TILLSYN · NIS2 · REVISION · KOMMUNER

Tillsyn utan uppsamlingsprojekt

Det som gör tillsyn tung är sällan själva kontakten med myndigheten. Tyngden uppstår när lägesbilden måste byggas i efterhand. Då förvandlas vardagens säkerhetsarbete till ett separat spår med exportuttag, kompletteringar och muntliga förklaringar under tidspress. När underlaget redan finns på plats blir tillsyn i stället en fråga om att visa hur läget såg ut, var risk har reducerats och vilka åtgärder som faktiskt har genomförts.

- Varför tillsyn utan underlag alltid blir ett akutprojekt
- Vad ett hållbart tillsynsunderlag faktiskt måste visa
- Tre principer som minskar uppsamlingslogiken

I KORTHET

Det vanliga mönstret

Frågan kommer utifrån och triggar ett internt arbete för att pussla ihop underlag i efterhand.

Det som saknas

Ett återkommande underlag som redan finns, går att återvända till och kan bäras av både IT och ledning.

Det som förändras

Svarstiden blir kortare, historiken tydligare och den interna friktionen betydligt mindre.

När frågan kommer utifrån måste lägesbilden redan vara gjord

Cybersäkerhetslagen har flyttat tillsynsfrågan närmare verksamheten. För vissa organisationer kan tillsyn ske proaktivt, inte bara efter incidenter eller misstankar om brister. Det betyder att frågan om underlag blir praktisk tidigare än många hade hoppats på.

När myndigheten hör av sig behöver organisationen kunna visa mer än ambition. Den behöver visa hur säkerhetsläget ser ut, hur det har förändrats och hur arbetet följs upp över tid.

> **Viktigt:** Det som saknas i stunden går sällan att skapa snabbt utan kostnad. En tillsynsförfrågan testar därför ofta inte bara säkerhetsnivån, utan också hur väl organisationen har byggt sin egen uppföljning.

Hur det brukar se ut i verkligheten

För många verksamheter ser mönstret ungefär likadant ut varje gång någon extern part vill se underlag. Först kommer förfrågan. Sedan börjar det interna projektet.

1

INITIERING

Myndigheten begär underlag

Frågan gäller ofta nuläge, uppföljning, ansvar och vilka åtgärder som har vidtagits.

2

INSAMLING

IT börjar samla ihop bilden

Utdrag, gamla rapporter, konsultmaterial och muntliga förklaringar måste fogas samman under tidspress.

3

GRANSKNING

Underlaget skickas in och kompletteras

När frågor kommer tillbaka behöver organisationen ofta gräva vidare eftersom underlaget inte från början var byggt för att hålla.

4

EFTERSPEL

Allt börjar lätt om nästa gång

När historiken inte är fastställd mellan mätningar finns ingen tydlig bas att återvända till.

Varför tillsyn så ofta blir en specialinsats

Tillsyn blir ett akutprojekt när underlaget i vardagen består av delar: ett exportuttag här, ett gammalt beslutsunderlag där, en konsultgenomgång från förra året och muntliga beskrivningar av vad som förändrats sedan dess.

Det är ofta tillräckligt för intern orientering. Det är betydligt sämre när någon utifrån vill se hur arbetet faktiskt har följts upp över tid. arbetet faktiskt bedrivs och hur effekten följs upp över tid.

Vad ett hållbart tillsynsunderlag faktiskt måste visa

För att tillsyn inte ska dra i gång ett nytt projekt behöver det redan finnas ett underlag som besvarar det viktigaste.

- **Teknisk status**. patch, sårbarheter, EOL, endpoint-skydd, diskkryptering, AD-hygien och extern exponering
- **Förändring över tid**. var risk har reducerats, vad som kvarstår och vad som står still
- **Kommentar och kontext**. vilka åtgärder som genomförts och varför vissa luckor fortfarande finns kvar
- **Ledningsbar form**. ett underlag som går att bära upp till ledning utan att förlora verklighetskontakten

Tre arbetssätt som minskar uppsamlingslogiken

Jämförbarhet

Underlaget måste återkomma i samma form. Annars blir historiken osäker även om varje enskild rapport ser rimlig ut.

Separation

IT behöver ett tekniskt underlag. Ledningen behöver en rapport som går att följa. Samma mätning kan bära båda, men formatet behöver vara tydligt.

Lugn drift

Det ska inte krävas ett nytt dagligt arbetsflöde för att kunna visa nuläge och förändring. Mätning, underlag och uppföljning ska hjälpa IT. inte skapa mer brus.

Slutsats

Tillsyn blir tung när organisationen först vid förfrågan måste försöka rekonstruera sitt säkerhetsläge. Den blir lättare när underlaget redan finns, är fastställt och går att återvända till mellan mätningar.