Säkerhetsnätverket

Minnesanteckning / sammanfattning

Säkerhetsnätverkets nätverksträff 1/12 2020
Plats: World Trade Center (Lexicon), Stockholm, men främst deltagande på distans.
Tema: Kvantitativ riskanalys genom föreläsning av Martin Bergling, RISE.
Närvarande: Madeleine Dahlkvist, Thomas Drugge, Johan Eckervad, Christina Einarsson, Ulf Gustafsson, Hans Leijonhufvud, Gustav Lind, Patrik Olsson, Annika Salomonsson, Bengt Axelsson (Nätverksledare).

Gäster: Jonas Blombäck, Coor

Endast Martin och jag var på plats i Lexicons lokaler. EvaLotta var där under lunchen och kunde hälsa på Martin och några av deltagarna. I övrigt var vi hänvisade till tekniken och digitalt deltagande.

Dagens program (som det blev)

1300-1310	Välkomna och presentation av deltagarna
1310-1430	Kvantitativ riskanalys
	Introduktion - dagens läge. Är IT-säkerhet svårare än andra säkerhetsområden?
	Varför behöver vi bättre riskanalyser? Vilka problem har vi idag?
	Kvantitativ riskanalys - några enkla metodsteg.
	Paus
	Monte Carlo-simulering av risk - demo av simuleringen.
	Hur kan jag införa detta i min organisation? Redan imorgon?
1430-1450	Kaffepaus
1450-1530	Frågestund och diskussion
1530-1545	Reflektion över dagen, nästa träff (1/12) och vårens teman (via medlemssidan)

Bengts anteckningar från träffen:

Eftersom ni har fått tillgång till presentation och simuleringsfilen så får ni inga särskilda anteckningar, utan mitt bidrag blir istället några personliga reflektioner.

Temat introducerades i inbjudan genom ett antal frågor, som för några kanske blev provocerande. Det är bra! För det är då som vi många gånger tänker till lite extra. Frågorna var:

Hur fungerar våra riskanalyser idag? Svarar de på frågan om hur stora riskerna är eller hur mycket riskerna minskar med den säkerhetsbudget man äskar? Riskhantering inom IT-verksamhet har alldeles för länge genomförts som en avancerad gissningslek där experter försöker ge sina bedömningar av risker. Det blir lätt fel, och det är definitivt inte effektivt. Hur kan vi då bedöma aktuella risker effektivare? Kort sagt - hur kan vi skapa bättre beslutsunderlag för säkerhetsinvesteringar?

Jag tror att vi alla känner igen oss i strukturen för s k kvalitativa riskanalyser. Trots namnet är det många gånger inte något annat än just ”avancerad gissningslek”. Då borde det vara angeläget att använda metoder som ökar kvaliteten i bedömningarna av riskerna och även i åtgärderna som ska minska riskerna. Användningen av en kvantitativ metod, ensam eller tillsammans med en kvalitativ metod, är en väg att gå för att öka kvaliteten i riskanalyserna.

Kunskapen om verksamheten, dess värden som måste skyddas och vilka sårbarheter den innehåller, är fundamental när det gäller riskanalyserna! Detsamma gäller även att bedöma relevanta åtgärder för att minska riskerna. En annan sak att ta i beaktande är den rådande säkerhetskulturen. Var finns den svagaste länken – är det cheferna eller medarbetarna? Är säkerhetskulturen något som värderas på er arbetsplats? Kan ni själva beskriva säkerhetskulturen på den egna arbetsplatsen? Är det isf något som ni upplever eller finns det dokumenterat underlag som hjälp för beskrivningen?

Jag vet inte hur länge ni får vara med i processen när det gäller riskanalyserna, men vill uppmana er att säkerställa att ni får vara med hela vägen fram till de som fattar beslut. Då har ni möjligheter att förklara och påverka utifrån er kompetens. Var noga med att dokumentera det som ligger till grund för riskanalyserna. Då har ni också möjlighet att följa utvecklingen (förhoppningsvis) över tid.

Att utveckla säkerheten är som att bygga förtroende, dvs det tar tid! Ni kommer förmodligen aldrig att bli klara, men ambitionen måste alltid vara att lämna en verksamhet som är säkrare än när ni tillträdde. Den inställningen, eller t o m den uttalade ambitionen, kan vara ett viktigt bidrag från dig för att påverka säkerhetskulturen.

Bilagor:

Martins presentation och Excelfilen (simuleringar) finns på medlemssidan.

Datum för kommande nätverksträff: 15/12 (kl 09:00-10:30)

Nästa träff är det vi själva som är våra egna inspiratörer genom att vi redovisar aktuell verksamhet. Vi håller på tills samtliga har fått redovisa, men längst intill kl 1030. Vi kommer också att prata om datum för vårens träffar, både digitala och fysiska samt kommande teman.