Skapa ramverk för IT-säkerhetsarbetet

Du behöver inte sitta ensam på kammaren längre och tänka fram smarta regler och strategier för IT-säkerheten på företaget. Det finns flera finurliga verktyg som ordnar det åt dig. Vi har testat tre av dem.

Text: Hans Husman

METODIKVERKTYG

- **SBA Check är ett ramverk för att skapa checklistor.**
- **SBA Scenario hjälper dig att analysera olika scenarier.**
- **Papai erbjuder en arbetsmetodik i fyra nivåer.**

Att strukturera säkerhetsarbetet är inget flum – det handlar om att få en säker miljö, och då är alla medel tillåtna. Åtminstone verktyg som hjälper dig att göra just detta.

Av de tre verktyg vi testat kommer två, SBA Check och SBA Scenario, från Dataföreningen. Idén är att de ska hjälpa till att strukturera informationssäkerhetsarbetet och ge en klar arbetsmetodik med ett tydligt flöde av aktiviteter.

SBA Check fungerar som ett ramverk för att skapa och arbeta med checklistor. Checklistor är en värdefull del av informationssäkerhetsarbetet som framför allt hjälper organisationen att leva upp till övergripande krav. Programmet fungerar relativt bra att skapa checklistor med. Frågorna kan struktureras på ett meningsfullt sätt och det går att lägga till lite extra information när man besvarar frågorna. Rapporterna vi skapar utifrån resultatet av frågorna blir acceptabla.

Tänker vi oss att detta ska vara ett verktyg som den informationssäkerhetsansvarige ruvar på för egen del räcker det kanske till. Men för den som aktivt vill föra ut sitt arbete i organisationen och ge medarbetarna ett konkret stöd i form av checklistor saknas det funktioner. Möjligheten att kunna exportera checklistorna från verktyget till ett snyggt Word-dokument eller en hemsida att ha på intranätet verkar inte finnas.

Dessutom hade det varit trevligt om man hade kunnat importera ifyllda checklistor automatiskt, till exempel genom att medarbetarna e-postar dem till ett konto som programmet kontrollerar. Ingen sådan import är möjlig. Hade det funnits hade den informationssäkerhetsansvarige kunnat följa det dagliga arbetet med checklistorna i hela organisationen.

Inga missar i checklistorna

Något som för de flesta är minst lika intressant som själva verktyget är checklistorna i sig. Det finns checklistor för 7799, FA22, två för PUL och en ganska generell checklista för nulägesanalyser av informationssäkerhetsstatusen. Alla checklistorna är bra. Det finns så vitt vi kan se inga uppenbara missar eller felaktigheter. Däremot hade det varit ett plus om man för varje fråga hade kunnat få fram en utförlig bakgrundstext. Det finns flera frågor där kunder kommer att göra olika tolkningar av frågan.

Sammanfattningsvis känns programmet otillräckligt för större företag. Genom de checklistor som kommer med är SBA Check ändå ett bra köp, också med tanke på priset på 14 000 kronor för en licens. SBA Check får fyra i betyg.

Dags att skapa scenarier

SBA Scenario är verktyget som hjälper till när det är dags att analysera scenarier som kan påverka era olika resurser. När man ska skapa ett nytt scenario får man upp en liten karta med knappar. Man fyller sedan i data av olika typer, till exempel analysledare, system som analysen görs på, de personer som deltar i analysen, brister med uppskattad skadekostnad och sannolikheten för att en händelse kan inträffa under året (förenklat till antal händelser). Utifrån detta kan man sedan ta fram bra sammanfattande rapporter. Här finns också möjligheten att generera rapporter som bygger på olika gruppers arbete med de här frågorna.

En bra sak med verktyget är att det nästan per automatik ger ett strukturerat och bra arbetssätt. Även om vi saknar en del funktioner så finns just kring själva arbetssättet det mesta som behövs.

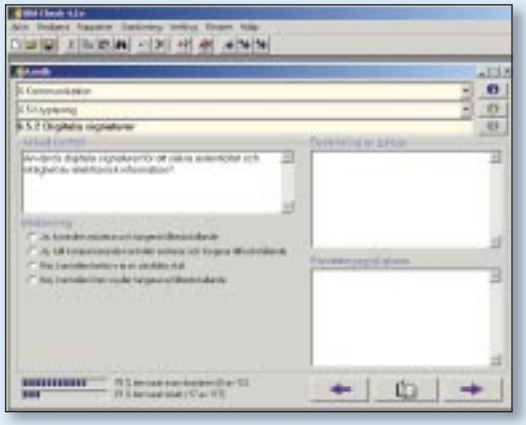
Den stora frågan är emellertid när det är vettigt att betala pengar för programmet. Ligger ett ganska stort företag efter med säkerhetsarbetet och behöver göra en tillfällig kraftsamling kring en större revision kan det vara värdefullt att ha SBA Scenario. Priset på 106 000 kronor för tio licenser och 15 000 kronor för en licens är dock lite väl magstarkt i förhållande till vad man får.

Frågan är också om större företag inte redan har andra verktyg som fungerar lika bra. Många har

Forts ▷▷

SBA CHECK

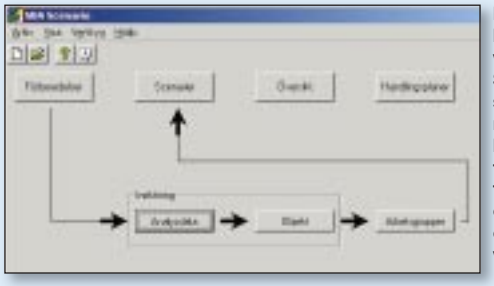
LEVERANTÖR: Dataföreningen
DISTRIBUTÖR: Dataföreningen
CIRKAPRIS: 1 licens 14 000 kronor, 30–50 licenser 360 000 kronor. Priser däremellan finns.
PLATTFORM: Microsoft Windows
S&S TYCKER: Checklistorna som kommer med är användbara. Däremot är själva verktyget ganska begränsat.
BETYG: ●●●●○



Här ser vi fönstret som används för att besvara frågorna i SBA Checks checklistor. Det finns stora möjligheter till förbättringar av verktyget, men de checklistor som kommer med är i alla fall riktigt bra.

SBA SCENARIO

LEVERANTÖR: Dataföreningen
DISTRIBUTÖR: Dataföreningen
CIRKAPRIS: 1 licens 15 000 kr, 380 000 kronor för 30–50 licenser. Priser däremellan finns förstås också.
PLATTFORM: Microsoft Windows
S&S TYCKER: Kan vara användbart i vissa fall, men värdet ligger inte ens i närheten av priset.
BETYG: ●●○○○



I bilden syns arbetsflödet för verktyget SBA Scenario. Arbetet sker genom att man klickar på knapparna och fyller i information allt eftersom om olika scenarier som man kan vänta sig.

PAPAI

LEVERANTÖR: Mixtum
DISTRIBUTÖR: Mixtum
CIRKAPRIS: 4 000 kronor för baspaketet
PLATTFORM: Webbaserad presentation
S&S TYCKER: En utmärkt lösning som hela IT- och informationssäkerhetsarbetet kan hängas upp på. Mycket prisvärt.
BETYG: ●●●●●

Papai ger oss en metodik som hela säkerhetsarbetet kan baseras på. I bilden ser du de fyra grundnivåerna i Papai. För varje aktivitet kan man klicka vidare för att på detta sätt få en högre finkornighet i aktiviteten.

▷▷ ju redan annat metodstöd, till exempel RUP, vars metodik och verktyg mer än väl även täcker upp det som SBA Scenario erbjuder.

Sammanfattningsvis kan SBA Scenario i vissa fall vara användbart men priset är omotiverat högt. Det får en tvåa i betyg.

Fyra nivåer för arbetet

Nästa system som vi testade var Papai, som är ett komplett ramverk för både IT- och informationssäkerhetsarbete. I centrum av systemet finns en arbetsmetodik som börjar i den aktuella verksamhetens krav och går vidare ända ner i implementeringen.

De olika aktiviteterna har delats in i fyra olika organisationsnivåer. Den översta nivån är ledningsnivån där verksamhetens krav ska resultera i en säkerhetspolicy. Nivån under är den administrativa. Där sker först ett analysarbete som påverkas dels av nuläget i den tekniska nivån och verksamhetens krav från den översta nivån, dels av omvärlden. Utifrån denna analys tas sedan en plan fram för organisationens säkerhetsarbete.

När planen är på plats lämnas den vidare till systemnivån, där arkitekturen för alla säkerhetsfunktionerna utvecklas. Arkitekturen påverkas uteslutande av planen. I Papai-metodiken säger man föredömligt nog att denna arkitektur bara ska ange och definiera säkerhetsfunktionen, inte göra enskilda produktval. Detta arbetssätt ger fördelar över tiden genom att man i implementeringsarbetet får en större frihet att byta ut produkter och göra konkurrerande upphandlingar.

I den lägsta Papai-nivån finns så tekniken. Här är implementering den enda aktiviteten, och arbetet ska bara påverkas av arkitekturen.

För varje aktivitet kan man i verktyget få en högre upplösning där aktiviteten delas upp i en steg för steg-lista. De data som verktyget presenterar är också anpassningsbara genom att man kan lägga till egna dokument, köpa till fler paket, lägga till checklistor och information om kontaktpersoner med mera. Presentationen sker via webbsidor, vilket fungerar bra.

Intressant är naturligtvis att fundera över i vilka situationer Papai är användbart. För den informationssäkerhetsansvarige fungerar det utmärkt som metodik för hela arbetet, planeringen och strukturering av dokument och information. Genom att hela miljön presenteras i form av klickbar HTML fungerar Papai även utmärkt på företagets intranät som en samlingspunkt för säkerhetsarbetet i företaget. En plats där alla medarbetare enkelt kan surfa in och hämta sådant man behöver i form av policyer, riktlinjer, checklistor med mera.

Du kan styra vad som köps in

Genom att det för varje aktivitet går att få en högre upplösning som man själv kan bygga ut går det även utmärkt att använda programmet som ramverk när man tar fram anpassade kunskapsstöd för olika delar av organisationen. Vill man att medarbetarna ska göra vissa säkerhetsaktiviteter när produkter köps in eller system utvecklas kan detta läggas in i Papai.

Verktyget som behövs för att uppdatera trädstrukturen kommer med på köpet. HTML-koden är även vettigt strukturerad, så det fungerar bra att göra många av förändringarna för hand om man föredrar det.

När man köper grundpaketet får man även med en lärobok. Den är omfattande och ger bra bakgrundsinformation både till olika säkerhetsområden och programmet i sig. Vidare får man hela metodikstrukturen och verktyg för att uppdatera denna, stöd för projektplanering, dokumenthantering och hantering av kontaktpersoner, checklistor och statistik. Däremot följer det inte med några färdiga checklistor eller paket för att hantera viktiga delområden. Paketen kan dock köpas till, till exempel för policyer, incidenthantering och katastrofhantering.

För drygt 4 000 kronor råder det ingen tvekan om att man får valuta för pengarna. Metodiken är bra och leverantören har lagt ordentligt med krut på att se till att det fungerar i verkligheten över en längre period.

Även om priset för baspaketet är rimligt anser vi att åtminstone ett av utbyggnadspaketen ska skickas med gratis. Många företag kommer inte att vilja köpa dessa i alla fall, eftersom de redan har inarbetade system för vissa områden. Det skulle dock vara värdefullt för dessa företag att få med ett komplett paket på köpet att använda som utgångspunkt när de anpassar sitt eget material.

Sammanfattningsvis är det väldigt mycket man får för pengarna när baspaketet med metodiken, webbsidorna, verktyget, boken och exemplen kostar så lite. Vårt betyg blir fem. ■

Hans Husman är IT-säkerhetskonsult i egen regi. Vill du e-posta honom når du honom på hans. husman@hanshusman.nu.