Myndigheten för samhällsskydd och beredskap

Exempel - klassningsmatris C

Det här är ett fiktivt exempel på en klassning av informationstillgångar i en statlig myndighet. Exemplet hör till MSB:s Metodstöd för systematiskt informationssäkerhetsarbete.

Inledning

En myndighet var i behov av att uppdatera sin klassningsmodell av flera olika anledningar. Flertalet av myndighetens avdelningar tyckte inte att modellen fungerade som ett stöd för att klassa information, myndigheten bedömde att de hade en förändrad hotbild och flera avdelningar hade fått nya arbetsuppgifter med nya informationsmängder.

Arbetet bedrevs av myndighetens säkerhetsavdelning, i samverkan med de andra avdelningarna. För att kunna förstå de problem som verksamheten upplevde med den nuvarande modellen, de krav på säker informationshantering verksamheten har och de konsekvenser som kan inträffa vid bristande informationshantering genomfördes flera workshops med alla avdelningar.

Men hjälp av detta underlag togs en klassningsmodell, bestående av en klassningsmatris och tillhörande stödmaterial, fram av säkerhetsavdelningen och skickades sedan ut på remiss till den övriga verksamheten. Efter att inkomna synpunkter hanterats så justerades delar av modellen för att bättre passa myndighetens behov och förutsättningar.

Nästa steg i arbetet var att genomföra ett pilotprojekt där klassningsmodellen testades i verksamheten. Tre av HR-avdelningens informationsmängder valdes ut att ingå i pilotprojektet.

Mer om hur modellen togs fram

Under de workshop-tillfällen som genomfördes med alla avdelningar framkom det att den klassningsmodell som fanns var otydlig och den användes därför inte av flera verksamheter. Många i verksamheten förstod inte hur och varför information ska klassas. Flera verksamheter ansåg också att konsekvensnivåerna behövde förtydligas.

Myndigheten hanterar stora mängder information som innehar olika behov av skydd utifrån interna och externa krav på konfidentialitet, riktighet och tillgänglighet. Viss verksamhet har dessutom utifrån den säkerhetsskyddsanalys som genomförts visat sig vara säkerhetskänslig och myndigheten hanterar också säkerhetsskyddsklassificerade uppgifter.

Den gamla klassningsmodellen innehöll tre konsekvensnivåer där skillnaderna mellan nivåerna var svåra att förstå och där det mesta av organisationens information bedömdes hamna i den mellersta nivån, även om verksamheten ansåg att konsekvenserna av felaktig informationshantering skiljde sig väldigt mycket åt. Då det

fanns brister i utformningen av de skyddsnivåer som var kopplande till klassningsmodellens tre konsekvensnivåer och dessutom brister i arbetssätt gällande riskbedömning valde verksamheterna att införa de säkerhetsåtgärder som föreslogs för en viss skyddsnivå utan riskbedömning. Informationen riskerade därför ofta att få antingen ett för lågt skydd eller ett för högt skydd, med omotiverat höga kostnader som följd.

Utifrån de workshops och analyser som genomfördes bedömdes att en klassningsmatris med fyra konsekvensnivåer skulle vara mer ändamålsenligt för myndigheten. Det framkom också att det var viktigt att det fanns bra stöd för hur informationen ska klassas.

Då myndigheten hanterar information som omfattas av säkerhetsskyddslagen var det viktigt att klassningsmodellen kunde hantera det. Detta löstes genom att all information klassades utifrån de konsekvensnivåer som organisationen beslutat och om informationen bedöms omfattas av säkerhetsskyddslagen klassificeras den därefter i en av de fyra säkerhetsskyddsklasserna med hjälp av organisationens säkerhetsskyddschef.

Eftersom myndigheten saknade en fungerande modell för riskbedömning togs en matris med konsekvenskategorier uppdelade i nivåer fram tillsammans med nyanställd ansvarig för myndighetens modell för riskbedömning som fungerar både för informationssäkerhetsarbetet och inom andra områden där risker bedöms. Matrisen för riskbedömning som togs fram visas nedan:

Konsekvenskategorier uppdelade i nivåer för riskbedömning och klassning

	Verksamhet	Medarbetare	Ekonomi	Rättsliga krav och avtalskrav
Allvarlig	Kärnverksamheten har inte tillräckligt med personal (mindre än 70% på plats) eller personalen kan inte påbörja sin arbetsuppgift inom 60 minuter. Stödverksamheter har inte tillräckligt med personal (mindre än 30% på plats) eller kan inte stödja kärnverksamheten på mer än en (1) månad.	Allvarlig fysisk eller psykisk skada. Kan leda till ett eller ett flertal dödsfall. Mycket lång sjukfrånvaro som är svårt att återhämta sig från.	En förlust på över 15% av budget.	Riskerar att inte skydda information enligt OSL (förutom säkerhetsskydd), Dataskyddsförordningen (GDPR) känsliga personuppgifter, eller inte följa grundlag. Brott mot avtal som ger motsvarande konsekvens.
Betydande	Kärnverksamheten har inte tillräckligt med personal (mindre än 80% på plats) eller personalen kan inte påbörja sin arbetsuppgift inom 30 minuter. Stödverksamheter har inte tillräckligt med personal (mindre än 50% på plats) eller kan inte stödja kärnverksamheten på mer 2 veckor.	Betydande fysisk eller psykisk skada. Lång sjukfrånvaro.	En förlust på mellan 10-15% av budget.	Riskerar att inte följa Dataskyddsförordningen (GDPR) enstaka känsliga personuppgifter, eller annan lag med motsvarande konsekvens. Brott mot avtal som ger motsvarande konsekvens.
Måttlig	Kärnverksamheten har inte tillräckligt med personal (mindre än 90% på plats) eller personalen kan inte påbörja sin arbetsuppgift inom 15 minuter. Stödverksamheter har inte tillräckligt med personal (mindre än 70% på plats) eller kan inte stödja kärnverksamheten på mer än en (1) vecka.	Viss fysisk eller psykisk skada. Kortare sjukfrånvaro.	En förlust på mellan 5-10% av budget.	Riskerar att inte följa Dataskyddsförordningen (GDPR) eller annan lag med motsvarande konsekvens. Brott mot avtal som ger motsvarande konsekvens.
Försumbar	Kärnverksamheten har inte tillräckligt med personal (mindre än 95% på plats) eller personalen kan inte påbörja sin arbetsuppgift inom mindre än 15 minuter. Stödverksamheter har inte tillräckligt med personal (mindre än 90% på plats) eller kan inte stödja kärnverksamheten på upp till en (1) vecka.	Obetydlig fysisk eller psykisk skada. Mycket kort sjukfrånvaro.	En förlust på upp till 5% av budget.	Riskerar inte att bryta mot lag, förordning eller ingångna avtal.

Organisationens klassningsmatris

	Konfidentialitet	Riktighet	Tillgänglighet
Sveriges säkerhet **Säkerhetsskydd**	Information som omfattas av Säkerhetsskyddslagen. Särskild hantering.	Information som omfattas av Säkerhetsskyddslagen. Särskild hantering.	Information som omfattas av Säkerhetsskyddslagen. Särskild hantering.
Allvarlig	**K4** Se nivå 4 i konsekvensbeskrivningen.	**R4** Se nivå 4 i konsekvensbeskrivningen.	**T4** Se nivå 4 i konsekvensbeskrivningen.
Betydande	**K3** Se nivå 3 i konsekvensbeskrivningen.	**R3** Se nivå 3 i konsekvensbeskrivningen.	**T3** Se nivå 3 i konsekvensbeskrivningen.
Måttlig	**K2** Se nivå 2 i konsekvensbeskrivningen.	**R2** Se nivå 2 i konsekvensbeskrivningen.	**T2** Se nivå 2 i konsekvensbeskrivningen.
Försumbar	**K1** Se nivå 1 i konsekvensbeskrivningen.	**R1** Se nivå 1 i konsekvensbeskrivningen.	**T1** Se nivå 1 i konsekvensbeskrivningen.

Testa klassningsmodellen i pilotprojekt

För att testa den nya klassningsmodellen valdes vissa delar av HR-avdelningens verksamhet ut som lämpligt pilotprojekt. Både inventeringen av informationen och informationsklassningen genomfördes i workshopform. De som deltog i workshopen var både chefer och handläggare från HR-avdelningen. Myndighetens CISO ledde workshopen samt vägledde deltagarna i informationsklassningsmetodik och myndighetens arbetssätt för informationsklassning.

De informationsmängder som valdes ut som klassningsobjekt för pilotprojektet fanns inom huvudområdena löneutbetalning, rekrytering och medarbetaruppgifter. De informationsmängder som klassades i pilotprojektet visas nedan:

Informationsmängd	Informationstyper
Löneutbetalning	Namn, hemadress, personnr, anställningsnummer, befattning, BESTA-kod, lön, ev. skyddade identiteter.
Rekrytering	Namn, personnr, adress, tidrapportering, anställningsnummer, frånvaro, lön, kontonummer, ev. skyddade identiteter.
Medarbetaruppgifter	Behovsanalys, kravställning, rekryterande chef, ansökningar (innehållandes namn, cv och personligt brev).

Organisationen beslöt att klassa varje ingående informationstyp och därefter klassa dem tillsammans som en informationsmängd. På så sätt får de både en klassning för hela informationsmängden, som sedan kan få tillräcklig skydd, och en klassning för varje ingående informationstyp då dessa ofta hanteras som egen informationsmängd. Beslutet att göra på det här sättet baserades på de behov som verksamheten i fråga har av att kunna bedöma skyddsbehovet för varje informationstyp separat i olika sammanhang.

Information och resultat av klassning i pilotprojektet

<table>
<tr><th>Informationsmängd</th><th>Informationstyper</th><th>K-R-T</th></tr>
<tr><td>Medarbetaruppgifter</td><td>Namn, hemadress personnr, anställningsnummer, befattning, BESTA-kod, lön, ev. skyddade identiteter.

<table>
<tr><th>Informationstyp</th><th>K-R-T</th><th>Kommentar</th></tr>
<tr><td>Enskilda namn</td><td>2-2-1</td><td>Vissa grupper av namn K=3. T=2, Alla anställda K=3</td></tr>
<tr><td>Hemadress</td><td>3-1-1</td><td>Skyddad identitet K=4.</td></tr>
<tr><td>Personnummer</td><td>3-2-2</td><td></td></tr>
<tr><td>Anställningsnummer</td><td>1-2-2</td><td></td></tr>
<tr><td>Befattning</td><td>1-1-1</td><td></td></tr>
<tr><td>BESTA-kod</td><td>1-2-2</td><td></td></tr>
<tr><td>Lön</td><td>1-2-2</td><td></td></tr>
<tr><td>Skyddad identitet</td><td>4-4-1</td><td></td></tr>
</table>
</td><td>4-4-2</td></tr>
</table>

<table>
<tr><td>Löneutbetalning</td><td>Namn, personnr, hemadress, tidrapportering, anställningsnummer, frånvaro, lön, kontonummer, ev. skyddade identiteter.

<table><tr><th>Informationstyp</th><th>K-R-T</th><th>Kommentar</th></tr><tr><td>Enskilda namn</td><td>2-2-1</td><td>Se motsvarande under ”Medarbetaruppgifter”</td></tr><tr><td>Personnummer</td><td>3-2-2</td><td></td></tr><tr><td>Hemadress</td><td>3-1-1</td><td>Se motsvarande under ”Medarbetaruppgifter”</td></tr><tr><td>Tidrapportering</td><td>1-3-1</td><td></td></tr><tr><td>Anställningsnummer</td><td>1-2-2</td><td></td></tr><tr><td>Frånvaro</td><td>4-1-1</td><td></td></tr><tr><td>Lön</td><td>1-2-2</td><td></td></tr><tr><td>Kontonummer</td><td>4-3-1</td><td></td></tr><tr><td>Skyddad identitet</td><td>4-4-1</td><td></td></tr></table></td><td>4-4-2</td></tr>
<tr><td>Rekrytering</td><td>Behovsanalys, kravställning, rekryterande chef, ansökningar (innehållandes namn, cv och personligt brev).

<table><tr><th>Information</th><th>K-R-T</th><th>Kommentar</th></tr><tr><td>Behovsanalys</td><td>1-3-2</td><td></td></tr><tr><td>Kravställning</td><td>1-3-2</td><td></td></tr><tr><td>Rekryterande chef</td><td>1-1-1</td><td></td></tr><tr><td>Ansökningar</td><td>2-1-2</td><td></td></tr></table></td><td>2-3-2</td></tr>
</table>

Resultatet från workshopen dokumenterades och informationsägaren, chefen-HR, beslöt att resultatet skulle diskuteras på arbetsplatsträffar på varje enhet för att kunna rätta till eventuella konsekvenser som missats. Efter det fastställdes klassningen.

Hantering av resultatet

Säkerhetsåtgärder i skyddsnivåer

I samband med att klassningsmodellen uppdaterades valde myndigheten även att uppdatera sin kravmassa av säkerhetsåtgärder för it-system och övrig informationshantering. Säkerhetsåtgärderna delades upp i skyddsnivåer motsvarande klassningsmatrisens konsekvensnivåer. För information som klassats till en viss nivå valdes säkerhetsåtgärderna i kravmassan utifrån klassningsresultatet och genomförd riskbedömning. Det innebar att säkerhetsåtgärder kunde tas bort eller tillkomma utifrån resultatet från riskbedömningen. När klassningen it-system genomfördes ingick ingående informations klassningsresultat och bedömningen huruvida aggregering eller ackumulering (om resultatet av den sammanlagda informationen ger ett högre skyddsvärde än de ingående informationsmängderna för sig) påverkade it-systemets skyddsnivå.

Efterverkningar i organisationen

Efter pilotprojektet beslutades klassningsmatrisen med tillhörande stödmaterial för att genomföra informationsklassning. Successivt började även andra verksamheter klassa sin information enligt den nya klassningsmodellen. Flera utbildningstillfällen genomfördes där myndighetens CISO utbildade personer i de olika verksamheterna som sedan skulle stödja operativt med informationsklassningar.

Som ett resultat av att den nya klassningsmodellen togs fram i samverkan med myndighetens olika verksamheter och därför anpassades efter myndighetens specifika behov ansågs den fungera bättre i verksamheten och fler använde den för att klassa sin information än vad den gamla klassningsmodellen gjorde.