STEP LOCK

Når det skal fungere.

NIS2

– Hvad betyder det for jer?

NIS2 – Hvad betyder det for jer?

NIS2 er EU's opdaterede regelsæt for cybersikkerhed. Formålet er at styrke beskyttelsen af samfundskritiske og vigtige aktiviteter gennem tydeligere krav til sikkerhed, ansvar og håndtering af hændelser.

Regelsættet omfatter både private virksomheder og offentlige organisationer inden for eksempelvis energi, bank, sundhed, transport, digital infrastruktur og den offentlige sektor.

Formålet er at beskytte virksomheder og samfund mod cybertrusler ved at sikre god risikostyring, beredskab ved hændelser og sikker udvikling.

Hvad stiller NIS2 krav om?

1. **Ledelsesansvar**
   Bestyrelse og ledelse har ansvar for, at cybersikkerheden er tilstrækkelig og håndteres systematisk.
2. **Risikostyring**
   Organisationer skal arbejde struktureret med at identificere, vurdere og reducere cyberrisici.
3. **Leverandørkontrol**
   Det er ikke nok, at ens egen virksomhed er sikker – leverandører skal også opfylde sikkerhedskrav.
4. **Incidentrapportering**
   Alvorlige cyberhændelser skal opdages, håndteres og rapporteres inden for fastsatte tidsrammer.

Gælder det jer?

Mange virksomheder og foreninger er ikke direkte omfattet af NIS2. I kan dog blive påvirket, hvis:

- I har lejere eller kunder inden for NIS2-sektorer
- I leverer tjenester til samfundskritiske aktiviteter
- I håndterer digital infrastruktur eller opkoblede systemer

Hvis en aktør, I samarbejder med, er omfattet af NIS2, skal aktøren sikre, at deres leverandører – herunder ejendomsejere og teknologileverandører – ikke udgør en sikkerhedsrisiko.

For at I som forening eller ejendomsejer kan blive omfattet, kan det for eksempel være nok, at I udlejer taget til en operatør, der placerer en telemast, eller stiller plads i kælderen til rådighed, så en internetoperatør kan installere et knudepunkt til områdets bredbånd.

Hvad betyder det i praksis?

- Dokumenteret IT- og informationssikkerhed.
- Sikker håndtering af digitale systemer og netværk.
- Sporbarhed og logning.
- Tydelige procedurer for håndtering af hændelser.
- Kontrol over lokale IT-systemer, cloudtjenester og underleverandører.

StepLocks forpligtelse

StepLock-koncernen arbejder aktivt for at opfylde og overholde de krav, som NIS2 stiller.

Vi har etablerede processer og tekniske løsninger for at sikre et højt niveau af cyber-sikkerhed, både i vores interne drift og i de tjenester, vi leverer til vores kunder.

Områder hvor StepLocks produkter hjælper dig i NIS2-arbejdet

OMRÅDE	STEPLOCKS ARBEJDE
Informationssikkerhed	Alle vores produkter anvender krypteret kommunikation. Al cloud-kommunikation er end-to-end-krypteret.
Standarder	Vi anvender åbne og etablerede kommunikationsstandarder. Det gør det muligt uafhængigt at gennemgå og verificere sikkerhed og kryptering, i modsætning til løsninger der bygger på proprietære protokoller og egenudviklet kryptering, hvor indsigt er begrænset.
Stærk autentificering	I modsætning til lokale systemer, som oftest kun anvender brugernavn og adgangskode, tilbyder vores cloud-platform sikre loginmuligheder som BankID, passkeys, tofaktor-godkendelse eller hardwaretokens som Qubico.
Sporbarhed	Vores systemer hjælper dig med at have kontrol over, hvem der har adgang til din ejendom.
Svensk hosting	Vores servere er placeret i Sverige i serverhaller, der opfylder høje krav til både driftssikkerhed og fysisk sikkerhed. *Læs gerne vores datablad om vores hosting.*
Svensk produktion	Alle vores produkter produceres i Sverige.
Svensk utveckling	Alle vores produkter udvikles i Sverige.

Fordele for dig som kunde

- Du får en partner, der aktivt arbejder i overensstemmelse med gældende EU-direktiver.
- Vores produkter og tjenester er udviklet med sikkerhed som grundlæggende princip.
- Du styrker din egen overholdelse af regler ved at vælge en leverandør, der tager ansvar.

StepLock Denmark A/S | Fælledvej 17, 7600 Struer, Danmark
+45 53 777 808 | www.steplock.dk | support@steplockaccess.dk