Slik bruker du sjekklisten

• Gå gjennom punktene sammen med IT-ansvarlig og ledelse
• Marker hva som allerede er på plass, og hva som må planlegges
• Bruk resultatet som grunnlag for videre prioritering og budsjett

1. Grunnleggende oversikt

■ Vi har en oppdatert oversikt over alle kritiske systemer og applikasjoner
■ Vi vet hvor de viktigste dataene våre faktisk ligger (lokalt, datasenter, sky)
■ Vi har identifisert hvilke systemer som er mest kritiske for daglig drift

2. Tilgang og identitet

■ Alle brukere har personlige kontoer (ingen delte «fellesbrukere» der det ka
■ Vi bruker multifaktor-autentisering (MFA) på e-post og andre sentrale tjene
■ Tilganger fjernes rutinemessig når ansatte slutter eller bytter rolle

3. Teknisk grunnmur

- ■ Vi har en oppdatert brannmur-/nettverksløsning med tydelige regler
- ■ Viktige tjenester er segmentert (ikke «alt i samme nett»)
- ■ Vi har rutiner for oppdatering/patching av servere, klienter og nettverksutstyr
- ■ Antivirus/EDR er på plass og overvåkes

4. Backup og gjenoppretting

- ■ Vi har minst én sikkerhetskopi som er logisk eller fysisk adskilt fra primær
- ■ Backup kjøres automatisk og overvåkes
- ■ Vi har testet gjenoppretting de siste 12 månedene

5. Hendelseshåndtering

- ■ Vi vet hvem som skal kontaktes først ved et sikkerhetsbrudd
- ■ Vi har en enkel plan for hvordan vi håndterer alvorlige hendelser
- ■ Vi vet hvilke systemer og logger vi må kunne hente ut ved en hendelse

6. Leverandører og tredjeparter

- ■ Vi vet hvilke leverandører som har tilgang til våre systemer og data
- ■ Avtaler med leverandører inkluderer minimumskrav til sikkerhet
- ■ Vi har kontroll på hvem som kan logge seg inn eksternt (VPN, fjernadminis

Hva gjør vi med funnene?

Denne sjekklisten er ikke en revisjonsrapport, men et verktøy for å få oversikt. • Marker områder dere er trygge på. • Marker områder dere er usikre på eller mangler helt. • Prioriter 3–5 konkrete tiltak for de neste 6 månedene. For mange SMB-er vil det være naturlig å starte med: • Nettverk og tilgangsstyring (VPN, brannmur, segmentering) • Backup og gjenoppretting • Logging og grunnleggende hendelseshåndtering NIS2 handler i stor grad om å kunne vise at dere jobber systematisk med disse områdene – ikke at alt er perfekt fra dag én.

Vil dere ha hjelp til å komme videre?

SignalNord hjelper SMB-bedrifter med praktiske grep innen nettverk,

tilgangsstyring, logging og overvåking – med utgangspunkt i NIS2-kravene.

Les mer på signalnord.no eller ta kontakt på post@signalnord.no.