INCIDENTER · CYBERSÄKERHETSLAGEN · KOMMUNER

Incidentrapportering under tidspress

När en allvarlig incident redan pågår är det sällan brist på aktivitet som är problemet. Problemet är att någon snabbt måste kunna visa vad som var känt före incidenten, vad som verkar ha förändrats och hur stor påverkan kan vara. Utan ett fastställt tekniskt underlag blir incidentrapporteringen lätt ett separat uppsamlingsprojekt mitt i det operativa arbetet.

- Varför loggar och larm inte löser hela rapportfrågan
- Tre rapportsteg som ställer olika krav
- Vad ett hållbart incidentunderlag måste kunna visa

I KORTHET

Det som händer i praktiken

När incidenten eskalerar måste verksamheten snabbt kunna beskriva läge, omfattning och vad som fortfarande är osäkert.

Det som ofta saknas

Senaste verifierade normalläge och en teknisk jämförelse som går att stå för under tidspress.

Det som gör skillnad

Ett återkommande tekniskt underlag som gör incidentrapporteringen snabbare, tydligare och mindre beroende av improvisation.

När incidenten pågår räcker det inte att veta att något är fel

Vid en betydande incident behöver verksamheten inte bara hantera det akuta läget. Den behöver också kunna rapportera uppåt och utåt med rimlig precision. Det betyder att IT snabbt måste kunna säga något meningsfullt om vad som verkar vara påverkat, hur stort problemet kan vara och vilket tekniskt läge som gällde innan incidenten bröt ut.

Det är här friktionen ofta uppstår. Verktyg för larm, loggning och incidentarbete kan vara helt nödvändiga. De ger ändå inte automatiskt ett sammanhållet underlag för rapportering.

> **Incidentrapportering blir tung när underlaget måste byggas i efterhand.** Då pågår både incidentarbetet och uppsamlingsprojektet samtidigt.

DET RAPPORTERINGEN KRÄVER

Det verksamheten snabbt måste visa

- Vad som var senaste verifierade tekniska läge
- Vad som verkar ha förändrats sedan dess
- Hur stor påverkan kan vara i antal och omfattning
- Vad som ännu inte går att bedöma säkert

DET SOM OFTA HÄNDER

Det IT ofta tvingas göra under press

- Samla ihop exporter från flera verktyg
- Återskapa en lägesbild från minne och muntliga förklaringar
- Skilja faktisk påverkan från databortfall och osäkerhet
- Formulera svar innan den tekniska bilden har satt sig

Varför loggar, larm och konsulter inte löser hela rapportfrågan

Det är lätt att tro att incidentrapportering i huvudsak är en fråga om övervakning. Men det är två olika saker. Det ena är att upptäcka, analysera och hantera incidenten operativt. Det andra är att kunna beskriva den på ett sätt som håller för ledning, tillsynsmyndighet, CSIRT och intern uppföljning.

Det senare kräver ett tekniskt underlag som går att återvända till. Annars blir rapporteringen tungt beroende av individer, konsultstöd och tillfälliga sammanställningar.

Tre rapportsteg som ställer olika krav

Cybersäkerhetslagen och NIS2 bygger på att informationen fördjupas stegvis. Det första svaret behöver inte vara fullständigt. Men det behöver vila på något mer än rena gissningar.

RAPPORTSTEG	DET SOM BEHÖVER FRAM	VAR UNDERLAGET OFTA BRISTER
Tidigt första svar	Vad som har hänt, vilken del av miljön som sannolikt berörs och vad som ännu inte går att bedöma säkert.	Senaste fastställda normalläge saknas eller är inte jämförbart med nuvarande bild.
Fördjupad uppdatering	Bättre avgränsning, trolig påverkan, tekniska brister före incidenten och vilka åtgärder som har påbörjats.	Data finns i flera system men är svår att översätta till en sammanhållen rapportbild.
Slutlig rapportering	Vad som faktiskt påverkades, vad som återställdes, vilka lärdomar som drogs och hur uppföljning ska ske framåt.	Historik och jämförbarhet saknas, vilket gör det svårt att visa förbättring och faktisk effekt efter incidenten.

Vad ett hållbart incidentunderlag måste kunna visa

För att incidentrapporteringen ska bli mer än en muntlig lägesbild behövs ett tekniskt underlag som klarar tre frågor samtidigt.

- Hur såg läget ut före incidenten?
- Vad verkar ha förändrats efter incidenten?
- Vad kan vi redan nu säga med tillräcklig säkerhet?

Just den kombinationen är svår att få fram om varje incident börjar från noll. Därför blir senaste verifierade normalläge ofta viktigare än man först tror.

Varför senaste normalläge är så viktigt

När en incident inträffar blir det snabbt viktigt att skilja mellan sådant som redan var känt, sådant som har förändrats nu och sådant som bara ser nytt ut därför att datainsamlingen är störd. Utan en tidigare fastställd bild blir den skillnaden betydligt svårare att göra trovärdig.

Ett bra incidentunderlag behöver därför inte vara realtid. Det behöver vara tillräckligt stabilt för att man ska kunna jämföra före och efter utan att ändra metod, scope eller språk varje gång.

Vad Statira inte ersätter

Statira ska inte vara SOC, SIEM, forensikverktyg eller incidentärendesystem. Det är inte där styrkan ligger. Styrkan ligger i att kunna bidra med ett fastställt tekniskt underlag när verksamheten behöver rapportera snabbt och samtidigt fortsätta hantera själva incidenten.

Det gör att incidentrapporteringen kan vila på samma logik som den löpande uppföljningen, i stället för att bli en separat specialövning.

Var Statira kommer in

Statira är byggt för att fastställa ett tekniskt nuläge, göra förändring synlig över tid och ge verksamheten ett underlag som går att använda både internt och utåt. Vid incidentrapportering betyder det att IT snabbare kan visa senaste normalläge, rimlig påverkan och vad som faktiskt går att stå för när tidspressen är hög.