

Checklista cybersäkerhetslagen

Det här behöver din organisation tänka på:

1.

Se över om ni omfattas

Cybersäkerhetslagen gäller verksamheter inom bland annat energi, transport, hälso- och sjukvård, offentlig förvaltning, finanssektorn samt leverantörer av digital infrastruktur och molntjänster. Börja med att se över om er verksamhet omfattas av den nya lagen och utvärdera vilka krav det ställer på er verksamhet.

2.

Rapportera och anmäl i tid

Organisationer som omfattas av lagen ska vara registrerade hos rätt tillsynsmyndighet. Säkerställ att ansvarsfördelning och rutiner för rapportering och anmälan är tydliga och fungerar i praktiken.

3.

Förankra ansvaret i ledningen

Cybersäkerhet är inte längre en fråga för IT-avdelningen – det är ett ledningsansvar. Styrelse och företagsledning behöver förstå sitt juridiska ansvar enligt lagen och säkerställa att efterlevnadsarbetet är en integrerad del av den övergripande verksamhetsstyrningen.

4.

Gör en riskanalys

Identifiera vilka system, leverantörer och processer som är mest kritiska för verksamheten. En systematisk riskanalys är grunden för att kunna prioritera rätt skyddsåtgärder. Tänk både tekniskt och organisatoriskt: var finns störst sårbarheter, och hur påverkar de er verksamhetsförmåga?

5.

Etablera tydliga rutiner

Lagen kräver att organisationer kan rapportera incidenter snabbt och transparent. Se till att ha processer för incidentrapportering, informationsdelning och intern kommunikation på plats. Rutinbeskrivningarna ska vara kända och testade, inte bara dokumenterade.

6.

Säkerställ tekniska skydd

Granska era befintliga lösningar för kommunikation, övervakning och backup. Finns redundans och kryptering där det behövs? Säkerställ att både IT- och OT-system omfattas, och att ni har kontroll över hela leveranskedjan.

7.

Höj kompetensen

Utbildning är en central del av lagen. Alla medarbetare, från ledning till driftpersonal, behöver förstå hur deras arbete påverkar cybersäkerheten. Planera för återkommande utbildning, övningar och uppföljning.

8.

Dokumentera och följ upp

Allt arbete med cybersäkerhet ska kunna visas upp för tillsynsmyndigheten. Dokumentera riskbedömningar, beslut och åtgärder. Regelbunden uppföljning gör att ni kan visa på systematik och kontinuerlig förbättring.

9.

Genomför oberoende granskning

Allt arbete med cybersäkerhet ska kunna visas upp för tillsynsmyndigheten. Dokumentera riskbedömningar, beslut och åtgärder. Regelbunden uppföljning gör att ni kan visa på systematik och kontinuerlig förbättring.

10.

Bygg långsiktig motståndskraft

Cybersäkerhetslagen handlar inte bara om att uppfylla krav, den handlar om att bygga säkra, motståndskraftiga, robusta system som tål störningar. Organisationer som investerar i säkerhet nu står starkare när krisen kommer.