Säkerhet
Sofia Gustafsson

PM - Uppföljning cybersäkerhetslagen
Regionens informationssäkerhetsstrateg samordnar arbetet med att säkerställa att Region Västerbotten följer den nya cybersäkerhetslagen som trädde i kraft den 15 januari 2026. Arbetet sker tillsammans med ICI-gruppen (informations-, cyber- och IT-säkerhet). Myndigheten för civilt försvar ansvarar för att ta fram de föreskrifter som kompletterar lagstiftningen. Den första föreskriften, som rör anmälningsskyldighet, trädde i kraft i februari. Däremot har två planerade föreskrifter blivit försenade:

- föreskriften om säkerhetsåtgärder och utbildning
- föreskriften om incidentrapportering och informationsskyldighet

Enligt tidigare kommunikation skulle dessa börja gälla i början av april. Nu meddelar Myndigheten för civilt försvar att föreskriften om incidentrapportering och informationsskyldighet skjuts fram till maj, och föreskriften om säkerhetsåtgärder och utbildning till efter sommaren. Förseningen beror på de omfattande synpunkter som inkom under remissprocessen. Mycket feedback rörde ”ledningens ansvar”, särskilt från kommuner och regioner som har både politisk styrning och tjänstemannaledning. Myndigheten för civilt försvar konstaterar därför att man behöver ta ett omtag för att hitta en väl avvägd och tydlig beskrivning av ledningsansvaret i kommande föreskrifter.

De försenade föreskrifterna innebär att det i nuläget är utmanande att fullt ut efterleva den nya cybersäkerhetslagen. Eftersom vägledningen kring både säkerhetsåtgärder, utbildning samt incidentrapportering och informationsskyldighet ännu inte är fastställd, saknas tydliga riktlinjer för hur vi som verksamhet konkret ska agera för att säkerställa laguppfyllelse.

Det första kravet att uppfylla är att verksamhetsutövare enligt cybersäkerhetslagen ska anmäla sin verksamhet enligt NIS2-direktivet. Region Västerbotten lämnade in sin anmälan till Myndigheten för civilt försvar den 4 februari.

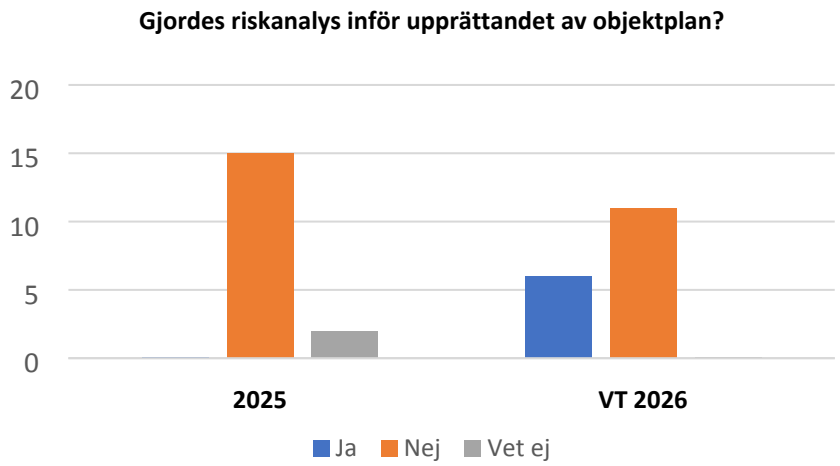
Säkerhetsåtgärder
Sedan tidigare har regionen arbetat med en årlig riskanalys och tillhörande säkerhetsåtgärder på övergripande nivå för regionens cyber-, IT- och informationssäkerhet. Detta arbete kommer att fortgå i enlighet med den nya lagstiftningen, men säkerhetsåtgärderna måste övervakas med ökad frekvens. Föreskrifterna föreslår att uppföljning bör genomföras kvartalsvis. Sedan tidigare har en CIS-analys (*Critical Security Controls* för cybersäkerhet) genomförts. Riskanalysen och CIS-analysen har identifierat flera säkerhetsåtgärder. Under februari 2026 organiserades en workshop-serie i syfte att samordna och informera berörda parter om dessa åtgärder. ICI-gruppen har även tagit fram riktlinjer och rutiner för säkerhetsåtgärder enligt standard från ISO27000-serien, vilka också ligger till grund för cybersäkerhetslagen. Dessa kommer att harmoniseras med föreskrifter för säkerhetsåtgärder när de slås fast av Myndigheten för civilt försvar.

Cybersäkerhetslagen och objekten
Regionens objektstruktur har identifierats som nyckelfunktioner för lyckad lagefterlevnad av den nya cybersäkerhetslagen. Under hösten 2025 har ett 15-tal informations- och utbildningsinsatser, både muntliga och skriftliga, riktats till objektet och då framför allt objektledare och objektledare teknik. Insatserna har handlat om den nya cybersäkerhetslagen, omvärldsläget, utbildning i utförande av riskanalys

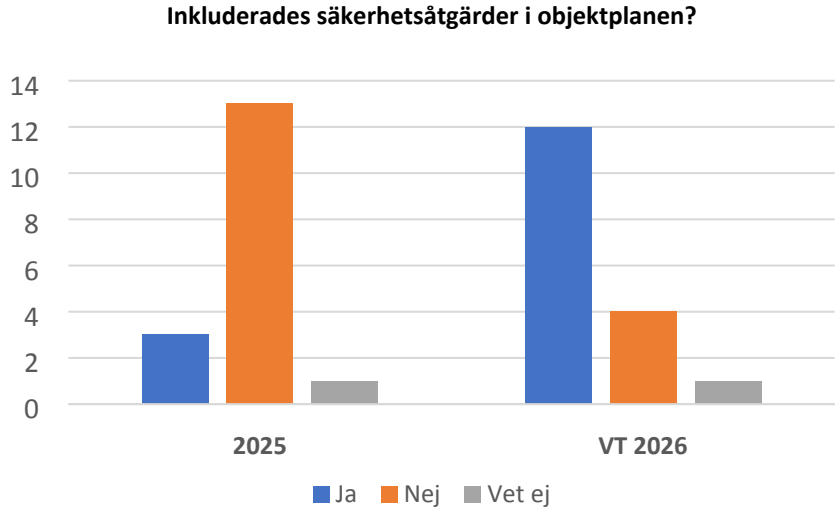
Säkerhet
Sofia Gustafsson

samt säkerhetsåtgärder. Även en obligatorisk effekt infördes i objektplanen för alla objekt att följa; ”*Efter genomförd riskanalys ska objektet under 2026 öka sin motståndskraft genom att införa minst X säkerhetsåtgärder enligt Nationellt cybersäkerhetscenters rekommendationer.”*

Uppföljning har genomförts via personliga intervjuer med samtliga objekt. Objekten arbetar i olika grad aktivt med informations- och cybersäkerhet, men detta är inte alltid formellt dokumenterat i objektplaner eller utfört enligt etablerad metodik. Tyngdpunkten ligger på konkreta säkerhetsåtgärder snarare än formell dokumentation. Säkerhetsarbetet omfattar flera olika åtgärder, vilka sällan återfinns i objektplanerna, utan ibland hanteras genom alternativa processer. Riskmedvetenheten är hög, men det systematiska arbetet och riskanalysens utformning varierar mellan objekten.

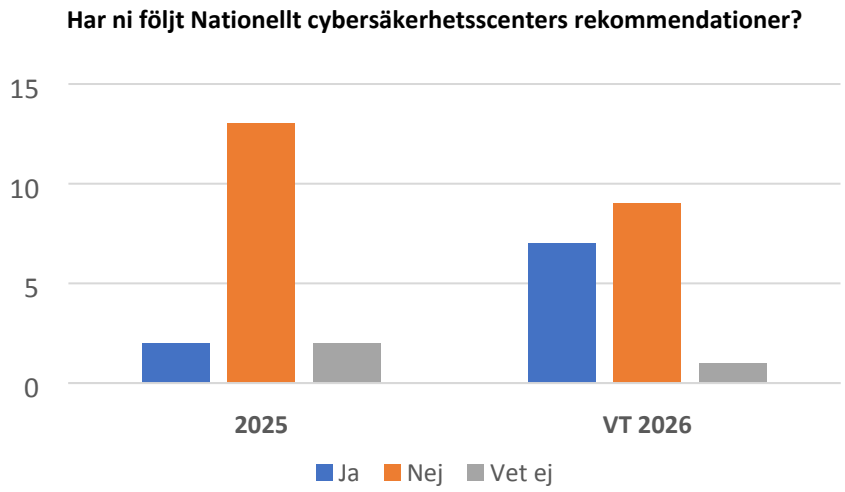


Tabell 1 Tabellen visar att inget objekt genomfört riskanalys inför 2025 års objektplan och att drygt 5 av objekten gjorde det inför årets objektplan.



Tabell 2 Tabellen visar att endast enstaka objekt inkluderade säkerhetsåtgärder inför 2025 års objektplan. Inför årets objektplan hade betydligt fler objekt inkluderat säkerhetsåtgärder.

Säkerhet
Sofia Gustafsson



Tabell 3 Tabellen visar att endast enstaka objekt följt Nationellt cybersäkerhetscenters rekommendationer inför 2025 års objektplan. Inför årets objektplan hade fler objekt uppgett att de följt rekommendationerna.

Utbildning
Cybersäkerhetslagen betonar både att ledningen ska genomgå utbildning om säkerhetsåtgärder samt att det ska finnas grundläggande praxis för cyberhygien och utbildning i cybersäkerhet. Föreskrifterna som preciserar riktning gällande säkerhetsåtgärder och utbildning är som tidigare nämnt försenade. Det är inplanerat en uppföljning och dragning om cybersäkerhetslagen den 14 april, en uppföljning den 13e maj samt ett utbildningstillfälle hösten 2026.

Utbildningen ”Säkerhetsmedvetenhet och säkert beteende” är sedan tidigare obligatorisk för samtliga medarbetare, och ICI-gruppen fortsätter att informera och säkerställa att denna utbildning når ut till alla berörda. Regionen genomför också mikro-utbildningar och simulerade phisingmejl genom tjänsteleverantören Nimblr där syftet är att höja medarbetarnas kunskaper om cybersäkerhet. Utifrån resultatet av utbildningarna och de simulerande inslagen planeras det att genomföras riktade utbildningsinsatser.

Incidenthantering
Den nya föreskriften för incidenthantering förväntas publiceras i april, med ikraftträdande i maj. En befintlig rutin enligt lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS1-incidenter) finns redan etablerad. ICI-gruppen arbetar för närvarande med att revidera denna rutin så att den harmoniserar med de nya föreskrifterna för anmälan av incidenter.

IT-säkerhet
Det arbetas även med tekniska lösningar för att göra våra miljöer mer säkra, där bland annat ThreatLocker har införts. ThreatLocker är ett cybersäkerhetsverktyg som skyddar regionens datorer och servrar genom att bara tillåta program och filer som uttryckligen godkänts. Det kan därmed stoppa ransomware, skadlig kod och obehörig åtkomst vilket minskar risker för attacker och dataintrång.

Det har också införts en pop-up-ruta vid användande av AI-tjänster i webläsaren. Rutan påminner användarna av vad de får använda AI-tjänster till samt hänvisar till riktlinjer gällande AI och digital informationshantering.

Det pågår arbete fler tekniska åtgärder. Bland annat ska det införas striktare lösenordsregler samt legitimering med bank-ID för att återställa sitt lösenord via servicedesk. Det arbetas även med att införa Microsoft AIP, som är ett verktyg för att klassificera, märka och skydda dokument och e-post inom regionen. AIP hjälper till att säkerställa att känslig information hanteras korrekt, både internt och extern.

Uppföljning styrande dokument inom Region Västerbotten
ICI-gruppen har påbörjat arbete med att se över samtliga styrande dokument kopplade till informationssäkerhet, IT-säkerhet och cybersäkerhet, med särskild hänsyn till den nya cybersäkerhetslagen. Som en del av detta arbete har en förteckning över alla dokument som berörs tagits fram. Ett första uppstartsmöte har hållits med dokumentansvariga där deltagarna informerades om den övergripande ambitionen att säkerställa att dokumenten är uppdaterade, ändamålsenliga och i linje med gällande lagstiftning. I nästa fas kommer dokumentansvariga att arbeta vidare med respektive dokument. Uppföljningsmöten planeras, där information om föreskrifterna ges när dessa har trätt i kraft.