Innehållsförteckning

4 FÖLJA UPP OCH FÖRBÄTTRA 2

4.1 ORGANISATIONENS SÄKERHETSÅTGÄRDER 3

4.1.1 Varför ska man följa upp säkerhetsåtgärder? 3

4.1.2 Att arbeta med att följa upp säkerhetsåtgärder 3

4.1.3 Planera hur du ska följa upp dina säkerhetsåtgärder 3

4.1.4 Följa upp och förbättra säkerhetsåtgärder för styrning 4

4.1.5 Följa upp och förbättra säkerhetsåtgärder som skyddar informationsbehandling 4

4.1.6 Informera och kommunicera 5

4 Följa upp och förbättra

4.1 Organisationens säkerhetsåtgärder

Den här vägledningen beskriver hur du kan arbeta med att följa upp arbetet med säkerhetsåtgärder i organisationen, både säkerhetsåtgärder för styrning och för informationsbehandling (**Utforma Organisationens säkerhetsåtgärder**).

4.1.1 Varför ska man följa upp säkerhetsåtgärder?

Säkerhetsåtgärder som vid en tidpunkt varit tillräckliga och fungerat bra kan över tid bli otillräckliga. Orsaken kan vara att det ställs nya externa krav eller att hoten mot organisationens informationsbehandling ändras. Det kan också komma nya tekniker som reducerar risker på ett bättre sätt än en tidigare vald lösning. Säkerhetsåtgärder kan också behöva förändras därför att organisationen utvecklas och nya verksamheter tillkommer eller att verksamheter förändras eller inte längre bedrivs.

4.1.2 Att arbeta med att följa upp säkerhetsåtgärder

Det är bra att tänka igenom hur olika säkerhetsåtgärder bör följas upp redan när man anpassar dem till organisationens behov men det går också att tänka igenom det senare. Men vänta inte för länge med att genomföra uppföljningar av införda säkerhetsåtgärder eftersom uppföljningar ger det underlag som behövs för att bedöma om skyddet är tillräckligt eller om det behöver förbättras.

Resultatet av uppföljningen kan innebära att de interna reglerna behöva förändras eller arbetssätten utvecklas. Det kan också resultera i att tekniska eller fysiska säkerhetsåtgärder behöver justeras eller bytas ut (se **Utforma Handlingsplan** och **Använda Organisationens säkerhetsåtgärder**).

4.1.3 Planera hur du ska följa upp dina säkerhetsåtgärder

Hur en säkerhetsåtgärd bör följas upp liksom frekvensen för uppföljningen varierar beroende på vilken säkerhetsåtgärd det handlar om. Gemensamt är dock att uppföljningen ska handla om åtgärdens

- **lämplighet** – säkerhetsåtgärden ska bidra till att ni når era mål,
- **tillräcklighet** – säkerhetsåtgärden ska bidra till ett tillräckligt skydd för att motverka era risker
- **verkan** – säkerhetsåtgärden ska vara fullt införd och fungera väl.

Syftet med uppföljningen påverkar hur ni genomför den. Syftet med uppföljningen kan också variera beroende på vilken roll som genomför den.

Som ansvarig för en säkerhetsåtgärd vill du veta att den fungerar som den ska och att den är tillräcklig. Det är något du kan vilja veta ofta.

Som CISO som ska ta fram underlag inför Ledningens genomgång är du intresserad av att förmedla en övergripande bild av hur väl säkerhetsåtgärderna fungerar och du lägger troligen fokus på åtgärder som ska motverka mycket allvarliga risker och på de inte fungerar som de ska.

4.1.4 Följa upp och förbättra säkerhetsåtgärder för styrning

Som CISO och ansvarig för att leda och samordna arbetet med styrningen av informationssäkerheten behöver du identifiera hur du ska följa upp ditt arbete liksom vilken uppföljning du behöver från andra ansvariga för säkerhetsåtgärder för att kunna sammanställa underlag om säkerhetsläget i organisationen exempelvis till ledningens genomgång.

De säkerhetsåtgärder som du som CISO är ansvarig för behöver du följa upp mer noggrant. Det innebär att du behöver följa upp att allt ni har utformat används och fungerar effektivt. En förutsättning för att du ska kunna göra detta är att du har en god dialog med organisationen gällande varför en säkerhetsåtgärd är utformad som den är, varför den behövs och hur den fungerar. Du behöver åtminstone följa upp arbetet med

- informationssäkerhetsorganisationen
- ledning och styrning
- informationssäkerhetsmål
- styrdokument på en övergripande nivå, såsom informationssäkerhetspolicyn
- organisationens säkerhetsåtgärder
- riskhantering
- klassningsmodell och skyddsnivåer
- organisationens handlingsplan för informationssäkerhet
- kontinuitetshantering
- incidenthantering.

Om du upptäcker brister i dessa säkerhetsåtgärder behöver du också kunna förklara vilka konsekvenser bristerna leder till. Det kan vara svårare här än när det gäller säkerhetsåtgärder för informationsbehandling eftersom effekten på den faktiska säkerheten är indirekt. Här gäller det alltså att kunna förklara till exempel att brister i klassningsmodell och skyddsnivåer innebär att ni inte får rätt värdering på er information eller fel skydd relaterat till värdet. Bristande användning av modellerna innebär att ni inte vet vilken information som är skyddsvärd.

4.1.5 Följa upp och förbättra säkerhetsåtgärder som skyddar informationsbehandling

Hur säkerhetsåtgärder som skyddar en viss informationsbehandling följs upp varierar beroende på vilken säkerhetsåtgärden är. Syftet är dock detsamma – att kontrollera att säkerhetsåtgärden är tillräcklig och att den fungerar väl.

Det är i första hand den som ansvarar för en säkerhetsåtgärd ansvarar för att följa upp att den fungerar som den ska.

Som CISO behöver du ha en nära dialog med den som ansvarar för en säkerhetsåtgärd för att komma överens om lämpliga sätt att följa upp att säkerhetsåtgärden fungerar. Du behöver också vara tydlig med vad du behöver för att kunna sammanställa status för hela organisationens informationssäkerhet. Du behöver kunna analysera, strukturera och sammanfatta resultat från den uppföljning som skett i organisationen. Det här blir underlag för att kunna utvärdera om säkerheten är tillräcklig och vid behov förbättra en säkerhetsåtgärd.

4.1.6 Informera och kommunicera

Förändringar i säkerhetsåtgärder behöver kommuniceras från dem som ansvarar för säkerhetsåtgärden till dem som har styrande dokument på lägre nivåer. Tänk på att kommunicera förändringar som innebär att olika målgrupper behöver ändra sitt sätt att arbeta på ett tydligt sätt.

Det behöver också finnas upparbetade rapporteringsvägar att påtala upplevda brister i säkerhetsåtgärder. Det kan till exempel göras genom att rapportera bristen som en avvikelse i ordinarie incidenthantering, antingen till den som ansvarar för säkerhetsåtgärden eller direkt till dig som CISO.

Använd upparbetade kanaler till ledningen för att förmedla både planerade avstämningar av hur informationssäkerheten ser ut i organisationen (Ledningens genomgång) och för händelsestyrd information, till exempel tillräckligt allvarliga incidenter eller risker som upptäckts.