

STEP
LOCK

Når det må fungere.



NIS2

– Hva innebærer det for dere?

NIS2 – Hva innebærer det for dere?

NIS2 er EUs oppdaterte regulatoriske rammeverk for cybersikkerhet. Målet er å styrke beskyttelsen av kritiske og viktige aktiviteter gjennom tydeligere krav til sikkerhet, ansvar og hendelseshåndtering.

Reguleringene omfatter både private selskaper og offentlige organisasjoner innen områder som energi, bank, helsevesen, transport, digital infrastruktur og offentlig sektor.

Målet er å beskytte bedrifter og lokalsamfunn mot cybertrusler ved å sikre god risikostyring, hendelsesberedskap og sikker utvikling.

Hva krever NIS2?

1. Ledelsesansvar

Styret og ledelsen har ansvar for å sikre at cybersikkerheten er tilstrekkelig og systematisk håndtert.

2. Risikostyring

Organisasjoner må arbeide på en strukturert måte for å identifisere, vurdere og redusere cyber-risiko.

3. Leverandørkontroll

Det er ikke nok at din egen virksomhet er sikker, selv leverandører må oppfylle sikkerhetskravene.

4. Hendelsesrapportering

Alvorlige cyberhendelser må oppdages, håndteres og rapporteres innenfor satte tidsrammer.

Gjelder det dere?

Mange selskaper og foreninger er ikke direkte dekket av NIS2. Du kan imidlertid bli berørt hvis:

- du har leietakere eller kunder i NIS2-sektorene
- du leverer tjenester til samfunnsviktige virksomheter
- du administrerer digital infrastruktur eller tilkoblede systemer

Hvis en aktør du jobber med er dekket av NIS2, må aktøren sikre at leverandørene deres, inkludert eiendomseiere og teknologileverandører, ikke utgjør en sikkerhetsrisiko.

For eksempel, for at du som forening eller eiendomseier skal være dekket, kan det være nok å leie ut taket til en operatør som kan plassere en telekommunikasjonsmast, eller å gi plass i kjelleren slik at en internettoperatør kan installere et tilkoblingspunkt for områdets bredbånd.

Hva betyr dette i praksis?

- Dokumentert IT- og informasjonssikkerhet.
- Sikker administrasjon av digitale systemer og nettverk.
- Sporbarhet og loggføring.
- Klare prosedyrer for hendelser.
- Kontroll over lokale IT-systemer, skytjenester og underleverandører.

StepLocks engasjement

StepLock-gruppen jobber aktivt for å møte og overgå kravene satt av NIS2.

Vi har etablert prosesser og tekniske løsninger for å sikre et høyt nivå av cybersikkerhet, både i våre interne operasjoner og i tjenestene vi leverer til kundene våre.

Områder hvor StepLocks produkter hjelper deg i NIS2-arbeidet ditt

OMRÅDET	STEPLOCKS ARBEID
Informasjons-sikkerhet	Alle våre produkter bruker kryptert kommunikasjon. All skykommunikasjon er end-to-end-kryptert.
Standarder	Vi bruker åpne og etablerte kommunikasjonsstandarder. Det muliggjør uavhengig revisjon og verifisering av sikkerhet og kryptering, i motsetning til løsninger basert på proprietære protokoller og proprietær kryptering hvor synligheten er begrenset.
Sterk autentisering	I motsetning til lokale systemer som vanligvis kun bruker brukernavn og passord, tilbyr vår skyplattform sikre innloggingsalternativer som BankID, Pass Keys, tofaktor-tokens eller maskin-varetokens som Qubico.
Sporbarhet	Våre systemer hjelper deg å holde oversikt over hvem som har tilgang til eiendommen din.
Skandinavisk hosting	hosting Våre servere ligger i Sverige og Norge, i serverhaller som møter høye krav til både sikker drift og fysisk sikkerhet. <i>Vennligst les vårt datablad for vår hosting.</i>
Alle våre produkter produseres i Sverige.	
Alle våre produkter er utviklet i Sverige.	

Fordeler for deg som kunde

- ▶ Du får en partner som aktivt arbeider i samsvar med gjeldende EU-direktiver.
- ▶ Våre produkter og tjenester er bygget med sikkerhet som et grunnleggende prinsipp.
- ▶ Du styrker din egen etterlevelse av regelverket ved å velge en leverandør som tar ansvar.

STEP
LOCK

StepLock Norway A/S Øvre Storgate 86, 3018 Drammen, Norway
+47 23 00 30 00 | www.steplock.no | post@steplock.no