IT-SÄKERHET · ÖVERLÄMNING · OFFENTLIG SEKTOR

När säkerhetsläget sitter i personer

I många kommuner och andra samhällsviktiga verksamheter finns personer som vet exakt var riskerna finns, vilka system som släpar efter och vilka undantag som fortfarande lever kvar. Det är värdefullt, men också sårbart. När den samlade bilden främst sitter i huvuden, gamla utdrag och lokala arbetssätt blir överlämning, chefsbyte och frånvaro ett reellt drift- och styrningsproblem.

- Varför personberoende är ett strukturproblem, inte ett kompetensproblem
- Vad lagkraven gör med sättet att arbeta med överlämning
- Vad som behöver fastställas för att hålla utan nyckelpersoner

I KORTHET

Kärnproblemet
Lägesbilden finns ofta i personer, minne och lokala utdrag snarare än i en återkommande struktur.

Konsekvensen
Överlämningar blir sköra och den nya ansvariga behöver lägga tid på att bygga upp bilden igen.

Det som minskar risken
Samma mätning, samma struktur och tydlig historik gör säkerhetsläget mindre personbundet.

När lägesbilden vilar på nyckelpersoner

I många kommuner och andra samhällsviktiga verksamheter bär en eller ett fåtal personer hela bilden av säkerhetsläget i huvudet. De vet ungefär vilka system som släpar efter, vilka konton som är känsliga och vilka gamla avvikelser som fortfarande väntar på åtgärd.

Det är inte ett kompetensproblem. Det är ett strukturproblem. Arbetet görs, men underlaget håller inte över tid. När någon slutar, byter roll eller blir sjuk måste bilden byggas upp igen.

1–2
personer bär ofta större delen av den samlade säkerhetsbilden i mindre organisationer

0
jämförbara mätpunkter finns ofta när någon frågar efter utvecklingen över tid

Art. 21
förutsätter ett systematiskt och återkommande säkerhetsarbete, inte muntliga lägesbilder

Varför kraven gör personberoendet svårare att bära

Cybersäkerhetslagen kräver inte perfekt säkerhet. Den kräver att organisationen kan visa ett systematiskt arbete som går att följa över tid. I praktiken behöver IT därför kunna svara tydligt på tre frågor:

- Hur såg läget ut vid senaste mätningen?
- Vad har förändrats sedan dess?
- Vilka åtgärder har genomförts och vilken effekt fick de?

När svaret främst sitter i personer blir detta svårt. När svaret finns i ett fastställt underlag blir det betydligt enklare att både styra arbetet och bära det vidare.

> **Nyckelinsikt:** Ett muntligt nuläge kan fungera i vardagen. Det fungerar sämre som överlämning, sämre som ledningsunderlag och sämre när tillsynsmyndigheten vill se hur arbetet utvecklats över tid.

Det här är också en konkurrensfråga. Varken punktverktyg eller enstaka konsultinsatser tar bort personberoendet av sig själva. De kan bidra med delar. Men om organisationen fortfarande måste luta sig mot samma nyckelpersoner när läget ska beskrivas, är problemet kvar.

Hur personberoendet byggs in i vardagen

Situationskunskap utan fast struktur

IT vet var luckorna finns, men kunskapen är utspridd mellan minne, script, exportfiler och gamla projekt. Bilden går att beskriva, men inte alltid att bära vidare.

Engångsrapporter utan historik

Organisationen beställer en genomgång, får en rapport och går vidare. Nästa gång börjar man i praktiken om, eftersom ingen återkommande mätning visar var risk faktiskt har reducerats.

Avvikelser utan fast nuläge

Larm hanteras när de uppstår. Men utan ett fastställt nuläge blir det svårt att se om avvikelsen är ett undantag eller en del av ett större mönster.

Vad organisationen vinner när lägesbilden går att lämna över

FRÅGA	PERSONBEROENDE	FASTSTÄLLT UNDERLAG
Vad är nuläget?	Beskrivs muntligt eller i utdrag	Fastställt och spårbart
Vad har förändrats?	Ofta oklart eller personbundet	Jämförbart mellan mätningar
Klarar överlämning?	Svagt	Ja
Klarar ledningsrapportering?	Manuellt och ad hoc	Återkommande
Klarar tillsyn?	Ofta tungt	Betydligt starkare utgångsläge

Vad som måste finnas med för att det ska hålla över tid

För att underlaget ska vara användbart måste det återkomma i samma form. Det handlar inte om att mäta allt, utan om att mäta rätt saker på ett sätt som håller över tid.

- **Patch och sårbarheter**. vad som faktiskt är eftersatt och hur det förändras
- **EOL-system och programvara**. vad som ligger kvar utan stöd
- **Endpoint-skydd**. täckning och luckor
- **Diskkryptering**. status och utveckling
- **AD-hygien**. privilegierade konton, inaktiva konton, policyavvikelser
- **Extern exponering**. vad som är synligt och kvarstår

När en ny ansvarig kan ta vid utan att börja om

När underlaget är fastställt kan en ny IT-chef eller nyckelperson ta över på ett annat sätt. Då går det att se var organisationen står, var risk har reducerats, vad som står still och vilka prioriteringar som redan gjorts.

Det minskar inte bara personberoendet. Det minskar också startsträckan till att ta ansvar i rollen.

Slutsats

Personberoende i säkerhetsarbetet löses inte med fler möten eller bättre ambitioner. Det löses när nuläge, förändring och prioritering fastställs period efter period i ett underlag som håller oavsett vem som råkar vara IT-chef just nu.