

NIS2 – så påverkas du och ditt företag

Secured By **Telia Cygate**

Digitala tjänster och samhällskritisk infrastruktur är idag lika viktiga som el och vatten – och lika sårbara. Cyberattacker har blivit mer sofistikerade, leverantörskedjor mer komplexa och beroendet av digitala lösningar är större än någonsin.

Med NIS2 sätter EU en ny standard för digital säkerhet och robusthet. I Sverige blir det verklighet genom Cybersäkerhetslagen.

I den här guiden får du en tydlig bild av vad NIS2 innebär och hur du möter kraven på ett sätt som bygger dina kunders förtroende och stärker din position på marknaden.

“Det finns stora möjligheter för svenska företag i och med NIS2 – möjligheter som alldeles för sällan lyfts fram. De företag som förstår att det här är en chans att bli mer konkurrenskraftiga kommer vinna kundernas förtroende och positionera sig som långsiktigt pålitliga partners.

Att bygga ett säkert och kvalitetsmedvetet bolag är inte bara ett krav, det är en strategisk investering som gör dig robust och attraktiv för framtiden.”

Adam Önder, Strategisk Säkerhetsrådgivare, Telia Cygate

1. Vad är NIS2?

NIS2 är ett EU-direktiv som höjer kraven på cybersäkerhet i samhällsviktiga och affärskritiska verksamheter. Det innebär skarpare krav på hur organisationer arbetar med risker, incidenter och ansvar.

Syftet är enkelt: EU vill göra digital infrastruktur mer robust och motståndskraftig mot dagens och morgondagens hot.

2. Är NIS2 och cybersäkerhetslagen samma sak?

Nästan, men inte riktigt.

NIS2 är EU-direktivet som sätter ramarna för hur medlemsländer ska höja nivån på cybersäkerhet.

Cybersäkerhetslagen är den svenska lagen som gör NIS2 till verklighet här. Den avgör:

- vilka verksamheter som omfattas
- vilka krav som gäller
- vilka tillsynsmyndigheter som följer upp



3. Vem påverkas?

Många tror att lagen bara gäller stora bolag eller traditionell “kritisk infrastruktur”. Det stämmer inte. Du kan påverkas både direkt och indirekt.

Du påverkas ofta direkt om du:

- driver verksamhet inom energi, transport, hälso- och sjukvård, vatten, digital infrastruktur, IT-tjänster eller molntjänster
- levererar samhällskritiska eller affärskritiska digitala tjänster
- är ett medelstort eller stort företag inom sektorer som klassas som viktiga eller väsentliga

Du kan påverkas indirekt om du är leverantör eller konsult till en organisation som omfattas.

Så om du är ett IT-bolag som levererar drift, support eller utveckling till ett elbolag, kan du bli en del av deras säkerhetskrav. Om du är en målarfirma som arbetar åt ett kommunalt bostadsbolag, kan du behöva visa hur du hanterar kunddata, åtkomst till bokningssystem eller digitala nycklar.

I praktiken innebär det att även om du inte står under tillsyn själv, så kan du behöva visa att du är en pålitlig och säker leverantör.



4. Vad behöver jag göra?

Lagen handlar mindre om teknik och mer om faktiskt förmåga.

Du förväntas ha:

- en bild av dina risker och sårbarheter
- rutiner för hur du upptäcker och hanterar incidenter
- tydligt ansvar för säkerhet på ledningsnivå
- kontroll över leverantörer och beroenden
- förmåga att rapportera allvarliga incidenter

Enkelt sammanfattat behöver du visa att du förstår din risk, har tänkt igenom den, och att du arbetar systematiskt med att minska den.

5. Hur börjar jag?

Börja med att skapa överblick. Ställ dig dessa tre frågor:

- vad i vår verksamhet måste fungera?
- vilka system, leverantörer och personer är vi mest beroende av?
- vad händer om vi tappar tillgång, kontroll eller insyn i dem?



Redo att lära mer?

Om du vill ta nästa steg har vi tagit fram tre fördjupande guider:

Guide 1: Fem steg som ger kontroll över cybersäkerhetsarbetet, fallgropar i identitets- och behörighetshanteringen.

Här berättar vi om vanliga fallgropar i identitets- och behörighetshanteringen, och vad som krävs för att ta sig över dem och Fem steg för att komma i gång.

Guide 2: Fallgropar i identitets- och behörighetshanteringen

Här berättar vi om vanliga fallgropar i identitets- och behörighetshanteringen, och vad som krävs för att ta sig över dem

Guide 3: Fem steg för att komma i gång

Vi hjälper er att komma i gång med NIS2 på ett sätt som är både hanterbart och hållbart.

Telia och Telia Cygate – Unik kombination av erfarenhet och expertis

Vi kombinerar säkra nät med djup teknisk kompetens inom cybersäkerhet. Som en del av totalförsvaret har vi en unik position där vi både skyddar samhällskritisk infrastruktur och stärker företags digitala motståndskraft i vardagen. Genom att förena förståelse för teknik, människor och organisationer bidrar vi till ett säkrare och mer robust digitalt Sverige.

[Läs mer](#)