
itm8®
Today. Tomorrow. Together

Slutbetänkande SOU 2024:18 Cybersäkerhetslagen & lag om motståndskraft hos kritiska verksamhetsutövare

Analys och tankar från itm8 av:
Hannes Edström
Shadi Domat
Jens Johansson

itm8

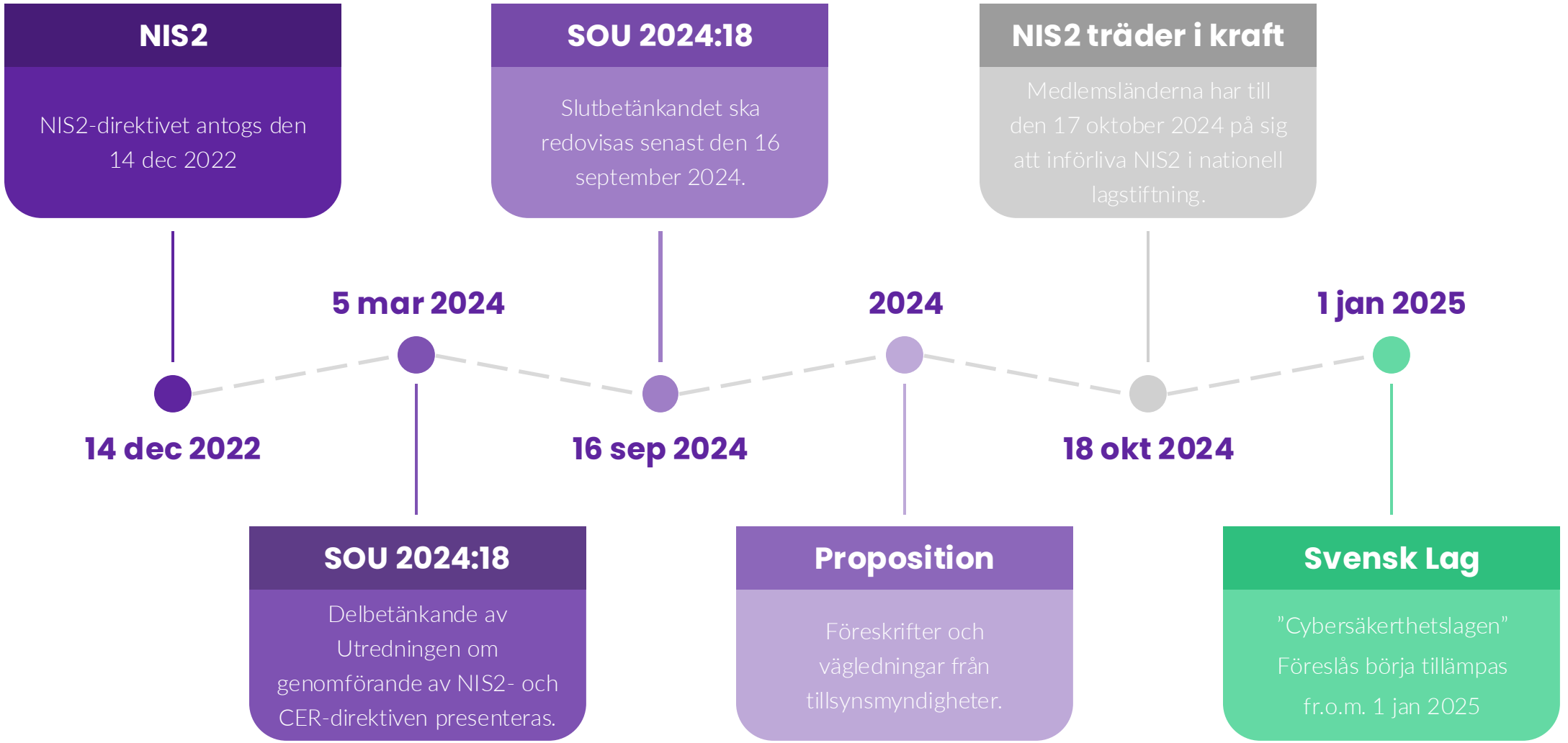
AGENDA

01. Vem kan omfattas?

02. Vad krävs av min verksamhet?

03. Ikraftträdande och nästa steg

TIDSLINJE – VAR STÅR VI JUST NU?



Vem kan omfattas?

Utredningens förslag:

En kritisk verksamhetsutövare är en offentlig eller enskild verksamhetsutövare som har identifierats enligt 2 kap. 1 § i den föreslagna lagen.

Utredningens förslag:

En enskild verksamhetsutövare är en juridisk eller fysisk person som bedriver verksamhet och som inte är en statlig myndighet, region eller kommun.

Vilka kan omfattas?

Kritiska verksamhetsutövare

- Energi
- Transporter
- Bankverksamhet
- Finansmarknadsinfrastruktur
- Hälso-och sjukvård
- Dricksvatten
- Avloppsvatten
- Digital infrastruktur
- Produktion, bearbetning och distribution av livsmedel
- Offentlig förvaltning
- Rymden

Enskilda verksamhetsutövare

- Post- och budtjänster
- Avfallshantering
- Tillverkning, produktion och distribution av kemikalier
- Tillverkning (ex. medicinteknik, elektronik, optik, transportmedel)
- Digitala leverantörer
- Förvaltning av IKT-tjänster
- Forskning

Vilka kan omfattas?

NIS

Kritiska verksamhetsutövare identifieras av tillsynsmyndigheterna.

Enskilda verksamhetsutövare som omfattas av bilaga 1 och 2 NIS2 direktivet.

Storleksdirektivet.

Vad krävs av min verksamhet? - Tydligare stöd

För att tydliggöra vad som krävs kommer tillsynsmyndighet/MSB tillhandahålla föreskrifter.

Riskbedömningar

Verksamhetsutövare måste genomföra en riskbedömning inom nio månader från att de har identifierats som kritiska verksamhetsutövare.

Riskbedömningen ska inkludera en bedömning av alla potentiella risker som kan leda till en incident och störa leveransen av samhällsviktiga tjänster.

Riskbedömningarna måste följas upp av konkreta åtgärder som syftar till att öka verksamhetens motståndskraft.

Åtgärder för motståndskraft

Verksamheter måste vidta tekniska och organisatoriska åtgärder för att säkerställa sin motståndskraft mot störningar och incidenter.

Åtgärderna ska vara baserade på riskbedömningen och proportionerliga i förhållande till verksamhetens storlek och den potentiella konsekvensen av en incident.

Verksamheterna förväntas också utveckla krisplaner som beskriver hur de ska agera vid en kris eller störning för att upprätthålla leveransförmågan.

Leverantörskedjan

Verksamhetsutövare måste säkerställa att även underleverantörer och tredje parter följer de säkerhetsåtgärder och riktlinjer som ställs för att upprätthålla motståndskraft i leveransen.

Verksamheter måste inkludera sina underleverantörer i riskbedömningen och utvärdera eventuella risker kopplade till leverantörskedjan.

Underleverantörernas förmåga att hantera och rapportera säkerhetsincidenter måste utvärderas och ligga till grund vid val av partner.

Bakgrundkontroller

Verksamhetsutövare måste genomföra bakgrundskontroller av personer i känsliga befattningar som kan påverka verksamhetens säkerhet och motståndskraft (kriminalregistret).

En befattningsanalys ska göras för att identifiera vilka roller som kräver bakgrundskontroller, och denna analys ska dokumenteras.

Bakgrundskontroller ska dokumenteras och vara tillgängliga vid en tillsyn.

Incidentrapportering

Kritiska verksamheter är skyldiga att rapportera incidenter som medför, eller kan medföra, betydande störningar i deras tjänster, till MSB.

En första rapport ska lämnas inom 24 timmar efter vetskap av incidenten, och en mer detaljerad rapport ska lämnas senast en månad därefter.

Samverkan och efterlevnad

Samarbete med tillsynsmyndigheter
Verksamheter måste samarbeta med tillsynsmyndigheterna genom att ge tillgång till nödvändig information och tillåta de tillsyner som tillsynsmyndigheterna anser nödvändiga.
De måste också bistå i nationella riskbedömningar och bidra med relevant information.

Samverkansansvarig
Varje kritisk verksamhetsutövare måste utse en samverkansansvarig som ska fungera som kontaktpunkt för berörda myndigheter och säkerställa att verksamheten följer sina skyldigheter.

Efterleva sanktioner och föreläggande
Vid bristande efterlevnad kan verksamheterna drabbas av sanktioner, som exempelvis sanktionsavgifter eller förelägganden om att åtgärda brister.

Samverkan och efterlevnad

Sekretess och informationssäkerhet
Verksamheter ska följa de sekretesskrav som ställs, särskilt kring incidentrapporter och bakgrundskontroller, för att säkerställa att känslig information inte sprids obehörigt.

Uppföljning och revision
Riskbedömningen ska kontinuerligt uppdateras anpassas efter förändrade förutsättningar och händelser i omvärlden.
Verksamheter måste kontinuerligt följa upp och vid behov justera sina åtgärder för att säkerställa att de förblir motståndskraftiga mot nya hot och risker.

Incidentövningar och krisplanering
Verksamheter förväntas genomföra regelbundna övningar för att testa sin förmåga att hantera incidenter och kriser, samt upprätthålla planer för kontinuitet i kritiska leveranser.

Ikraftträdande och nästa steg

Föreskrifter från tillsynsmyndigheterna och MSB kommer att komma.

Lagen om cybersäkerhet föreslås träda i kraft den 1 januari 2025.

Den föreslagna lagen om motståndskraft hos kritiska verksamhetsutövare föreslås träda i kraft den 1 augusti 2025.

Tack för ert deltagande

Jens Johansson

jjoha@itm8.com