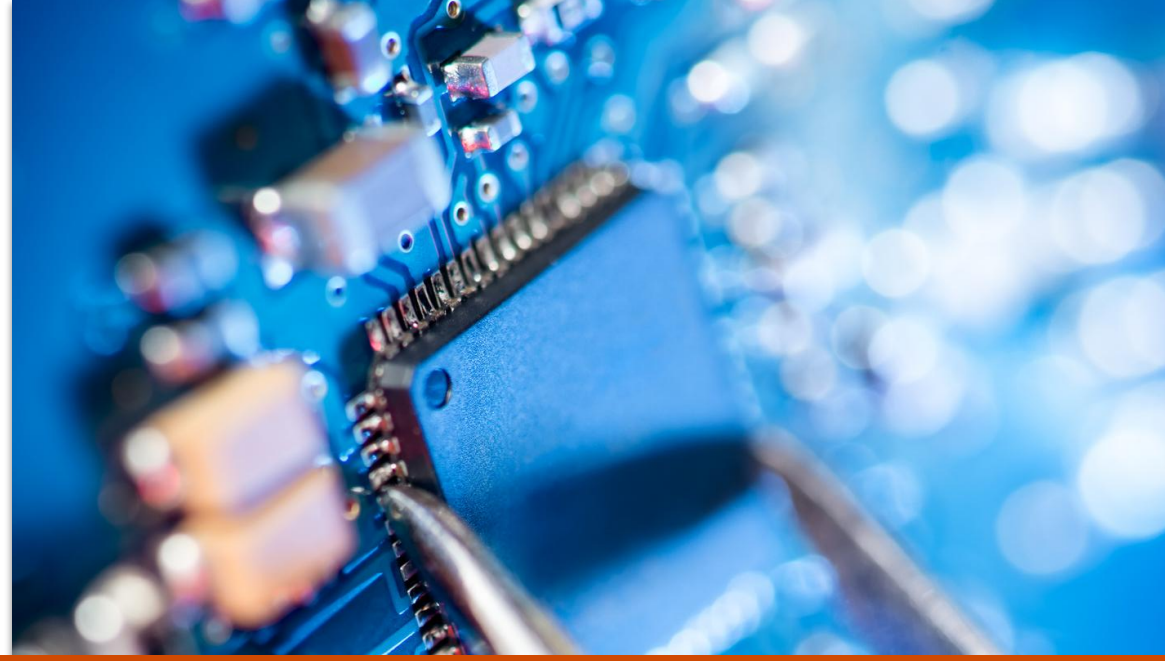
## Riskhanteringsåtgärder

Därutöver ska verksamhetsutövarna vidta riskhanteringsåtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. Åtgärderna ska utgå från en riskanalys, vara proportionella i förhållande till risken och de ska utvärderas.

Åtgärderna ska omfatta följande områden:

- incidenthantering,
- kontinuitetshantering,
- säkerhet i leveranskedjan,
- säkerhet vid förvärv,
- utveckling och underhåll av nätverks- och informationssystem inklusive hantering av sårbarheter och sårbarhetsinformation,
- strategier och förfaranden för användning av kryptografi och kryptering,
- personalsäkerhet,
- strategier för åtkomstkontroll och tillgångsförvaltning,
- säkrade lösningar för kommunikation och lösningar för autentisering.

Det ställs även krav på att verksamhetsutövaren ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete. Dessutom föreslås att ledningen måste genomgå utbildning om riskhanteringsåtgärder och att samtliga anställda erbjuds utbildning inom samma område.



**Incidenthantering och rapportering**

Utredningen föreslår en skyldighet att rapportera betydande incidenter till MSB (Myndigheten för samhällsskydd och beredskap). Detta innebär att verksamhetsutövaren ska lämna en varning om incidenten till MSB inom 24 timmar efter det att verksamhetsutövaren fått kännedom om incidenten. Vidare ska en incidentanmälan göras inom 72 timmar och en slutrapport ska upprättas inom en månad.

Vad är då en betydande incident? Utredningen föreslår följande definitioner:

1. En incident som orsakat eller kan orsaka allvarlig driftstörning för den erbjudna tjänsten eller ekonomisk skada för den berörda verksamhetsutövaren, eller,
2. En incident som har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada.

# Riskhanteringsåtgärder

### Incidenthantering och rapportering

Utredningen föreslår en skyldighet att rapportera betydande incidenter till MSB (Myndigheten för samhällsskydd och beredskap). Detta innebär att verksamhetsutövaren ska lämna en varning om incidenten till MSB inom 24 timmar efter det att verksamhetsutövaren fått kännedom om incidenten. Vidare ska en incidentanmälan göras inom 72 timmar och en slutrapport ska upprättas inom en månad.

Vad är då en betydande incident? Utredningen föreslår följande definitioner:

1. En incident som orsakat eller kan orsaka allvarlig driftstörning för den erbjudna tjänsten eller ekonomisk skada för den berörda verksamhetsutövaren, eller,
2. En incident som har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada.

### Leveranskedjan

En särskild fråga som uppmärksammats mycket inför detta lagförslag är vad som avses med säkerhet i leveranskedjan och hur många led i kedjan som verksamhetsutövaren ansvarar för. Utredningen bedömer att direktivet ska tolkas så att säkerhet i leveranskedja betyder säkerhetsaspekter som rör förbindelserna mellan varje verksamhetsutövare och dess direkta leverantörer eller tjänsteleverantörer. Det betyder enligt utredningens uppfattning att varje verksamhetsutövare endast behöver vidta riskhanteringsåtgärder i förhållande till sin leverantör. Det innebär att förslaget är att varje verksamhetsutövare ansvarar för **ett** led i leveranskedjan.

# Tillsyn
# Sanktioner och ingripanden

## Tillsynsmyndighet

Systemet för tillsyn bör enligt utredningen utgå från den struktur som finns enligt dagens regelverk. Enligt nuvarande regelverk finns det för varje sektor och för de digitala tjänster som omfattas av lagen en utpekad tillsynsmyndighet. Utredningen förslår att det även fortsatt ska finnas en tillsynsmyndighet för varje sektor. I de sektorer som är oförändrade i förhållande till nuvarande lagstiftning är förslaget att redan befintliga tillsynsmyndigheter fortsätter vara det. Utredningen föreslår därutöver fem nya tillsynsmyndigheter; länsstyrelserna i Stockholm, Skåne, Västra Götalands och Norrbottens län (för sektorn offentlig förvaltning) samt Läkemedelsverket (för del av sektorerna hälso- och sjukvård samt tillverkning).

Inom ramen för tillsynen föreslås att tillsynsmyndigheterna får rätt att under vissa omständigheter genomföra säkerhetsrevision och säkerhetsskanning hos verksamhetsutövaren.

## Sanktionsavgifter

Sanktionsavgifternas maxnivåer föreslås att höjas till två procent av verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller tio miljoner euro. För myndigheter föreslås den maximala sanktionsavgiften bli 10 miljoner kronor.

**Övriga sanktioner och ingripanden**

- Tillsynsmyndigheterna föreslås kunna förelägga en verksamhetsutövare att offentliggöra information om överträdelser av lagens bestämmelser, och att informera användare som kan påverkas av ett betydande cyberhot.
- Det föreslås även att personer med ledningsansvar hos en verksamhetsutövare ska kunna förbjudas att utöva ledningsfunktioner där. I huvudsak avses styrelseledamöter samt VD och vice VD.

# Kontakta oss gärna om du vill veta mer!

Juridisk rådgivare
072-880 95 72
charlotte.arnell@pwc.com

Juridisk rådgivare
070-929 11 33
alexandra.selander@pwc.com

pwc.se