

MiniGuide

Metoder för att analysera säkerhetsrisker

IT- & Informationssäkerhet



Introduktion
Riskanalys är en grundläggande del i säkerhetsarbetet och om man arbetar med stöd av ISO/IEC 27000 är det en del av riskbedömning och riskbehandling.

Definitionen riskanalys innebär att man systematiskt använder information för att kartlägga källor till risker och uppskatta hur de påverkar organisationen. Risk i sin tur är produkten av sannolikheten för att en händelse skall inträffa och vilka konsekvenserna blir av denna händelse.

Metoder för att bedöma risker
Det finns i huvudsak två metoder för att bedöma risker, kvantitativ och kvalitativ.

Kvantitativ metod: Innebär att man försöker ange verkliga tal för hur mycket en händelse som inträffar skulle kosta organisationen samt hur mycket det skulle kosta att skydda sig mot att händelsen inträffar. Detta förutsätter att sannolikhet och konsekvens uppskattas i procenttal.

Kvalitativ metod: Innebär att man gör en graderingen eller ranking för att beskriva om en risk har liten eller stor betydelse för organisationen. För att göra detta kan man använda hög, medel eller låg som gradering eller siffror för ranking.

Tillvägagångssätt för att göra riskanalyser
Du kan gå tillväga på olika sätt för att göra riskanalyser, där valet utgår ifrån de förutsättningarna som finns i den egna organisationen.

Finns det en medarbetare som har detta som en del i sina arbetsuppgifter, innebär det oftast ett rutinarbete där information och tillgångar identifieras och värderas. Därefter analyseras vilka hot som finns för dessa samt hur de skulle påverka organisationen. Med stöd av detta kan man ta fram en plan för att behandla risker.

Man kan även använda sig av arbetsmöte där man bjuder in olika representanter för att identifiera risker och bedöma hur de skall behandlas. I detta fall är det vanligt att man utgår ifrån scenario, dvs händelseförlopp, för att beskriva vad som kan inträffa och göra bedömning av sannolikhet och påverkan. Fördelen med arbetsmöten är en ökad riskmedvetenhet.

Behandling av risker
Det finns fyra huvudalternativ för att behandla risker:
Överföra - Låt någon annan ta risken, t.ex. försäkring.
Reducera - Inför motåtgärder för att minska risken.
Acceptera - Ta beslut att inte göra något åt risken.
Ävissa - Förneka eller ignorera risken.

IT Ledarskap

Vi erbjuder spjutspetskompetens med hög integritet för att hjälpa företag och organisationer till ett effektivt utnyttjande av IT med målsättning att verksamhetsprocesser skall leverera och skapa värde.