Myndigheten för samhällsskydd och beredskap

Innehållsförteckning

2 Identifiera och analysera

2.1 [Identifiera och analysera] Organisationens säkerhetsåtgärder

Den här vägledningen ger stöd i arbetet med att förstå vilka säkerhetsåtgärder som behövs för att skydda organisationens information och de resurser som hanterar information. Varför och hur du arbetar med säkerhetsåtgärder så att de anpassas till vad din organisation behöver beskrivs i **Utforma Organisationens säkerhetsåtgärder**. Hur din organisations säkerhetsåtgärder anpassas, införs och förvaltas beskrivs i **Använda Organisationens säkerhetsåtgärder**. Arbetet med att kontrollera att de säkerhetsåtgärder som ni infört i organisationen är tillräckliga beskrivs i **Följa upp och förbättra Organisationens säkerhetsåtgärder.**

2.1.1 Syftet med analysen av organisationens säkerhetsåtgärder

Denna analys ger kunskap om vilken styrning av informationssäkerhet ni ska utforma för inom er organisation (till exempel underlag för allt arbete som beskrivs under steget **Utforma**). Mer konkret innebär det att det sammanlagda resultatet från samtliga analyser (av omvärld, verksamhet, risk, och säkerhetsåtgärder) ger svar på dels hur er organisation bäst angriper informationssäkerhetsfrågan (var ni ska börja arbeta, varför, vem och i vilken ordning), dels vilka säkerhetsåtgärder ni behöver för att skydda er information.

Det här innebär att utformning av allt ifrån organisation (ansvar och roller) för informationssäkerhet till policy, riktlinjer, arbetssätt och aktiviteter utgår från resultatet av dessa analyser.

Om ni vill ha en mer sammanfattande bild av analysresultatet kan ni sammanställa samtliga analysers resultat i ett separat dokument. Ett sådant dokument kan ni sedan använda som grund för att beskriva värdet av det systematiska informationssäkerhetsarbetet (s.k. ”business case”).

Resultatet av denna analys är en nulägesbeskrivning av hur långt organisationen har kommit med olika säkerhetsåtgärder och en prioriterad lista över de tillämpliga säkerhetsåtgärder (se **Utforma Organisationens säkerhetsåtgärder**) din organisation behöver arbeta med härnäst. Detta är ett viktigt underlag för att ledningen ska kunna fatta beslut om aktiviteter och resurser för att införa och förvalta dessa. Att arbeta med listan tillsammans med andra hjälper också dig som CISO att etablera goda samarbeten med de roller som har ansvar för olika säkerhetsåtgärder i din organisation, öka förståelsen för informationssäkerhetsarbetet och syftet med själva säkerhetsåtgärderna.

2.1.2 Analysera organisationens säkerhetsåtgärder

2.1.2.1 Analysera i tre steg

För att kunna avgöra vilka säkerhetsåtgärder som är tillämpliga för organisationen och vilka ni behöver arbeta med härnäst, det vill säga vilka som behöver införas eller förbättras analyserar du dessa i tre steg.

1. **Uttalande om tillämplighet: Vilka säkerhetsåtgärder behöver organisationen?**
   I organisationens Uttalande om Tillämplighet (UoT, på engelska Statement of Applicability, förkortat SoA) utgår ni en sammanställning av interna och externa organisationsövergripande krav (se **Identifiera och analysera Verksamhetsanalys** respektive **Omvärldsanalys**) och från best practice. Den färdiga UoT:n är en sammanställning av de krav och behov på att skydda informationen ni behöver arbeta med. Den hjälper er också att undvika att lägga tid på säkerhetsåtgärder som inte behövs.
2. **Gapanalys: Vilka säkerhetsåtgärder är införda och hur väl fungerar de?**
   Med hjälp av en gapanalys synliggör ni ett eventuellt ”gap” mellan vad ni behöver och vad ni har. Gapanalysen innebär att ni identifierar skillnaden mellan de säkerhetsåtgärder som organisationen behöver ha och de säkerhetsåtgärder som faktiskt finns och fungerar vid analystillfället.
3. **Prioritering – Vilka säkerhetsåtgärder behöver införas eller förbättras först?**
   I det här steget sorterar du listan över säkerhetsåtgärder ni behöver arbeta med så att det blir tydligt vilka brister ni behöver börja med och hur bråttom det är. För att ni ska kunna ta er an att arbeta med att stänga det gap som identifierats i steg 2 behöver de säkerhetsåtgärder som inte är införda eller inte fungerar tillräckligt bra prioriteras utifrån organisationens förutsättningar och den risk bristen medför.

2.1.2.2 Analysens resultat – kunskap om tillämpliga säkerhetsåtgärder och en väg framåt

Med hjälp av övriga analyser inom Identifiera och analysera ger analysen av organisationens säkerhetsåtgärder er en bild av var ni står i ert informationssäkerhetsarbete. Den resulterar också i den prioriterade lista som ger en startpunkt att utgå ifrån för att komma igång och komma vidare i arbetet med att skydda information och de resurser som hanterar information som organisationen behöver.

Om något av underlagen som nämns i denna vägledning ännu inte finns går det bra att fortsätta ändå, men kom ihåg att i sammanfattningen tydligt ange vilka underlag som har funnits tillgängliga och vilka som inte har det. En analys av organisationens säkerhetsåtgärder som bygger enbart på best practice och en individuellt bedömd uppfattning om risk är bättre än ingen analys alls. Var ärlig med din ledning om förutsättningarna och basera dina rekommendationer på vad du vet.

2.1.3 Uttalande om tillämplighet – Vilka säkerhetsåtgärder behöver organisationen?

Det här avsnittet beskriver hur din organisation kommer fram till vilka säkerhetsåtgärder som är lämpliga att införa. Arbetet innefattar att sammanställa säkerhetsåtgärder som vanligen behövs i en organisation med hjälp av best practice och därefter bestämma vilka säkerhetsåtgärder som behövs i organisationen (**UoT**).

Om detta blir för stort i ett första läge kan ett annat sätt vara att börja med att identifiera vilka säkerhetsåtgärder som organisationen redan har införda och därefter jämföra dem mot någon best practice-lista.

2.1.3.1 Förarbete

Som utgångspunkt för din UoT är det bra att utgå från din sammanställda lista av legala krav (**Identifiera och analysera Omvärldsanalys**) och någon lämplig ”best-practice-lista” av säkerhetsåtgärder[1]. Genom att utgå från best practice minskar risken att du missar någon viktig säkerhetsåtgärd.

När de legala kraven uttrycks som att organisationen ska införa ”lämpliga” eller ”tillräckliga” säkerhetsåtgärder går det inte bara att skriva ner kravet ”lämpliga säkerhetsåtgärder” i listan. Du behöver då ta hjälp av vägledningar och best practice-listor för att identifiera de säkerhetskrav som kan avses.

Har du genomfört fler analyser är det bra att ha resultaten från dem med dig när du väljer vilken eller vilka best practice-listor av säkerhetsåtgärder som ni bör utgå ifrån för att få med så många relevanta säkerhetsåtgärder som möjligt.

När du sammanställer dina legala krav med säkerhetsåtgärder från lämpliga best practice-listor kan dessa överlappa. Lägg inte till ett nytt likadant krav utan lägg till en referens till det existerande kravet istället (se **Verktyg Säkerhetsåtgärder**)

Komplettera därefter med krav som är unika för din organisation, det vill säga krav på säkerhetsåtgärder som kommer från interna och externa intressenter. (**Identifiera och analysera Verksamhetsanalys** respektive **Omvärldsanalys**). När du kompletterar din kravlista, kontrollera om dina organisationsspecifika krav redan finns med. Finns kravet redan med lägger du till en referens. Om kravet saknas: komplettera listan.

Det är mycket troligt att de flesta av kraven i din sammanställning vid någon tidpunkt kommer att förändras. Då underlättar det mycket att ha referenser till varifrån kraven i sammanställningen kommer. Fundera igenom om det finns något annat underlag, till exempel från organisationens riskbild (**Identifiera och analysera Riskbild**) som kan visa på behov av säkerhetsåtgärder.

Nu har du en sammanställning av rättsliga krav, säkerhetsåtgärder från best practice, samt krav från interna och externa intressenter.

2.1.3.2 Genomförande

Utifrån din sammanställning av krav, och förslag på säkerhetsåtgärder från best practice behöver du identifiera om alla säkerhetsåtgärder är relevanta i din organisation.

I de flesta fall är nästan alla säkerhetsåtgärder som nu finns i din sammanställning relevanta. Antingen är de relevanta att införa i er organisation eller så är de relevanta att ställa krav på om ni utkontrakterar någon del av er verksamhet, som personalfunktionen (HR), it-

[1] Exempel på best practice är ISO 27001 och 27002, 62443, branschstandarder, tekniska standarder och andra ramverk med säkerhetsåtgärder som beskriver relevanta säkerhetsåtgärder för olika verksamheter eller informationsbehandling.

utveckling eller it-drift. Vid utkontraktering kan vissa säkerhetsåtgärder behöva utföras av både er och den ni utkontrakterat till.

Krav på säkerhetsåtgärder från listan som kan väljas bort för att de inte är tillämpliga är ofta relaterade till en viss informationsbehandling. Exempelvis finns best practice som beskriver säkerhetsåtgärder som är bra att införa om organisationen använder sig av molntjänster. Används inte molntjänster kan alla dessa krav markeras som inte relevanta med förklaringen att molntjänster inte används. Det är enklare att bara markera sådana krav som inte relevanta men ändå behålla säkerhetsåtgärder som inte behövs just nu eftersom era förutsättningar kan ändras snabbt.

Överväg att också dokumentera varför sammanställningen innehåller en viss säkerhetsåtgärd om det inte är uppenbart varför, som till exempel när en säkerhetsåtgärd bara behövs i en del av en verksamhet, en informationsbehandling eller motsvarande.

För att säkerställa att du förstått vilka säkerhetsåtgärder organisationen behöver kan det vara bra att stämma av dina antaganden med roller som har djupare kännedom om en viss säkerhetsåtgärd. Ett sätt att identifiera dessa roller kan vara att se vem som äger de styrdokument som kan tänkas beröras av säkerhetsåtgärden.

2.1.3.3 Resultat – de säkerhetsåtgärder som organisationen behöver

Nu har du en sammanställning av de säkerhetsåtgärder som är relevanta för din organisation, en beskrivning av varför de behövs och varifrån de kommer. Sammanställningen är utgångspunkten för din gapanalys.

2.1.4 Gapanalys - Vilka säkerhetsåtgärder är införda och hur väl fungerar de?

I gapanalysen kontrollerar du vilka av säkerhetsåtgärderna i din sammanställning som är införda i din organisation och hur väl de fungerar. Att en säkerhetsåtgärd är införd betyder inte att den fungerar väl. Därför behöver du förutom att ange att säkerhetsåtgärden är införd också analysera hur väl den fungerar (se **Utforma Organisationens säkerhetsåtgärder)**.

2.1.4.1 Förarbete

Du förbereder din gapanalys genom att ta reda på vilka säkerhetsåtgärder som ni redan har infört och vilka ni planerar att införa men som ännu inte är på plats. Säkerhetsåtgärderna bör vara dokumenterade i interna regelverk, men de är inte alltid nedskrivna utan kan finnas införda på annat sätt och kunskapen om det finns hos olika roller i organisationen. Ofta behöver du både ett internt regelverk, för att verifiera att en åtgärd är införd, och en person, som kan verifiera hur väl den fungerar. Du kan utifrån organisationsstruktur, roller och ansvar troligen identifiera vilken roll som kan veta mest om eller redan är ansvarig för en viss säkerhetsåtgärd (se vidare **Utforma Organisationens arbete med säkerhetsåtgärder**).

Om säkerhetsåtgärden redan följs upp löpande (se **Följa upp och förbättra Organisationens säkerhetsåtgärder**) finns det information i den dokumentationen som kan ge en indikation på hur väl säkerhetsåtgärden fungerar.

Dokumentera i din sammanställning var du hittat informationen om de olika säkerhetsåtgärderna, om du inte hittar någon information alls och vilka personer du kan fråga och senare har frågat för att få den information du saknar.

2.1.4.1.1 Bedömningskriterier

Bedömningskriterierna använder du för att bedöma hur väl en säkerhetsåtgärd fungerar. De flesta säkerhetsåtgärder kan fungera på en skala någonstans mellan ”finns inte alls och fungerar därmed inte” och ”är införda, fungerar bra och anpassas vid behov”. Det finns modeller som kan användas för att bedöma hur väl en säkerhetsåtgärd fungerar. Inspiration gällande bedömningskriterier kan hämtas från till exempel MSB:s Cybersäkerhetskollen, nivåerna i MSB:s Mognadsdialog eller andra modeller som till exempel Capability Maturity Model (CMM).

Exempel på egna kriterier kan vara:

1. Förstått behovet
2. Utformat säkerhetsåtgärden
3. Infört
4. Följer upp och förbättrar regelbundet.

eller

1. Fungerar 0–50 procent tillfredsställande.
2. Fungerar 50–75 procent tillfredställande.
3. Fungerar tillräckligt bra.

Placera dina kriterier i ett lämpligt antal nivåer. Tre nivåer kan räcka, medan tio troligen är för många.

2.1.4.1.2 Planera analysen

Att genomföra gapanalys på alla säkerhetsåtgärder själv och vid ett tillfälle bli sannolikt för omfattande. För att underlätta vidare arbete kan du kategorisera dina säkerhetsåtgärder utifrån till exempel

- vem du bedömt har mer kännedom om hur väl en säkerhetsåtgärd fungerar (se vidare om kategorisering i **Utforma Organisationens säkerhetsåtgärder**)
- om du utifrån övriga analysresultat själv kan göra en ungefärlig bedömning av vilka säkerhetsåtgärder som kan vara viktigare än andra att börja med.

Gör sedan en plan för vilka säkerhetsåtgärder som bör analyseras, när – och med vem.

2.1.4.2 Genomförande

Det finns flera sätt att genomföra en gapanalys. Vad som fungerar bäst i din organisation kan variera över tid och sätten kan kombineras. Samma säkerhetsåtgärd kan behöva analyseras vid flera tillfällen för att få fram all nödvändig information.

Om uppföljning sker och ger tillräckliga svar på hur väl en säkerhetsåtgärd fungerar kan svaren överföras direkt till gapanalysen. Andra sätt kan vara till exempel att boka en intervju eller att bjuda in till en workshop. Ibland finns det inte någon ytterligare information att tillgå, då är din bästa gissning bättre än ingenting.

Börja gapanalysen genom att läsa igenom säkerhetsåtgärden och varför den är med. Därefter svarar du eller ni gemensamt på följande frågor:

- Stämmer det att säkerhetsåtgärden är relevant för organisationen (UoT:n är korrekt)?

- Utifrån bedömningskriterierna: är säkerhetsåtgärden införd? Om den är införd: hur väl fungerar den?
- Om åtgärden inte är införd eller inte fungerar tillräckligt väl, gör om möjligt ett snabbt överslag på vilken resursåtgång som krävs för att införa eller förbättra säkerhetsåtgärden så att den blir tillräckligt bra. Detta är ett bra underlag att ha med till nästa analys --prioriteringen av vilka åtgärder som behöver arbetas med först. (se **Utforma Organisationens säkerhetsåtgärder**).

Observera att du kan välja att gå olika djupt när du kontrollerar hur väl en säkerhetsåtgärd fungerar. Hur djupt du går kan bero på till exempel hur mycket tid du har, hur viktigt säkerhetsåtgärden är. Vi ger här ett exempel på hur man kan identifiera om en säkerhetsåtgärd finns och hur väl den fungerar på en relativt detaljerad nivå.

Säkerhetsåtgärden: Byt ut förinställda lösenord innan driftsättning.

Frågor som kan ställas för att förstå om säkerhetsåtgärden finns och fungerar.

- Finns det ett internt regelverk som säger att alla förinställda lösenord ska bytas till ett lösenord med godkänd komplexitet och längd innan driftsättning?
- Följer alla relevanta verksamheter i organisationen detta regelverk?
- Finns det en kontrollpunkt att lösenord är utbytta, innan ett it-system får driftgodkännande?
- Genomförs säkerhetstester för att kontrollera att förinställt lösenord inte finns kvar?
- Tas beslut om driftgodkännande först när säkerhetstester har visat att lösenordet är bytt?

Var särskilt noga med att dokumentera hur du har kommit fram till slutsatserna så att resonemanget alltid är transparent. Det är stor skillnad på kvalitet i resultat som bygger på noga genomförd årlig uppföljning respektive om du har behövt uppskatta. Identifierar du brister som är så allvarliga att du bedömer att de behöver åtgärdas direkt: kontakta riskägaren (se **Utforma Organisationens säkerhetsåtgärder** respektive **Risk** och **Organisation**).

2.1.4.3 Resultat – en organisationsövergripande gapanalys

Resultatet är att du kompletterat din UoT-lista med bedömningar av om organisationsövergripande säkerhetsåtgärder är införda och med en uppgift om hur väl de fungerar.

2.1.4.3.1 Utvärdera arbetet med gapanalysen

Reflektera över hur arbetet med gapanalysen har gått. Var den valda metoden, intervju/workshop bra? Hur fungerade de valda kriterierna? Vad kan göras annorlunda till nästa gång?

2.1.5 Prioritering – Vilka säkerhetsåtgärder behöver införas eller förbättras först?

Du har analyserat hur väl de olika säkerhetsåtgärderna fungerar och du har eventuellt fått förslag på hur man kan åtgärda de brister som identifierats. Nu behöver du bedöma i vilken ordning de säkerhetsåtgärder som brister behöver åtgärdas och hur brådskande det är.

2.1.5.1 Förarbete

Utgå gärna från organisationens riskbild (**Identifiera och analysera Riskbild**) och kategorisera säkerhetsåtgärderna utifrån vilka risker de motverkar. Informationen du sammanställer kommer då att innehålla bedömd nivå av hur väl säkerhetsåtgärden är införd och fungerar samt vilken risk säkerhetsåtgärden motverkar. Om ni saknar en riskbild eller vill komplettera med en riskanalys, kontakta personer du vill ha med i en sådan riskbedömning (se **Använda Riskanalys**)

Fortsättning på exemplet gällande säkerhetsåtgärden att byta ut förinställda lösenord.

- Säkerhetsåtgärden har i gapanalysen bedömts vara på ”nivå 2. Fungerar 50–75 procent tillfredsställande”. Det finns ett internt regelverk, en riktlinje, som säger att lösenorden ska bytas men inga instruktioner för byte inför driftsättning och inga tester som kontrollerar att förinställda lösenord är utbytta. De tekniker som deltog i workshopen uppger att de alltid byter förinställda lösenord och att de bedömer att alla gör det.
- Det är bedömt i organisationens riskbild att hot mot it-miljön där sårbarheter utnyttjas ökar och att risken är hög att drabbas av försök att infektera it-miljön eller ta över it-system.

2.1.5.2 Genomförande

Fortsätt med att analysera säkerhetsåtgärdernas brister utifrån risk. Använd organisationens riskanalysmodell och gör riskbedömning för varje säkerhetsåtgärd. Gå igenom listan med säkerhetsåtgärder och sätt prioritet på dessa utifrån risk. Börja med de säkerhetsåtgärder som noterats motverka de allvarligaste riskerna. Gå sedan vidare med de säkerhetsåtgärder som motverkar flest risker.

Riskbilden ger en uppfattning om vilket hot som föreligger och hur allvarliga de är för organisationen. Gapanalysen visar hur väl säkerhetsåtgärden är införd och fungerar. Riskanalysen anger bristens eller sårbarhetens konsekvens.

Fortsättning på exemplet gällande säkerhetsåtgärden att byta ut förinställda lösenord.

Om lösenord inte bytts ut kan obehöriga använda standardlösenord för att komma åt vår it-miljö och infektera eller ta över den. Konsekvenser kan bli att vår information blir åtkomlig för obehöriga, ändras utan att vi känner till det eller att vi själva inte kan nå vår information.

Ibland finns det inte tillräcklig information för att kunna avgöra vilka säkerhetsåtgärder som blir viktigast att prioritera, då är din bästa gissning bättre än ingenting – var transparent med hur du kommit fram till resultatet.

Om du inte redan har regelbunden kontakt med samordnare för andra närliggande områden, såsom dataskydd, samhällsskydd och beredskap, säkerhetsskydd, är det läge att stämma av dina iakttagelser och få återkoppling på att resultatet är rimligt. Fråga också om dessa roller har andra ingångsvärden som kan påverka prioriteringen av i vilken ordning arbetet med att förbättra säkerhetsåtgärderna bör genomföras.

2.1.5.3 Resultat – ett beslutsunderlag för vidare åtgärder

Resultatet blir en prioriterad lista som kan användas för din rekommendation av vilka säkerhetsåtgärder som behöver förbättras och i vilken ordning. Stäm av prioriteringen och resursbehoven med de som berörs av de åtgärder som prioriteras den närmaste tiden, innan du lämnar beslutsunderlaget till ledningen (se **Utforma Handlingsplan**).

Du kan hamna i en situation där du har en prioritering av vilka säkerhetsåtgärder som behöver införas först och kunskap om att resurser att göra det inte finns tillgängliga. I det läget har du möjlighet att införa flera säkerhetsåtgärder i övergripande styrdokument, men inte införa dem i sin helhet.

I dessa lägen är det bra att bedöma

1. värdet av att förbereda styrdokument för att senare när resurser finns kunna införa dem mot att lägga tid på att införa andra säkerhetsåtgärder fullt ut.
2. om du prioriterar bättre om du använder tiden till att arbeta med att planera och följa upp informationssäkerhetsarbete och göra egna förbättringar och effektiviseringar av arbetet.

2.1.5.4 Förvalta säkerhetsåtgärder

Se över organisationens UoT, gapanalys och prioriteringen årligen, förslagsvis efter uppdatering av Verksamhetsanalys och Omvärldsanalys. Uppdatera också relevanta delar vid till exempel organisationsförändringar, förändringar i reglering och andra referenser till krav, utkontraktering, större förändringar i it-miljön. Se till att versionshantera dina förändringar så att du kan gå tillbaka och se vilka ändringar som gjorts.