Guide till NIS2

Vad svenska företag behöver veta och göra

1. Inledning – Vad är NIS2 och varför spelar det roll?

NIS2 är EU:s nya cybersäkerhetsdirektiv, skapat för att stärka den digitala säkerheten inom unionen. Det är en uppdatering av det tidigare NIS-direktivet från 2016, och innebär skärpta krav på informationssäkerhet, riskhantering och incidentrapportering för en bredare krets av företag och organisationer.

Kort sagt: NIS2 är inte längre något som bara gäller myndigheter och storbolag. Om ditt företag, verkar inom vissa sektorer eller levererar till kritiska aktörer, är det hög tid att börja arbeta med cybersäkerhet på ett mer strukturerat sätt.

Bakgrunden till direktivet är en snabbt föränderlig hotbild där cyberattacker blir allt vanligare, mer sofistikerade och i ökande grad riktas mot samhällsviktig verksamhet. Det tidigare NIS-direktivet ansågs otillräckligt – tillämpningen varierade kraftigt mellan medlemsländer, sektorsomfånget var begränsat och kraven på åtgärder ofta otydliga. NIS2 syftar därför till att skapa en mer enhetlig och robust reglering för cybersäkerhet i hela EU, med tydligare ansvar, hårdare krav och utökad tillsyn.

Direktivet började gälla på EU-nivå den 16 januari 2023, och alla medlemsländer skulle införa det i nationell lagstiftning senast den 17 oktober 2024. I Sverige är det dock ännu inte infört – ett lagförslag i form av en ny "cybersäkerhetslag" är ute på remiss och väntas träda i kraft under 2025.

Trots att lagen ännu inte är på plats, rekommenderar MSB att svenska företag förbereder sig redan nu, eftersom kraven kommer att införas och efterlevnad kommer att krävas så snart lagen är på plats.

Till skillnad från tidigare omfattar NIS2 inte bara stora aktörer inom samhällsviktig infrastruktur – utan även många mindre till medelstora företag, särskilt inom branscher med höga säkerhetskrav eller beroenden av digital infrastruktur. Det gäller oavsett om företaget har en egen IT-avdelning eller inte.

2. Vilka företag omfattas?

En av de stora förändringarna med NIS2 är att det omfattar fler typer av verksamheter än tidigare, och inkluderar även privata företag i fler sektorer. Det betyder att många fler svenska företag nu omfattas av kraven – även om man tidigare inte berörts av NIS-lagstiftning.

Två huvudkategorier i NIS2:

1. Väsentliga enheter (Essential Entities)
2. Viktiga enheter (Important Entities)

Båda dessa grupper omfattas av NIS2, men tillsynen och sanktionsmöjligheterna är något olika beroende på kategori.

Branscher som omfattas inkluderar energi, transport, hälso- och sjukvård, digital infrastruktur, posttjänster, tillverkning av kritiska produkter, samt leverantörer av IT- och säkerhetstjänster.

Storlekskriterier:

- 50 anställda eller fler
- Årlig omsättning över 10 miljoner euro

Kombinationen av sektor och storlek avgör om företaget omfattas. Även leverantörer till dessa sektorer kan påverkas, eftersom NIS2 ställer krav på hela leverantörskedjan.

Viktigt: Om ditt företag levererar till en verksamhet som omfattas, måste du kunna visa att du följer tillräckliga säkerhetsrutiner, eftersom din kund är skyldig att säkerställa sin leverantörskedjas cybersäkerhet enligt NIS2.

Scenarioöversikt:

- Namngiven sektor + storleksgräns: Ja, direkt reglerad
- Namngiven sektor men under gräns: Kanske, om samhällskritisk funktion
- Ej i sektor men över gräns: Troligen inte direkt, men kan påverkas via kundkrav

3. Vad innebär det i praktiken?

Att omfattas av NIS2 innebär inte bara att man behöver "ha bra IT-säkerhet" – utan att man ska kunna visa upp ett strukturerat, riskbaserat och dokumenterat cybersäkerhetsarbete.

Krav i praktiken:

- Riskhantering
- Incidenthantering (rapportering inom 24h)
- Tekniska och organisatoriska säkerhetsåtgärder
- Dokumentation och ansvarsfördelning
- Uppföljning och förbättring
- Kontroll av leverantörer

Certifiering krävs inte, men dokumenterad struktur och metodik är avgörande. I den kommande Cybersäkerhetslagen väntas detta förtydligas ytterligare.

4. Krav på leverantörer – kontroll över hela kedjan

Företag som omfattas av NIS2 måste säkerställa att deras leverantörer också håller en tillräcklig säkerhetsnivå.

Det innebär att man ska:

- Kartlägga affärskritiska leverantörer
- Säkerställa att dessa följer god cybersäkerhetspraxis
- Ha säkerhetskrav i avtal/SLA:er
- Inkludera leverantörer i riskanalys och incidentrutiner

Exempel på checklista till leverantörer:

- ✓ Följer ni en säkerhetsstandard (ex. ISO 27001)?
- ✓ Hur hanterar ni incidentrapportering?
- ✓ Vilka tekniska skyddsåtgärder har ni?
- ✓ Kan ni dokumentera ert säkerhetsarbete?
- ✓ Hur styr ni säkerhet i er egen leverantörskedja?

Även företag som inte omfattas direkt av NIS2 kan påverkas genom kundkrav

FEM STEG FÖR ATT KOMMA IGÅNG MED NIS2-ARBETET

1. Identifiera om ni omfattas

- Kontrollera sektor och storlek
- Tänk även på indirekt påverkan via kunder

2. Kartlägg era digitala beroenden och risker

- Gör en enkel riskanalys
- Identifiera kritiska system och leverantörer

3. Utse ansvarig för cybersäkerhet

- Intern eller extern resurs med tydligt mandat

4. Dokumentera era rutiner

- Skriv ner det ni redan gör bra
- Skapa styrdokument

5. Skapa en åtgärdsplan och följ upp

- Lista förbättringsområden och prioritera
- Sätt en plan för löpande uppföljning

Det viktigaste är att komma igång och skapa struktur. Arbetet med cybersäkerhet är inte ett projekt – det är en pågående process

5. Vanliga utmaningar vid införande av NIS2-krav

Vanliga utmaningar inkluderar:

- Missuppfattningen att “det gäller inte oss”
- Otydliga ansvarsförhållanden
- Brist på resurser och kompetens
- Otillräcklig dokumentation
- Svårigheter att kontrollera leverantörers säkerhet

Det viktiga är att börja strukturera arbetet – inte att ha allt på plats direkt.

6. Resurser och stöd

Officiella källor:

- MSB: msb.se/nis2
- PTS: pts.se
- ENISA: enisa.europa.eu

Ramverk att använda:

- ISO/IEC 27001
- NIST Cybersecurity Framework
- MSB:s metodstöd
- CIS Controls

När kan extern hjälp vara värdefull?

- Saknad kompetens eller tid
- Behov av oberoende granskning
- Behov av att möta kunders säkerhetskrav