Myndigheten för samhällsskydd och beredskap

Innehållsförteckning

3 Använda

3.1 [Använda] Organisationens säkerhetsåtgärder

Den här vägledningen beskriver hur du som CISO stöttar organisationen med att anpassa säkerhetsåtgärder till organisationens behov och förutsättningar. Det vill säga när ni arbetar med att genomföra de aktiviteter ni tagit fram i den övergripande handlingsplanen (se **Utforma Handlingsplan**) för att införa och förbättra säkerheten i organisationen.

Här beskrivs hur du som CISO stödjer de som är ansvariga för en säkerhetsåtgärd utifrån deras behov. Stödet kan bestå i att tolka innebörden av säkerhetsåtgärden, förstå hur åtgärden kan passas in i styrdokumentstrukturen i olika detaljeringsgrader och samordna säkerhetsåtgärder mellan olika ansvariga. Stödet kan också bestå i att vara bollplank åt den ansvarige i anpassningen av en säkerhetsåtgärd så att den blir tillräckligt bra.

- Varför och hur du arbetar med säkerhetsåtgärder och hur de anpassas till vad din organisation behöver beskrivs i **Utforma Organisationens säkerhetsåtgärder**.
- Stöd för hur du analyserar vilka säkerhetsåtgärder ni behöver finns i **Identifiera och analysera Organisationens säkerhetsåtgärder.**
- Arbetet med att kontrollera att de säkerhetsåtgärder som ni infört i organisationen är tillräckliga beskrivs i **Följa upp och förbättra Organisationens säkerhetsåtgärder.**

3.1.1 Varför anpassa säkerhetsåtgärder för informationsbehandling?

Att anpassa säkerhetsåtgärder är det sista steget i arbetet med att säkerställa att säkerhetsåtgärderna ger informationen tillräckligt skydd. Syftet är att avgöra hur säkerhetsåtgärden faktiskt ska införas och se till att alla som har ett ansvar kopplat till säkerhetsåtgärden är medvetna om och har accepterat vad som förväntas av dem.

3.1.2 När ska säkerhetsåtgärderna anpassas?

Säkerhetsåtgärder för informationsbehandling behöver i många fall anpassas så att skyddet är tillräckligt för varje ny eller förändrad informationsbehandling.

Säkerhetsåtgärder från olika källor i beskrivs i olika detaljeringsgrad. Vissa säkerhetsåtgärder ser likadana ut för all information, medan andra kommer att behöva variera i styrka beroende på skyddsbehovet. En del säkerhetsåtgärder behöver ni förtydliga utifrån era förutsättningar medan ni kan ta andra direkt från källan.

Vissa säkerhetsåtgärder för informationsbehandling lämpar sig bäst att enbart anpassas i en version som sedan gäller för hela organisationen. Ibland blir anpassning som görs i en del av organisationen så bra att den kan göras generell och användas i hela organisationen. Omvänt kan en säkerhetsåtgärd som anpassats för att gälla hela organisationen behöva anpassas särskilt för att ge tillräckligt skydd för en viss verksamhet eller viss information.

Säkerhetsåtgärderna bör därefter ses över i samband med att informationsklassningar och riskanalyser uppdateras. Detta för att säkerställa att införda säkerhetsåtgärder fortsatt är tillräckliga. Säkerhetsåtgärderna bör också ses över när UoT uppdateras (se **Identifiera och analysera Organisationens säkerhetsåtgärder**).

Säkerhetsåtgärder anpassas alltså när:

- kravet är för generellt beskrivet och behöver konkretiseras utifrån organisationens mål och behov (anpassning till styrdokumentsnivå)

- kravet – som det står i organisationens styrdokument – behöver anpassas på något annat sätt för att kunna tillämpas vid en viss informationsbehandling (anpassning på verksamhets- och informationsbehandlingsnivå).

3.1.3 Planering och förberedelser

Utgångspunkten för arbetet är de regler och arbetssätt som har tagits fram i arbetet med att **Utforma Organisationens säkerhetsåtgärder**.

Ett bra underlag för att kunna anpassa säkerhetsåtgärden till organisationens behov och förutsättningar kan vara:

- en beskrivning av den information som behandlas och hur den används (**Identifiera och analysera: Verksamhetsanalys)**
- resultat från klassningar och riskanalyser som genomförts (**Använda Klassning och Riskanalys**)
- kunskap om övriga säkerhetsåtgärder som skyddar aktuell informationsbehandling.

Hjälps åt att inhämta relevanta underlag från informationssäkerhetsarbetet, från informations- och riskägare samt från ansvariga för andra säkerhetsåtgärder. Exempel på relevant underlag kan vara:

- organisationens riskregister
- status för olika införda säkerhetsåtgärder
- önskemål från riskägare för prioriterade verksamheter och liknande.

3.1.4 Genomförande

För att en säkerhetsåtgärd ska införas och fungera väl behöver det för varje säkerhetsåtgärd framgå tydligt:

- **Var** och **när** säkerhetsåtgärden ska användas i organisationen – till exempel av alla, av medarbetare i arkivfunktionen, vid it-utveckling eller inför inköp.
- **Vem** – alltså vilken roll – som ansvarar för att säkerhetsåtgärden används och ger det skydd som informationsbehandlingen behöver, till exempel informationsägare.
- **Hur** säkerhetsåtgärden ska användas för att fungera väl, vilket till exempel kan beskrivas i användarmanual.

Ett första steg när du börjar anpassa en säkerhetsåtgärd är att läsa säkerhetsåtgärdens beskrivning i er UoT och förstå på vilken nivå i styrdokumentsstrukturen som den behöver finnas beskriven för att ge effekt i din organisation.

Exempel på en säkerhetsåtgärd som behöver införas på alla nivåer (se **Utforma Styrdokument**)

- Kravet att ”endast behöriga ska få åtkomst till information” innebär att säkerhetsåtgärden ”behörighetshantering” behöver finnas. Här bör det som en del av **informationssäkerhetspolicyn** framgå att endast behöriga användare ska få tillgång till information.
- Därefter behövs en **riktlinje** för hur beslut om behörigheter fattas, att den som är ansvarig för informationsbehandlingen får fatta beslut om behörighet och hur ofta

det ska följas upp att behörigheter som inte längre behövs är borttagna eller blockerade.

- Det behövs också en **instruktion** för den personal som lägger upp behörigheter i organisationens behörighetssystem eller i enskilda it-system så att det är tydligt vem som får besluta om att en viss behörighet ges, förändras eller tas bort och hur detta genomförs i it-systemet.

3.1.4.1 Förstå i vilket styrdokument en säkerhetsåtgärd ska föras in

För att säkerhetsåtgärden ska fungera i organisationen behöver den kunna hittas av den som ska följa den. Målet är att säkerhetsåtgärden ska hamna på en plats i styrdokumentsstrukturen som är logisk för organisationen. Här är det bra att tänka målgruppsanpassat det vill säga vilka roller som behöver veta vad. Fundera på om det redan finns en bra plats i ett befintligt styrdokument eller om nya styrdokument behöver tas fram.

3.1.4.2 Att beskriva säkerhetsåtgärder på olika nivåer i styrdokumentsstrukturen.

Hur säkerhetsåtgärden beskrivs på olika nivåer beror på hur organisationen beskriver saker i olika styrdokument.

På det vi kallar riktlinjenivå beskriver ni följande:

- Vad ska göras

Exempel: ”Byt ut förinställda lösenord i alla it-system före driftsättning.”

Detta kan till exempel göras i en informationssäkerhetsriktlinje, som en del av en säkerhetsriktlinje eller uppdelat på riktlinjer där säkerhetsåtgärden passar in, exempelvis hos HR eller it.

På det vi kallar instruktionsnivå beskriver ni följande:

- Vilken roll, vem, som ska genomföra säkerhetsåtgärden
- Under vilka omständigheter, i vilka situationer, vid vilken tidpunkt, det ska göras
- Hur säkerhetsåtgärden ska genomföras.

Exempel: ”Ansvarig it-tekniker ska innan it-system sätts upp i produktionsmiljön, utvecklingsmiljön eller testmiljön byta ut förinställda lösenord till lösenord som följer [riktlinje för lösenordshantering]. Detta gäller oavsett om det är fråga om nyinstallation eller om utrustningen ska används för nytt syfte. Hur tillgång till lösenord ges ska dokumenteras i it-systemets driftsdokumentation.”

3.1.4.3 Ta fram instruktioner

Instruktioner behöver ofta målgruppsanpassas och kan finnas i minst fyra varianter. De som

- beskriver vad som ska göras innan information behandlas för att få underlag för att veta vilka säkerhetsåtgärder som behövs, till exempel klassning av information, riskbedömning, juridisk analys
- direkt rör själva informationen, vilken information som ska sparas var, hur den ska användas, vem den får delas med och hur den får delas.

- beskriver hur resurser ska hanteras, till exempel nycklar till lås, konfiguration av system, hur tester ska genomföras med mera
- handlar om vad man ska göra om någonting inte fungerar som det ska.

Några vanliga målgrupper som kan behöva instruktioner:

- slutanvändare – medarbetare, chef
- kontinuitetsansvariga, riskhandläggare, incidenthanterare
- systemadministratörer, fastighetsskötare, HR-handläggare

Exempel på instruktioner till specifika målgrupper:

- **Slutanvändare:** Du ska hantera ditt passerkort som en värdehandling. Misstänker du att du förlorat det ska du anmäla detta till: Anmäl incident/behörighetskort.

- **Incidenthanterare:** Vid anmälan om förlorat passerkort förmedla incidenten till systemadministratören samt starta den utredning som behövs vid sådan incident.

- **Systemadministratörer:** Vid anmälan om förlorat passerkort ska du blockera kortets behörigheter och skapa en ny behörighet för medarbetaren att använda enligt [instruktion om utfärdande av tillfällig behörighet].

De utpekade rollerna i organisationen behöver samverka i arbetet med att ta fram de instruktioner som rör själva informationen och hur de informationsbehandlande resurserna ska hanteras. Informationsägarna beskriver hur informationen får användas och systemägarna beskriver hur it-systemen får användas.

Processägare eller motsvarande stödjer med att beskriva hur olika instruktioner passar in i befintliga eller nya informationsflöden och hjälper till med arbetssätt som säkerställer att organisationen behandlar sin information säkert. Detta ska samordnas genom att informationsägaren ser till att informationen klassas och att en riskanalys genomförs för att identifiera de säkerhetsåtgärder som behövs för att skydda informationsbehandlingen.

Systemägaren föreslår utifrån informationsägarens behov vilka säkerhetsåtgärder som behövs för att skydda informationen, i vilket it-system eller it-miljö informationen ska behandlas för att få tillräckligt skydd, eller vad som krävs för att ett nytt informationssystem ska passa in.

3.1.4.4 Säkerställ samverkan mellan ansvariga för olika säkerhetsåtgärder

Det behöver finnas en dialog mellan roller med olika ansvar för informationssäkerheten, till exempel informationsägare, den som ansvarar för det personalrelaterade arbetet, systemägare och ansvariga för lokaler för att skyddet ska fungera som helhet. Tillsammans kan ni säkerställa att säkerhetsåtgärder för informationsbehandling, it-system och lokaler samspelar med varandra och sammantaget ger ett tillräckligt skydd för hela behandlingen.

3.1.4.5 Testa styrdokument

Innan styrdokumenten beslutas är det bra att kontrollera att någon eller några som ska använda dokumentationen förstår vad som står. Testa riktlinjer på de som ska skriva instruktioner. Testa slutligen instruktioner på de som ska utföra arbetet så att de förstår hur de ska göra. När styrdokumentet beslutats, planera att efter någon vecka stämma av med

någon eller några användare hur styrdokumentet fungerar när det börjat användas (se **Följa upp och förbättra Organisationens säkerhetsåtgärder**).

3.1.4.6 Relaterade vägledningar

Ytterligare stöd i anpassning av specifika typer av säkerhetsåtgärder finns i vägledningarna

- Säkerhetsåtgärder i informationssystem
- Grundläggande säkerhet i cyberfysiska system
- Upphandla informationssäkert
- Vägledning för informationssäkerhet i IT utrymmen.

3.1.5 Utbilda och informera medarbetare

Medarbetare bör så tidigt som möjligt, helst innan de kommer i kontakt med organisationens information, få en grundläggande utbildning i informationssäkerhet (se **Använda Utbilda och kommunicera**). Utbildningen behöver sedan kompletteras med vilka instruktioner som gäller för den information som den enskilda medarbetaren kommer i kontakt med, till exempel via olika it-system.

Målet med detta är att alla medarbetare som behandlar information ska ha en förståelse för

- varför informationen är viktig för organisationen,
- att instruktionerna finns där för att säkerställa att informationen är skyddad och
- att medarbetaren har en viktig roll att skydda informationen och ett ansvar att följa de regler som finns.

3.1.6 Följa upp och förbättra

För att du ska kunna följa upp och förbättra arbetet med säkerhetsåtgärder på en övergripande nivå (se **Följa upp och förbättra Organisationens säkerhetsåtgärder**) behövs två saker. Dels behöver det finnas löpande uppföljning av att styrande dokument, riktlinjer och instruktion och tillhörande stöd, fungerar som det är tänkt. Dels behöver det finnas arbetssätt för den som är ansvarig för ett styrdokument att återrapportera resultat från sin uppföljning på ett sammanfattat sätt till dig som CISO.

Varje införd säkerhetsåtgärd behöver alltså följas upp (se **Följa upp och förbättra**). Baserat på den uppföljningen kan den som är ansvarig för säkerhetsåtgärden vid behov vidta relevanta åtgärder.

Att bygga in återkoppling i arbetssättet kan vara till nytta för flera i organisationen, i exemplet ”Byt ut förinställda lösenord i alla it-system före driftsättning” sätter nätverksteknikern sin signatur att lösenordsbytet genomförts, det kontrolleras med automatiska tester, och innan driftsättning som en del av ändringshanteringsarbetet hos organisationen säkerställs att testet som kontrollerar att förinställda lösenord är utbytta har genomförts.

Här kan du också välja att kontrollera att instruktionerna följer riktlinjer som i sin tur har sin utgångspunkt i ledningens mål och inriktning. Det viktigaste är dock att instruktionerna följs och ger tillräcklig säkerhet.

Det finns olika sätt att sammanfatta för att kunna följa upp på en övergripande nivå. Ofta behövs någon form av analysarbete för att identifiera vad som är intressant att följa upp på en övergripande nivå.

I exemplet i exemplet ”Byt ut förinställda lösenord i alla it-system före driftsättning” kan antalet tester som identifierat avvikelser räcka. I andra fall vill man veta mer, som till exempel efter en anmälan om en incident kan man exempelvis vilja följa upp:

- Om det inte var en incident: Varför rapporterades det som en sådan? Behövs mer utbildning? Var det en avvikelse som kunde ha lett till en incident?
- Om det var en incident: Vad berodde den på? Vad behöver göras för att den inte ska upprepas? Eller för konsekvenserna ska bli mindre om det trots allt händer igen?

3.1.7 Resultat

Du har tagit fram och infört eller gett möjlighet till att införa säkerhetsåtgärder i din organisation som är anpassade för era behov och förutsättningar. Du har förutsättningar för att följa upp att dina säkerhetsåtgärder fungerar och är tillräckliga över tid.