Myndigheten för samhällsskydd och beredskap

Exempel klassningsmatris A

Det här är ett fiktivt exempel på en klassning av information i ett privat företag. Exemplet hör till MSB:s Metodstöd för systematiskt informationssäkerhetsarbete.

Bakgrund

Ett medelstort företag inom bevaknings- och säkerhetsbranschen som jobbar främst med stationär och patrullerande bevakning för privata företag men även med brandskydd samt larminstallationer. Företagets ledning har beslutat att införa ett ledningssystem för informationssäkerhet som ska baseras på SS-EN ISO/IEC 27001. I och med att arbetet med informationssäkerhet startades anställdes också en CISO.

Under arbetet med gapanalysen framkom bland annat behov av att ta fram och införa en klassningsmodell för att klassa den information som företaget hanterar. Till klassningsmatrisen framkom behov av att ta fram och införa rutiner, såsom arbetssätt för informationsklassning, hanteringsregler för medarbetare och säkerhetsåtgärder i skyddsnivåer för it-system motsvarande konsekvensnivåerna i klassningsmatrisen. Arbetet med att ta fram en klassningsmodell och testa den på viss del av de informationstillgångar företaget har berörs i detta exempel.

Inventering av information

Företagets CISO höll i en workshop för att inventera vilken information de hanterar. Representanter från de olika verksamheterna deltog i workshopen.

Under inventeringen identifierades fyra informationsmängder som ansågs vara de viktigaste. Dessa var kunduppgifter, information om larminstallationer och bevakningsuppdrag, medarbetaruppgifter samt uppgifter om schemaläggning.

Informationen lagras i två inköpta it-system som förvaltas av it-avdelningen. Det ena it-systemet hanterar kunduppgifter och de larminstallationer kunderna eventuellt har, det andra it-systemet hanterar medarbetaruppgifter samt information gällande schemaläggning.

Konsekvensnivåer

För att ta fram en klassningsmatris genomfördes workshop med företagets olika verksamheter i syfte att få fram deras krav på klassningsmatrisen. Enligt den bedömning som gjordes ansågs de fyra nivåer som redan var definierade i riskhanteringsmodellen fungera bra.

Tabell 1 – Företagets riskmatris

	Verksamhetsförmåga	Förtroende	Ekonomisk förlust
Allvarlig	Mer än 20% av larminstallationerna fungerar inte. Kan inte utföra bevakningsuppdrag enligt ingångna avtal som ger skadestånd på mer än 20% av avtalsvärdet. Mer än 20% av kunderna får sådana anmärkningar vid tillsyn av brandskydd att de säger upp avtal.	Dödsfall eller skada som leder till en invaliditetsgrad på minst 50% på egen personal. Dödsfall eller allvarliga skador på person vid ingripande som leder till omfattande negativ publicitet. Inbrott och bränder i objekt där vi har engagemang fram till vi kan avskriva ansvar.	Förlust på mer än 2 miljoner eller 20% av kontraktsvärdet eller minskad omsättning med mer än 20%.
Betydande	Mer än 10% av larminstallationerna fungerar inte. Kan inte utföra bevakningsuppdrag enligt ingångna avtal som ger skadestånd på mer än 10% av avtalsvärdet. Mer än 10% av kunderna får sådana anmärkningar vid tillsyn av brandskydd att de säger upp avtal.	Skada som leder till en invaliditetsgrad på 20-50% på egen personal. Skada på person vid ingripande som leder till negativ publicitet i mindre omfattning. Om våra bristande insatser gällande brandskydd, larminstallationer och bevakning bidragit till kundens skador.	Förlust på mer än 1 miljon eller 10-20% av kontraktsvärdet eller minskad omsättning med 10-20%.
Måttlig	Mer än 5% av larminstallationerna fungerar inte. Kan inte utföra bevakningsuppdrag enligt ingångna avtal som ger skadestånd på mer än 5% av avtalsvärdet. Mer än 5% av kunderna får sådana anmärkningar vid tillsyn av brandskydd att de säger upp avtal.	Skada som leder till en invaliditetsgrad på mindre än 20% på egen personal. Personal åter i tjänst inom 3 månader. Skada på person vid ingripande som leder till enstaka kortvarig negativ publicitet. Våra larminstallationer, brandskydd och bevakningsinsatser har inte bidragit till kundens skador men vi behöver ändå göra insatser för att behålla kundens förtroende.	Förlust på mer än 500 000 kronor eller 5-10% av kontraktsvärdet eller minskad omsättning med 5-10%..
Obetydlig/Försumbar	Mindre än 5% av larminstallationerna fungerar inte. Kan inte utföra bevakningsuppdrag enligt ingångna avtal som ger skadestånd på mindre än 5% av avtalsvärdet. Mindre än 5% av kunderna får sådana anmärkningar vid tillsyn av brandskydd att de säger upp avtal.	Obetydande skada på egen personal. Åter i tjänst inom ett par dagar. Mindre skada på person vid ingripande som leder till enskaka upprörda inlägg i exempelvis sociala medier. Larminstallationer, brandskydd och bevakningsinsatser har inget med kundens skador att göra. Enskata extrainsatser behövs för att behålla kundens förtroende.	Förlust på minde än 500 000 kronor eller 5% av kontraksvärdet eller minskad omsättning på mindre än 5%.

Klassning av information

Klassningsmatrisen visualiseras nedan.

Tabell 2 – företagets klassningsmatris

	Nivå	Konfidentialitet	Riktighet	Tillgänglighet
3	**Allvarlig**	**K3** **Mycket känslig** information där förlust av konfidentialitet kan leda till allvarliga konsekvenser för verksamhetens förmåga, förtroende eller skonomisk förlust.	**R3** Information där förlust av riktighet kan leda till allvarliga konsekvenser för verksamhetens förmåga, förtroende eller ekonomisk förlust.	**T3** Information där förlust av tillgänglighet kan leda till allvarliga konsekvenser för verksamhetens förmåga, förtroende eller ekonomisk förlust.
2	**Betydande**	**K2** **Känslig** information där förlust av konfidentialitet kan leda till höga konsekvenser för verksamhetens förmåga, förtroende eller ekonomisk förlust.	**R2** Information där förlust av riktighet kan leda till höga konsekvenser för verksamhetens förmåga, förtroende eller ekonomisk förlust.	**T2** Information där förlust av tillgänglighet kan leda till höga konsekvenser för verksamhetens förmåga, förtroende eller ekonomisk förlust.
1	**Måttlig**	**K1** **Intern** information där förlust av konfidentialitet kan leda till måttliga konsekvenser för verksamhetens förmåga, förtroende eller ekonomisk förlust.	**R1** Information där förlust av riktighet kan leda till måttliga konsekvenser för verksamhetens förmåga, förtroende eller ekonomisk förlust.	**T1** Information där förlust av tillgänglighet kan leda till måttliga konsekvenser för verksamhetens förmåga, förtroende eller ekonomisk förlust.
0	**Obetydlig eller försumbar**	**K0** **Öppen** information där förlust av konfidentialitet inte kan leda till några konsekvenser för verksamhetens förmåga, förtroende eller ekonomisk förlust.	*Krav finns alltid att information ska vara riktig, bedöms ej.*	*Krav finns alltid att information ska vara tillgänglig, bedöms ej.*

Även informationsklassningen genomfördes under en workshop, som leddes av företagets CISO, tillsammans med representanter från de olika verksamheterna där identifierade informationsmängder hanteras.

Alla informationstyper identifierades och grupperades i fyra informationsmängder och sedan genomfördes en klassning av de definierade informationsmängderna.

Tabell 3 - inventering och klassning av information

Informationsmängder	Informationstyper	K-R-T
Kunduppgifter	Organisationsnummer, kontaktuppgifter, brandsskyddsplaner, typ av kund.	2-2-3
Larminstallationer och bevakningsuppdrag	Larmritningar, bevakningsåtgärder, scheman för bevakning/rondering, kundens larmkontaktuppgifter	3-2-3
Medarbetaruppgifter	Namn, personnr, adress, utbildning, kompetens, titel, lön.	2-2-1
Schemaläggning	Scheman, namn, personnr, beskrivning.	2-2-1

Klassning av it-system

Klassning av de it-system som hanterar företagets information genomfördes i samband med informationsklassningen. Vid klassning av it-systemen tog man hänsyn till aggregerad och ackumulerad information och om detta kunde leda till en högre klassning än den som gjorts för de olika informationsmängderna ovan. Tabell 3 visar klassningen av it-systemen samt vilken information som hanteras i dem.

Tabell 4 – resultat av klassning av it-system

System	Informationstyp	K-R-T
1	Organisationsnummer, kontaktuppgifter, larmritningar, brandsskyddsplaner, bevakningsåtgärder, bevakningscheman, rutter, kundens larmkontaktuppgifter	3-2-3
2	Scheman, , namn, personnr, beskrivning, adress, utbildning, kompetens, titel, lön.	3-2-2

Bedömningen som genomfördes kom fram till att det i nuläget inte fanns skäl att klassa it-systemen högre än den klassning som motsvarar det högsta värdet i ingående informationsmängd fått i klassningen av informationsmängder. Under workshopen kom man dock fram till att om företaget får flera kunder eller mer personal kan klassningen av it-systemen komma att bli högre. Systemägaren får i uppdrag att bevaka mängden information i systemen.

Användning av resultatet

Efter att klassningsmodellen testats började ett större klassningsprojekt där all företagets information och alla it-system inventerades och klassades.

I samband med att klassningsmodellen togs fram och testades genomfördes också ett arbete med att ta fram säkerhetsåtgärder baserat på SS-EN IEC/ISO 27002. De säkerhetsåtgärder som berörde it-system samlades i skyddsnivåer motsvarande konsekvensnivåerna i klassningsmodellen.

Företaget tog också fram ett antal styrdokument, såsom riktlinjer för vilket ansvar systemägare och informationsägare har, för när och hur klassning ska genomföras, samt hanteringsregler för information som riktades till alla anställda.

För att öka förståelse och kunskap kring klassning och informationssäkerhet i stort genomfördes olika typer av utbildningar riktade mot olika målgrupper i företaget såsom anställda och chefer i deras roll som informationsägare och systemägare.