Cybersäkerhetslagen kräver att säkerhetsåtgärder följs upp. Vilket underlag har ni för det tekniska läget?

Cybersäkerhetslagen, som genomför NIS2-direktivet i Sverige, gäller sedan den 15 januari 2026. Den kräver att verksamhetsutövare vidtar lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska säkerhetsåtgärder (2 kap. 3 §). Säkerhetsåtgärderna ska åtminstone avse bland annat strategier och förfaranden för att bedöma åtgärdernas effektivitet (2 kap. 3 § p. 6).

Cybersäkerhetslagen (2025:1506) och MCFFS 2026:11 Oktober 2026 5 min läsning

Den 1 oktober 2026 trädde MCF:s föreskrifter och allmänna råd om säkerhetsåtgärder och ledningens utbildning, MCFFS 2026:11, i kraft. De gör kravet på uppföljning konkret. Frågan för den tekniska delen av säkerhetsarbetet är: vilket underlag har ni för att följa upp det faktiska läget?

01 / Vad föreskrifterna säger om uppföljning

För att kunna bedöma effektiviteten ska verksamhetsutövaren följa upp och utvärdera om säkerhetsåtgärderna är lämpliga och proportionella. För sektorskritiska system ska det ske vid behov, men minst en gång per år.

Verksamhetsutövaren bör använda etablerade metoder som granskning, mätning och tester.

Ledningen ska godkänna och övervaka genomförandet av säkerhetsåtgärderna. Den ska bland annat säkerställa att den blir informerad om genomförandet och om nivån av cybersäkerhet, vid behov men minst en gång per år.

Samordnaren ska säkerställa att de underlag som ledningen behöver sammanställs.

Verksamhetsutövaren ska identifiera behovet av att spara information för uppföljning, utvärdering och tillsyn.

Allmänna råd är inte tvingande. De visar hur MCF tänker sig att kraven kan uppfyllas.

02 / Infört är inte samma sak som verifierat

En säkerhetsåtgärd kan vara beslutad och införd utan att omfatta alla användare, enheter eller system som den är avsedd att skydda. Det kan finnas undantag, bristande konfigurationer eller system som inte rapporterar aktuella uppgifter.

Genom att undersöka data från organisationens befintliga säkerhetssystem går det i många fall att kontrollera hur åtgärderna faktiskt har införts och hur stor del av IT-miljön de omfattar.

Det ger ett bättre underlag för uppföljning än att enbart utgå från beslut, policyer och systeminställningar.

Föreskrifterna pekar åt samma håll. I 4 kap. 13 § rekommenderas tekniskt systemstöd för att följa upp att systemen är korrekt konfigurerade, och 4 kap. 27 § kräver säkerhetstester för att kontrollera att systemen är uppdaterade, att publicerade sårbarheter är omhändertagna och att valda konfigurationer har införts.

03 / Förändring måste gå att följa över tid

För att veta om säkerheten faktiskt förbättras räcker det inte att jämföra två rapporter. Det måste också vara tydligt vad som har kontrollerats, vilka system och användare som ingår och hur resultaten har tagits fram.

Annars kan en förändring i siffrorna bero på att underlaget har ändrats, snarare än att säkerheten blivit bättre eller sämre.

Ledningen behöver inte alla tekniska detaljer, men ska kunna lita på att jämförelsen är rättvisande.

04 / Teknisk evidens är en del av underlaget, inte hela

Cybersäkerhetslagen omfattar betydligt mer än det som går att observera tekniskt. Riskanalys, ansvar, interna regler, leverantörsstyrning, incidenthantering och utbildning kräver andra typer av underlag. En teknisk mätning visar därför inte i sig om en organisation uppfyller lagen, och den ersätter inte uppföljningen av de organisatoriska delarna.

Den kan däremot ge ett spårbart underlag för de säkerhetsåtgärder där det faktiska tekniska tillståndet går att verifiera, till exempel åtkomstkontroll och MFA, kryptering, äldre inloggningsmetoder, loggning och klientskydd. Det gör uppföljningen mer konkret och minskar beroendet av manuella sammanställningar och antaganden.

05 / Från uppföljning till mätbart underlag

Iviron använder information från organisationens befintliga säkerhetssystem för att visa hur det tekniska säkerhetsläget faktiskt ser ut vid en bestämd tidpunkt.

Resultatet sparas och kan jämföras med senare mätningar. IT får ett konkret underlag för att identifiera och åtgärda brister, medan ledningen kan följa utvecklingen utifrån samma fakta.

Iviron förändrar ingenting i kundens system. Åtgärderna genomförs som tidigare i de verktyg organisationen redan använder.

Principen Mät. Åtgärda. Verifiera.

Mätningen omfattar den del av säkerhetsarbetet som går att kontrollera tekniskt. Den ersätter inte riskanalyser, organisatorisk uppföljning eller bedömningar av om verksamheten uppfyller lagen.

Verifierat betyder här att mätresultatet är reproducerbart och spårbart till definierad källa, population, omfattning och mätprincip. Det är inte en revision eller certifiering.

Källor och vidare läsning

Cybersäkerhetslag (2025:1506), 2 kap. 3 och 4 §§ www.riksdagen.se

Cybersäkerhetsförordning (2025:1507) www.riksdagen.se

MCFFS 2026:11, föreskrifter och allmänna råd om säkerhetsåtgärder och ledningens utbildning för väsentliga och viktiga verksamhetsutövare www.mcf.se

NIS2-direktivet, (EU) 2022/2555, artikel 21 eur-lex.europa.eu