Lag om Informationssäkerhet för Samhällsviktiga och Digitala Tjänster

NIS direktivet - Checklista

Denna checklista innehåller 7 punkter som rekommenderas att alla aktörer som berörs av den nya lagen bör gå igenom då lag om informationssäkerhet för samhällsviktiga och digitala tjänster började gälla från 1 augusti 2018.

Det nya regelverket har börjat gälla fullt ut och detta förutsätter att alla leverantörer av samhällsviktiga tjänster kan visa att man följer reglerna.

NIS direktivet är ett EU direktiv, vars syfte är att höja den inre marknadens funktioner och därigenom uppnå ekonomisk stabilitet. Vidare ska direktivet främja samarbete mellan medlemsstaterna för att lösa de utmaningar som verksamheter och nationer ställs inför. Genom att kontinuerligt arbeta med informationssäkerhet för att säkerställa leverans av samhällsviktiga och digitala tjänster är förhoppningen att samhällen ska fungera bättre, både vid kris och i vardagen.

Gällande samhällsviktiga tjänster är det sju sektorer som berörs, där en tillsynsmyndighet för respektive sektor har utsätts i syfte att kontrollera efterlevnad av de lagstadgade kraven. Sektorer och respektive tillsynsmyndighet finns att läsa i tabellen nedan.

Sektor	**Tillsynsmyndighet**
Energi	Energimyndigheten
Transport	Transportstyrelsen
Bankverksamhet	Finansinspektionen
Finansmarknadsinfrastruktur	Finansinspektionen
Hälso- och sjukvård	Inspektionen för vård och omsorg (IVO)
Leverans och distribution av dricksvatten	Livsmedelsverket
Digital infrastruktur	Post- och telestyrelsen (PTS)

Lagen lägger stor vikt vid leverantörens skyldighet att kunna visa att direktivet följs och att den rätta dokumentationen finns på plats.

Leverantörer av samhällsviktiga är skyldiga att anmäla sig till den tillsynsmyndighet som har tillsynsansvar för den sektor leverantören verkar inom. Detta ska ske utan dröjsmål och ska följa föreskrift framtagen av MSB (MSBFS 2018:7).

MSBFS 2018:7 finns att läsa här https://www.msb.se/externdata/rs/0264c176-6b31-43c6-9fd8-807102df3844.pdf

Vid frågor om NIS direktivet kan MSB kontaktas på fraga.nis@msb.se

1. Förbered verksamheten

Är er organisation medveten om nya lagen om informationssäkerhet för samhällsviktiga och digitala tjänster?

- Ni bör försäkra er om att beslutsfattare, medarbetare och nyckelpersoner inom er organisation är medvetna om att lagen om informationssäkerhet för samhällsviktiga och digitala tjänster träder trädde i kraft 1 augusti 2018.
- Ni bör också undersöka hur er organisation kommer att påverkas av lagen och identifiera de områden som ni måste arbeta särskilt med.

Ni kan behöva avsätta betydande resurser för att hinna anpassa er organisation till de nya kraven. Inledningsvis bör ni särskilt fokusera på att öka medvetenheten om de kommande förändringarna. Det kan bli både kostsamt och svårt att uppfylla reglerna i förordningen om ni väntar med förberedelserna till sista stund.

2. Organisera NIS-arbetet

Se till att det finns en organisation på plats som kan arbeta med att säkerställa leverans av samhällsviktiga tjänster. Detta sker genom systematiskt informationssäkerhetsarbete, vilket är att krav i lagen. MSB har tagit fram föreskrift för hur systematiskt och riskbaserat informationssäkerhetsarbete ska bedrivas inom ramen för lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (MSBFS 2018:8). Där specificeras att standarder så som SS-EN ISO/IEC 27000-serien eller motsvarande ska användas för att bygga upp ett ledningssystem för informationssäkerhet (LIS) och därigenom uppnå systematik.

MSBFS 2018:8 finns att läsa här https://www.msb.se/externdata/rs/9b5c0905-20c5-4fe6-8341-5b481cc570a4.pdf

En nyhet med det nya regelverket är att leverantörer av samhällsviktiga tjänster har fått ett tydligare ansvar för kontinuerligt och säkert leverera en tjänst. Det finns även nya krav på att organisationen måste kunna visa upp att man följer regelverket och hur man följer det.

- Aktörer rekommenderas att se över sin interna styrning och sina riktlinjer för hur den samhällsviktiga tjänsten levereras.
- Se till att det finns en organisation med utpekat ansvar och roller som inte enbart är en projektorganisation utan ger förutsättningar för att kontinuerligt arbeta med området.

- Utse någon ansvarig för organisationens arbete som kan rapportera till ledningen.

3. Kartlägg

Identifiera vilka system som finns i verksamheten som är nödvändiga för att kunna leverera tjänsten på ett korrekt och säkert sätt.

- Inventera och dokumentera vilka system ni har, hur er infrastruktur ser ut, samt hur dessa system samverkar.
- Se över rutiner och instruktioner så att det inte blir ett engångsarbete utan att inventering av system och infrastruktur sker regelbundet samt vid behov.

4. Analysera

Identifiera vilka skyddsåtgärder som behövs och vilka risker som kan tillkomma.

- Genomför riskanalys över vilka risker som finns mot systemet som kan påverka organisationens förmåga att leverera den tjänst ni leverera på ett säkert och korrekt sätt.
- Genomför konsekvensanalys för vilka konsekvenser misslyckande av leverera tjänsten kan få.

5. Dokumentera

Samla systematiskt och fortlöpande dokumentation som visar hur ni följer lagen om informationssäkerhet för samhällsviktiga och digitala tjänster.

- Besluta en övergripande policy för informationssäkerhet som beskriver mål, styrning, organisation och ansvar för informationssäkerhet.
- Se till att dokumentation om informationssäkerhet hålls på ett ordnat och systematiskt sätt och att rutiner finns för att hålla det uppdaterat.
- Samla bevis för hur reglerna följs.

Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster ställer krav på att den organisationen som leverera en samhällsviktig eller digital tjänst ska kunna visa att man följer reglerna och även hur man följer reglerna. Detta kan kräva att ytterligare analyser utförs, utöver risk och konsekvensanalyser, så som GAP-analyser för att påvisa att organisationen strävar mot efterlevnad av lagrummet.

6. Inför nya rutiner

Se till att förberedelsearbetet tar sikte på att arbetet med informationssäkerhet för samhällsviktiga och digitala tjänster ska fungera kontinuerligt i organisationen.

- Planera för att organisationen ska kunna upprätthålla ett långsiktigt arbete kring informationssäkerhet och kontinuerlig leverans av tjänster.
- Se även över befintliga processer och styrdokument för processer som kan påverka leveransen av tjänsten, t.ex. dokument- och ärendehantering, upphandling, systemförvaltning och IT-drift så att de vid behov kompletteras med dataskyddsåtgärder.
- Gör regelbunden eller behovsbaserad (till exempel vid inköp av nya system eller omgjord infrastruktur) inventering av IT system.

7. Incidenthantering

Se till att det finns rutiner för incidenthantering och rapportering vid en incident som påverkar organisationens förmåga att leverera en samhällsviktig eller digital tjänst. Detta är ett krav ställd av det nya lagrummet.

- Utse vem som internt ska rapportera en incident till ägare av system eller ägare av tjänsten.
- Utse vem som är ansvarig att stoppa incidenten, så att leverans av tjänst kan återupptas så snabbt som möjligt.
- Utse vem som ska rapportera till MSB/CERT-SE att en incident har inträffat.

MSB har tagit fram föreskrifter för hur rapportering av incident ska ske. Ur dessa framgår att MSB/CERT-SE ska underrättas via telefon vid en incident som påverkar tillhandahållandet av en samhällsviktig eller digital tjänst. Därefter ska skriftlig information om incident och hur tjänsten blivit störd inkomma. Detta kan ske via post eller med personlig överlämning i MSB:s reception i Stockholm. Mer om hur incidenter ska rapporteras kan läsas på MSB:s hemsida (https://www.msb.se/sv/Forebyggande/Informationssakerhet/NIS-direktivet/Incidentrapportering/Incidentrapportering-fran-1-november/), alternativt genom att kontakta CERT-SE.