LEDNING · STYRNING · CYBERSÄKERHETSLAGEN

Ledningsrapport för cybersäkerhet

En ledningsrapport blir inte stark för att den är kort. Den blir stark när den går att fatta rimliga beslut på. Det kräver att rapporten visar ett fastställt läge, var risk har reducerats sedan sist och vad som fortfarande kräver uppföljning. Utan den strukturen blir rapporten antingen för teknisk för ledningen eller för tunn för att vara användbar.

- Vad ledningen faktiskt behöver se för att fatta rimliga beslut
- Varför jämförbarhet över tid är kärnan
- Vad rapporten måste vila på för att inte bli frikopplad

I KORTHET

Vanligt misstag

Teknisk data kortas ned men är fortfarande byggd för drift, inte för styrning och uppföljning.

Det ledningen behöver

Ett tydligt nuläge, en begriplig riskreducering över tid och ett format som går att återvända till.

Det rapporten måste vila på

Ett tekniskt underlag med samma logik vid varje mätning, annars blir jämförelsen skakig.

En ledningsrapport får inte vara en nedkortad teknisk dump

Många organisationer har säkerhetsdata, driftdata och punktvisa underlag, men saknar fortfarande en rapport som fungerar för uppföljning på ledningsnivå. Informationen finns, men den är byggd för andra syften: drift, incidenthantering, förvaltning eller teknisk felsökning.

När den ska lyftas uppåt blir den ofta antingen för tunn eller för teknisk. Båda varianterna gör rapporten svag som styrunderlag.

Vad ledningen faktiskt behöver se

Ledningen behöver i grunden inte veta allt. Den behöver veta tillräckligt mycket för att kunna följa utvecklingen och fatta rimliga beslut.

- Hur ser läget ut just nu?
- Vad har förändrats sedan föregående mätning?
- Var är riskerna eller bristerna tydligast?
- Vad behöver prioriteras nu?

> **Det viktiga är inte att rapporten försöker säga allt.** Det viktiga är att den gör läget uppföljningsbart och möjligt att återkomma till.

FÖR LEDNING

Det ledningen faktiskt ser

- Hur säkerhetsläget ser ut just nu
- Var risk har reducerats sedan förra mätningen
- Vad som fortfarande kräver uppföljning
- Var prioritering eller beslut behövs

FÖR IT

Det IT faktiskt slipper

- Bygga en ny sammanställning varje gång frågan kommer
- Översätta rådata under tidspress
- Försvara en engångsbild utan historik
- Bära hela lägesbilden muntligt

Varför rapporteringen ofta tappar kraft i praktiken

I många organisationer uppstår ledningsrapporteringen först när någon frågar efter den. Då börjar arbetet med att samla ihop material från flera håll. Någon tar fram en punktlista. Någon annan gör en snabb sammanställning. IT fyller i mellanrummen muntligt.

Det kan fungera en gång. Det fungerar sämre som återkommande modell.

Vad en ledningsrapport måste innehålla för att hålla

En bra ledningsrapport för cybersäkerhet behöver inte vara lång. Men den behöver vara tydlig och byggd på samma struktur varje gång.

- Ett fastställt nuläge
- En tydlig jämförelse med föregående mätning
- Ett fåtal områden som går att följa över tid
- En kort kommentar om var risk har reducerats, försämrats eller står still
- Ett underlag för prioritering, inte bara beskrivning

Varför jämförbarhet över tid är kärnan

Den största skillnaden mellan en engångsrapport och en fungerande ledningsrapport är jämförbarheten. Om varje rapport ser olika ut, bygger på olika data eller använder olika logik blir det svårt att veta vad som faktiskt har förändrats.

Det är därför ledningsrapporten måste vila på återkommande mätningar i samma form.

Varför rapporten måste stå på en fast teknisk grund

En ledningsrapport får inte bli frikopplad från verkligheten i IT-miljön. Då blir den lätt för generell, för trygg i tonen eller för beroende av formuleringar i stället för faktiska förändringar.

När grunden är fast går det däremot att hålla rapporten kort och tydlig utan att den blir tunn.

Vilken roll rapporten ska spela i organisationen

En bra ledningsrapport ska göra tre saker samtidigt. Den ska ge ledningen en begriplig bild av läget. Den ska ge IT en rimlig väg att rapportera uppåt utan att börja om varje gång. Och den ska ge organisationen ett bättre underlag när frågor kommer från revision eller tillsyn.

Var Statira kommer in

Statira är byggt för att fastställa ett tekniskt nuläge, göra riskreducering över tid synlig och ge organisationen ett underlag som både IT och ledning kan använda. Det gör ledningsrapporten mindre beroende av manuella sammanställningar och betydligt mer användbar som återkommande uppföljningspunkt.