Fem steg som ger kontroll över cybersäkerhetsarbetet

Cybersäkerhetslagen innebär tydligare krav på hur organisationer ska arbeta med cybersäkerhet. För många känns kraven både omfattande och svåra att översätta till praktiskt arbete i vardagen. Vad är egentligen viktigt att få på plats, och var börjar man? Den här guiden tar avstamp i de vanligaste utmaningarna och visar fem steg som ger bättre kontroll över cybersäkerhetsarbetet.

1. Red ut ansvarsfrågan

Utmaning:
Många organisationer arbetar med cybersäkerhet utan att det är helt tydligt vem som äger helheten. Frågorna hamnar ofta hos IT, och verksamheten utgår från att säkerheten därmed är omhändertagen. Men när ansvar, mandat och beslutsvägar inte hänger ihop blir säkerhetsarbetet fragmenterat, och glappet som uppstår ställer till stora problem i en situation som kräver snabba beslut.

Lösning:
Cybersäkerhetslagen förutsätter att ansvaret är tydligt förankrat i verksamheten. Ett första steg är därför att klargöra vem som äger systemen, vem som har mandat att fatta beslut, och vem som är ansvarig när något inträffar. När ansvar är tydligt blir det också möjligt att arbeta systematiskt och långsiktigt med säkerhet.

2. Få koll på nuläget

Utmaning:
En vanlig svårighet är att det är oklart var organisationen faktiskt står. Många vet att det finns brister, men upplever samtidigt att säkerhetsarbetet är komplext och svåröverskådligt. Resultatet blir att man famlar mellan olika åtgärder utan att ha en gemensam bild av nuläget.

Lösning:
I stället för att försöka lösa allt på en gång behöver man börja med att skapa en ärlig nulägesbild. Det handlar inte om att peka ut allt som saknas, utan om att förstå vilka tillgångar som är mest kritiska, vilka risker som är verkliga och vad som redan fungerar. En gemensam förståelse för nuläget gör det möjligt att prioritera rätt.

3. Gör det som är mest viktigt

Utmaning:
När hotbilden upplevs som omfattande och ständigt föränderlig är det lätt att allt känns lika viktigt. Det kan skapa en känsla av att stå handlingsförlamad inför vad som faktiskt behöver göras. Det leder ofta till reaktiva beslut, där åtgärder vidtas utan tydlig koppling till verksamhetens faktiska risker och behov.

Lösning:
Cybersäkerhetslagen bygger på ett riskbaserat synsätt. Det innebär att åtgärder ska vara proportionerliga och motiverade utifrån verksamhetens förutsättningar. Genom att arbeta riskbaserat går det att fokusera resurser där de gör störst nytta, i stället för att försöka göra allt samtidigt.

4. Från punktinsatser till förmåga

Utmaning:
Säkerhetsarbete drivs ofta i form av projekt eller punktinsatser. Nya verktyg införs, rutiner tas fram och initiativ genomförs, men efter ett tag tappar arbetet fart och struktur. Säkerhet blir något som görs ibland, snarare än något som är en del av vardagen.

Lösning:
Lagen förutsätter ett kontinuerligt arbetssätt. I stället för att tänka i projekt behöver säkerhet ses som en förmåga som byggs över tid. Det innebär att arbetet följs upp, justeras och utvecklas i takt med att verksamheten förändras. Förmåga slår punktinsats – varje gång.

5. Börja där du är

Utmaning:
Många upplever att kraven i cybersäkerhetslagen är stora och svåra att ta sig an. Ambitionen finns, men omfattningen kan skapa stress och passivitet. När allt känns överväldigande är risken att man inte kommer i gång alls.

Lösning:
Cybersäkerhetslagen kräver inte perfektion, men den kräver riktning och framdrift. Det viktigaste steget är ofta att börja där man står i dag. Med rätt struktur går det att bygga säkerhetsarbetet steg för steg, utan att skapa onödig belastning i organisationen.

Läs mer