PUBLITECH
by VISMA

# Checklista för NIS2

Så förbereder du din organisation för den nya cybersäkerhetslagen.

# Vad du behöver veta om den nya lagen

Den nya cybersäkerhetslagen, som bygger på EU:s NIS2-direktiv, blir snart verklighet i Sverige. För dig som arbetar med lön, HR eller ekonomi – och för beslutsfattare i offentlig sektor – innebär lagen tydligare krav på riskhantering, informationssäkerhet och skydd av kritiska system. Att ha kontroll över känslig data och förstå ledningens ansvar är viktigare än någonsin.

Mycket av det som lagen kräver ska redan vara på plats i en verksamhet som hanterar känslig data. Med den nya lagen blir det dock skarpare krav på **ledningens ansvar, säkerhetsåtgärder** och **incidentrapportering.**

Vad innebär det för dig i praktiken? Och hur kan du säkerställa att din organisation är redo? I den här guiden ger vi dig en praktisk översikt och konkreta råd för hur ni kan möta kraven.

# Vad är NIS2-direktivet?

NIS2-direktivet är en EU-lag som syftar till att höja cybersäkerheten inom hela EU genom att skapa en gemensam hög standard. Lagen omfattar fler sektorer och organisationer än sin föregångare, NIS1. För dig inom offentlig sektor innebär det att kraven på riskhantering, incidentrapportering och säkerhetsåtgärder skärps. Det handlar om att skydda samhällsviktiga tjänster från cyberhot som kan slå ut kritisk infrastruktur.

## Vem omfattas av NIS2?

NIS2 gäller inte alla organisationer, utan de som klassas som **”väsentliga” eller ”viktiga” aktörer**. Hit hör bland annat:

- Offentliga aktörer (kommuner, myndigheter, regioner) med ansvar för samhällsviktiga funktioner.
- Privata aktörer inom bl.a. energi, transport, hälso- och sjukvård, vattenförsörjning, avfall, digital infrastruktur, livsmedel, posttjänster, offentlig förvaltning och tillverkning av kritiska produkter.
- IT- och molntjänstleverantörer.

Även underleverantörer som levererar tjänster till dessa aktörer kan omfattas indirekt genom **krav i avtal**.

## Vad händer om man inte följer lagen?

NIS2 innehåller sanktioner som gör det nödvändigt att agera:

- Böter på upp till 10 miljoner euro eller 2 % av global årsomsättning.
- Möjlighet till personligt ansvar för ledningen vid bristande efterlevnad.

# NIS2 i praktiken: En checklista

NIS2-kraven påverkar hur alla verksamheter inom offentlig sektor hanterar känslig och kritisk information. Oavsett om det handlar om personaldata, ekonomidata eller annan samhällsviktig information, är det avgörande att ha tydlig kontroll och rutiner på plats.

Här är en checklista på områden du bör se över:

### Ledningens ansvar

- ☐ **Engagera ledningen:** Säkerställ att styrelse och ledning är direkt involverade och tar ansvar för cybersäkerheten. De kan hållas personligt ansvariga om kraven inte efterlevs.

- [ ] **Utbilda beslutsfattare:** Ge ledningen regelbunden utbildning så att de kan fatta välgrundade beslut.

## Säkerhet i leverantörskedjan

- [ ] **Kartlägg era leverantörer:** Identifiera alla som har åtkomst till era system och data.
- [ ] **Gör en riskbedömning:** Värdera riskerna med varje leverantör och ställ krav i avtal.
- [ ] **Övervaka leverantörers säkerhet:** Följ upp deras säkerhetsnivå regelbundet.

## Informationssäkerhet

- [ ] **Inventera känslig data:** Kartlägg var HR-, löne- och ekonomidata lagras.
- [ ] **Uppdatera era säkerhetspolicyer:** Säkerställ att informationssäkerhetspolicyer är aktuella.
- [ ] **Genomför interna revisioner:** Kontrollera system och rutiner regelbundet.

## Riskbedömning och incidenthantering

- [ ] **Gör en gapanalys:** Jämför er nuvarande säkerhetsnivå med NIS2.
- [ ] **Incidentrapportering i tre steg:**
- Förvarning inom **24 timmar**.
- Detaljerad rapport inom **72 timmar**.
- Slutrapport inom **en månad**.
- [ ] **Utbilda personal och ledning:** Alla ska förstå sin roll vid en incident.

## Datasäkerhet

- [ ] **Starka autentiseringsmetoder:** Använd MFA, starka lösenord och regelbundna byten.
- [ ] **Patchning och uppdateringar:** Ha en process för att snabbt täppa till sårbarheter.
- [ ] **Nätverkssegmentering:** Minimera skador vid intrång genom att isolera system.
- [ ] **Loggning och övervakning:** Implementera kontinuerlig loggning och hotdetektion.
- [ ] **Säkerhetskopior:** Ta regelbundna kopior och testa återställning.

### Återhämtningsplaner

- ☐ **Utveckla en BCP (Business Continuity Plan):** Beskriv hur verksamheten återställs snabbt.
- ☐ **Samarbeta med leverantörer:** Säkerställ att även de har planer för katastrofåterställning.

# Viktigt om systemleverantörer

NIS2 ställer krav på att ni har kontroll på leverantörers säkerhet. Dina mjukvaruleverantörer är en central del av säkerhetskedjan. Att välja en partner som aktivt arbetar för att uppfylla NIS2-kraven är en stor del av riskhanteringen.

# Publitech: En trygg partner för en NIS2-säker vardag

På Publitech är säkerhet en integrerad del av våra system:

- **ISO-certifieringar:** Vi är certifierade enligt ISO 9001 (kvalitet), ISO 14001 (miljö) och ISO 27001 (informationssäkerhet) – tre internationellt erkända standarder som visar att vi arbetar systematiskt och långsiktigt för att leverera hög kvalitet, minska vår miljöpåverkan och skydda känslig information.
- **Datacenter i Sverige** enligt MSB:s skyddsklass 3.
- **Säkerhetsprogram i Visma-koncernen:** penetrationstester, övervakning av darknet och sårbarhetsskanning.

👉Läs mer om vårt säkerhetsarbete