Granskning av informationssäkerhet

Rapport

Ludvika kommun och kommunala bolag

KPMG AB

2023-10-20

Antal sidor 23

Antal bilaga 1

Ludvika kommun och kommunala bolag
Granskning av informationssäkerhet

2023-10-20

Innehållsförteckning

1 Sammanfattning

KPMG har av Ludvika kommuns förtroendevalda revisorer och lekmannarevisorer fått i uppdrag att genomföra en granskning av kommunstyrelsens, utvalda nämnders och bolags informationssäkerhet. Uppdraget ingår i revisionsplanen för år 2023.

Syftet med granskningen har varit att bedöma om kommunstyrelsen, nämnder och bolagsstyrelser bedriver ett systematiskt informationssäkerhetsarbete så att det sker på ett ändamålsenligt sätt.

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen, granskade nämnder och bolagsstyrelser inte säkerställt ett systematiskt och ändamålsenligt informationssäkerhetsarbete.

Vi bedömer att ledningssystemets omfattning inte är i paritet med varken de informationstillgångar som hanteras av kommunkoncernen, eller med vad som rekommenderas av MSBs metodstöd. Vi saknar styrande dokument som tydliggör ansvar, krav samt beskrivning över hur informationssäkerhetsarbetet ska genomföras.

Det saknas en etablerad klassningsmodell som utgör grund och vägledning i klassningsarbetet och det riskanalysarbete som genomförs anser vi inte vara tillräckligt för att kunna identifiera säkerhetsåtgärder i den utsträckning som behövs i syfte att skydda kommunens och bolagens informationstillgångar.

Ansvariga nämnder och styrelser har inte säkerställt en tillräcklig säkerhetskultur. Vi anser därmed att det finns behov av utbildningsinsatser inom området som en del i att stärka säkerhetskulturen. Utbildningarna bör även omfatta vad en informationssäkerhetsincident är i syfte att höja kunskap och medvetenheten angående detta. Det finns upprättade incidenthanteringsrutiner, dock är de vid tid för granskningen inte etablerade fullt ut varken inom kommunen eller bolagen.

Utöver detta saknas ett etablerat uppföljningsarbete inom samtliga revisionsobjekt som kan ligga till grund för beslut om åtgärder i syfte att stärka kommunens informationssäkerhet. Som följd saknas därmed även en upprättade informationssäkerhetsberättelser samt mål- och handlingsplaner.

Utifrån ovan är vår sammantagna bedömning att varken kommunen eller bolagen har säkerställt att det finns en tillräcklig informationssäkerhet i förhållande till aktuella hot och risker. Vi ser att detta är förenat med risk att det vid en incident kan innebära allvarliga konsekvenser för kommunen och bolagen i form av ekonomisk skada eller förtroendeskada.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Revidera policyn med reglering avseende de helägda bolagen.
- Upprätta styrande dokument som tydliggör ansvar, krav och hur informationssäkerhetsarbetet ska bedrivas samt säkerställa att de implementeras i kommunkoncernens organisation.
- Säkerställa att en ändamålsenlig organisation etableras i kommunen i enlighet med ansvar och krav där en del är att etablera linjeansvaret och en annan är att tydliggöra informationssäkerhetssamordnarens roll och mandat.
- Fastställa en kommun/koncerngemensam modell för riskbedömning och informationsklassning samt säkerställa att informationsklassning och riskbedömning av kommunens informationstillgångar genomförs.
- Säkerställa att obligatoriska utbildningsinsatser genomförs samt att medarbetarnas samt förtroendevaldas medverkan följs upp.
- Säkerställa att incidenthanteringsrutinen implementeras i hela organisationen.
- Etablera ett uppföljningsarbete för informationssäkerhet samt säkerställa att en informationssäkerhetsberättelse upprättas.
- Utifrån eget verksamhetsansvar samt uppsiktsplikt över andra nämnder samt bolag följa upp det informationssäkerhetsarbetet som bedrivs i syfte att erhålla en nulägesbild för beslut om eventuella insatser.
- Överväga på vilka sätt koncernsamverkan kan utvecklas avseende informationssäkerhetsarbetet.

Utifrån vår bedömning och slutsats rekommenderar vi kultur- och samhällsutvecklingsnämnden, social- och utbildningsnämnden samt vård- och omsorgsnämnden att:

- Säkerställa att kommunövergripande styrdokument implementeras i organisationen.
- Säkerställ att en ändamålsenlig organisation upprättas i enlighet med ansvar och krav.
- Säkerställa att informationsklassning och riskbedömning av nämndens informationstillgångar genomförs.
- Säkerställa att obligatoriska utbildningsinsatser genomförs samt att medarbetarnas samt förtroendevaldas medverkan följs upp.
- Säkerställa att incidenthanteringsrutinen implementeras i organisationen samt att inträffade incidenter analyseras i syfte att utgöra underlag för förbättringar.
- Följa upp det nämndspecifika informationssäkerhetsarbetet som bedrivs i syfte att erhålla en nulägesbild för beslut om eventuella insatser i syfte att stärka informationssäkerheten.

Utifrån vår bedömning och slutsats rekommenderar vi Ludvika kommun Stadshus AB att:

- Överväg på vilka sätt koncernsamverkan kan utvecklas avseende informationssäkerhetsarbetet.
- Säkerställ att koncernövergripande dokument implementeras i de helägda bolagen.
- Årligen värdera informationssäkerhetsrisker och konsekvenser för koncernen.
- Säkerställa att styrelsen erhåller regelbunden information om informationssäkerhetsarbetet hos kommunen och dotterbolagen för att vid behov kunna besluta om åtgärder för att stärka säkerheten i koncernen.

Utifrån vår bedömning och slutsats rekommenderar vi Ludvika Kommunfastigheter AB att:

- Säkerställa att bolaget efterlever koncernövergripande styrdokument.
- Säkerställ att en ändamålsenlig organisation upprättas i enlighet med ansvar och krav.
- Säkerställa att informationsklassning och riskbedömning av bolagets informationstillgångar genomförs.
- Säkerställa att incidenthanteringsrutinen implementeras i organisationen samt att inträffade incidenter analyseras i syfte att utgöra underlag för förbättringar.
- Följa upp det informationssäkerhetsarbetet som bedrivs i bolaget i syfte att erhålla en nulägesbild och kunna besluta om eventuella insatser i syfte att stärka informationssäkerheten.

Utifrån vår bedömning och slutsats rekommenderar vi Västerbergslagen Kraft AB att:

- Säkerställa att bolaget efterlever koncernövergripande styrdokument.
- Säkerställ att det finns en ändamålsenlig organisation upprättad i enlighet med ansvar och krav samt att ansvarsfördelning avseende informationssäkerhetsarbetet tydliggörs i avtal med Västerbergslagen Energi AB.
- Säkerställa att informationsklassning och riskbedömning av bolagets informationstillgångar genomförs.
- Säkerställa att incidenthanteringsrutinen implementeras i organisationen samt att inträffade incidenter analyseras i syfte att utgöra underlag för förbättringar.
- Följa upp det informationssäkerhetsarbetet som bedrivs i bolaget i syfte att erhålla en nulägesbild och kunna besluta om eventuella insatser i syfte att stärka informationssäkerheten.

Utifrån vår bedömning och slutsats rekommenderar vi Wessman Vatten & Återvinning AB att:

- Säkerställa att koncernövergripande styrdokument implementeras i organisationen.
- Säkerställ att ansvarsfördelning avseende informationssäkerhetsarbetet tydliggörs i avtal med WessmanBarken Vatten & Återvinning AB.
- Säkerställa att informationsklassning och riskbedömning av bolagets informationstillgångar genomförs.
- Säkerställa att incidenthanteringsrutinen implementeras i organisationen samt att inträffade incidenter analyseras i syfte att utgöra underlag för förbättringar.
- Följa upp det informationssäkerhetsarbetet som bedrivs i bolaget i syfte att erhålla en nulägesbild och kunna besluta om eventuella insatser i syfte att stärka informationssäkerheten.

2 Bakgrund

KPMG har av Ludvika kommuns förtroendevalda revisorer och lekmannarevisorer fått i uppdrag att genomföra en granskning av kommunstyrelsens, utvalda nämnders och bolags informationssäkerhet. Uppdraget ingår i revisionsplanen för år 2023.

Organisationer i offentlig sektor hanterar ovärderliga informationstillgångar och blir alltmer beroende av sina informationssystem. Ny teknik innebär nya möjligheter men introducerar även nya risker som ställer krav på ett balanserat risktagande och ett väl fungerande säkerhetsarbete.

Informationssäkerhet innebär att all skyddsvärd information ska vara tillgänglig, konfidentiell, riktig och spårbar. Den digitala transformationen innebär att det har skapats ett beroende av kontinuerligt fungerande informations- och kommunikationsteknik. Brister i informationshanteringen och säkerhetsarbetet kan få allvarliga konsekvenser, till exempel att integritetskänslig information sprids eller att verksamhetskritiska processer stoppas. Detta kan leda till både ekonomisk skada och förtroendeskada för kommunen och bolag. Det är således väsentligt att kommunen och de kommunala bolagen bedriver ett systematiskt informationssäkerhetsarbete så att arbetet sker på ett ändamålsenligt sätt.

Med anledning av ovanstående drar kommunens revisorer och lekmannarevisorer slutsatsen i sin riskanalys, att arbetet med informationssäkerheten behöver granskas.

2.1 Syfte, revisionsfrågor och avgränsning

Granskningen syftar till att bedöma om kommunstyrelsen, nämnder och bolagsstyrelser bedriver ett systematiskt informationssäkerhetsarbete så att det sker på ett ändamålsenligt sätt.

Granskningen avser att besvara följande revisionsfrågor:

- Finns aktuella styrande dokument som tydliggör ansvar, krav och hur arbetet ska bedrivas?
- Finns en ändamålsenlig organisation för informationssäkerhetsarbetet?
- Finns beslutade informationssäkerhetsmål med tillhörande handlingsplaner?
- Har styrelse och nämnder tillsett att det finns en god säkerhetskultur?
- Har riskanalyser och informationsklassning genomförts för de informationstillgångar som verksamheten ansvarar för?
- Finns incidenthanteringsrutiner som inkluderar krav på hur incidenter ska dokumenteras och följas upp tillsammans med tydliggjorda eskaleringsvägar?
- Finns en etablerad uppföljning av informationssäkerhetsarbetet och rapporteras denna till styrelse och nämnder med regelbundenhet?

Granskningen har omfattat kommunstyrelsens övergripande ansvar för informationssäkerhet samt deras ansvar för informationssäkerhet för de informationstillgångar som ingår i verksamhetsansvaret.

Granskningen har avsett nämndernas ansvar för informationssäkerhet för de informationstillgångar som ingår i verksamhetsansvaret.

Granskningen har omfattat bolagsstyrelsernas övergripande ansvar för informationssäkerhet samt deras ansvar för informationssäkerhet för de informationstillgångar som ingår i verksamhetsansvaret.

Granskningen har omfattat år 2023.

Granskningen har avsett kommunstyrelsen, kultur- och samhällsutvecklingsnämnden, social- och utbildningsnämnden och vård- och omsorgsnämnden samt bolagsstyrelserna i Ludvika kommun Stadshus AB, Västerbergslagens Kraft AB, Wessman vatten och Återvinning AB och Ludvika Kommunfastigheter AB.

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller

- Kommunallagens 6 kap. 6 §
- Aktiebolagslagen (de kommunala bolagen)
- Tillämpbara interna regelverk, policys och beslut
- MSB:s rekommendationer avseende Ledningssystem för informationssäkerhet

2.3 Metod

Granskningen har genomförts genom dokumentanalys av övergripande styrdokument fastställda av kommunfullmäktige och kommunstyrelsen i Ludvika kommun samt interna styrdokument för respektive bolag.

Vi har inom ramen för granskningen genomfört intervjuer med representanter för kultur- och samhällsutvecklingsnämnden, social- och utbildningsnämnden, vård- och omsorgsnämnden samt från kommunstyrelseförvaltningen. Vi har även genomfört intervjuer med representant från respektive bolag.

Samtliga medverkande har getts möjlighet att faktakontrollera rapporten.

3 Resultat av granskningen

3.1 Styrning och organisering av informationssäkerhetsarbetet

3.1.1 Ledningssystem för informationssäkerhet (LIS)

En kommuns eller ett bolags verksamhet kan identifieras som samhällsviktig tjänst och står då under kraven i Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, även kallat NIS-direktivet. I lagen ställs krav på att verksamheter som är identifierade som samhällsviktiga tjänster ska ha ett etablerat ledningssystem för informationssäkerhet, ett så kallat LIS. Inom Ludvika kommunkoncern omfattas Västerbergslagens Kraft AB (VBKAB) samt Wessman Vatten & Återvinning AB av NIS-direktivet.

Av Ludvika kommuns ledningssystem för informationssäkerhet framgår att informationssäkerhetspolicyn[1] utgör grunden för arbetet. Policyn omfattar samtliga nämnder och dess syfte är att skydda kommunen mot förlust av information och oavsiktlig eller obehörig förändring av informationen. Målet med policyn anges bland annat vara att säkerställa att rätt information är tillgänglig för rätt person, att förhindra och minska effekter av störningar samt skydda information och system mot hot.

Det saknas reglering i policyn angående bolagens omfattning. Intervjuade uppger att policyn ska omfatta helägda bolag i kommunkoncernen, men att detta vid upprättande inte har tydliggjorts.

Policyn anger att kompletterande styrdokument ska konkretisera policyns mer övergripande viljeriktning. I nuläget har varken kommunen eller bolagen upprättat och etablerat kompletterande styrdokument avseende informationssäkerhet. Avsaknad av riktlinjer som konkretiserar informationssäkerhetspolicyn anges utgöra grundorsaken till att ett systematiskt informationssäkerhetsarbete inte har etablerats i kommunen och bolagen.

3.1.2 Ansvarsfördelning informationssäkerhet

3.1.2.1 Kommunstyrelsens övergripande ansvar

Av informationssäkerhetspolicyn framgår att ansvar för utveckling av informationssäkerhetsarbetet åligger kommunstyrelsen. Utöver detta saknas reglering avseende kommunstyrelsens ansvar avseende informationssäkerhetsarbetet. Däremot ansvarar kommunstyrelsen för att följa upp nämndernas informationssäkerhetsarbete som en del i sin uppsiktsplikt i enlighet med kommunallagen (2017:725).

Enligt policyn ska ansvarsfördelningen tydliggöras i riktlinjer för informationssäkerhet. Som vi beskrivit ovan saknas riktlinjer och därigenom saknas i nuläget en dokumenterad ansvarsfördelning utöver det som nämns ovan.

[1] Beslutad av kommunfullmäktige 2019-11-11

Enligt policyn ska en informationssäkerhetssamordnare fungera som stöd till kommunens verksamheter för att dessa ska fullfölja informationssäkerhetsansvaret.

I Ludvika kommun har säkerhetschef uppdragits rollen som informationssäkerhetssamordnare. Denna är tillika chef över enheten för säkerhet och brottsförebyggande, vilken är placerad inom kommunstyrelseförvaltningen.

Vid granskningens genomförande var nuvarande informationssäkerhetssamordnaren relativt nytillträdd. Vi delges att arbetet hittills fokuserats mot att få grundläggande delar som rollbeskrivningar, helhetssyn och styrande dokument på plats.

Vidare framgår i intervju att det har funnits brister i ansvarsfördelningen inom kommunen avseende informationssäkerhetsarbetet och att detta därmed behöver förtydligas ytterligare.

3.1.2.2 Kommunstyrelsens och nämndernas verksamhetsansvar för informationssäkerhet

Av policyn framgår att varje nämnd ansvarar för informationssäkerhetsarbetet inom respektive verksamhetsområde. Därtill anges att ansvar för informationssäkerhet följer ordinarie verksamhetsansvar.

I de intervjuer vi genomfört råder en delad bild om det informationssäkerhetsansvar som följer linjeansvaret är tydligt förankrat. Samtliga intervjuade uttrycker behov av kommunövergripande riktlinjer då det i dag saknas struktur och stöd i en fråga som uppfattas som utmanande och komplex. Informationssäkerhetssamordnaren anses vara ett bra stöd för att bolla frågor men som enskild resurs uppfattas tillgång till stöd inte tillräckligt för att möta de behov som finns i verksamheterna.

Vi uppfattar att informationssäkerhetsarbetet på förvaltningsnivå i stor utsträckning är knutet till enskilda personer med kunskap och engagemang, för samtliga är informationssäkerhetsarbetet en uppgift som adderats utöver ordinarie arbetsuppgifter.

- Inom social- och utbildningsförvaltningen är det en nämndsekreterare och en systemförvaltare som arbetar med informationssäkerhetsfrågor.
- Hos vård- och omsorgsförvaltningen samt kultur- och samhällsutvecklingsförvaltningen hanteras informationssäkerhetsfrågor av respektive kanslienhet.
- Inom kultur- och samhällsutvecklingsförvaltningen samt kommunstyrelseförvaltningen saknas en utsedd funktion som arbetar med informationssäkerhetsfrågor internt på förvaltningen.

3.1.2.3 Kommunala bolags ansvar för informationssäkerhet

Kommunfullmäktige har beslutat om gemensamma ägardirektiv[2] som gäller för Ludvika Kommun Stadshus AB, Ludvika Kommunfastigheter AB, LudvikaHem AB och VB Kraft AB (av de bolag som ingår i granskningens avgränsning). För varje bolag (exkl. Ludvika Stadshus AB) finns ett särskilt ägardirektiv som innehåller unika direktiv för

[2] Kommunfullmäktige 2018-03-05, KS 2017/387

respektive bolag samt eventuella preciseringar av sådant som står i det gemensamma direktivet.

Reglering av krav avseende informationssäkerhet saknas i både gemensamt ägardirektiv och specifika ägardirektiv. Som vi beskrivit tidigare i rapporten så saknas beskrivning av bolagens ansvar i den informationssäkerhetspolicy som fullmäktige har fastställt. Då företrädare uttrycker att policyn utgör styrning för bolagen gör vi tolkningen att benämningen styrelse/nämnd även ska tolkas för bolagen.

Ludvika kommun Stadshus AB

Bolaget utgör moderbolag till övriga helägda bolag i kommunen. Bolaget ansvarar för att se till att den kommunala bolagskoncernen styrs och verkar på ett sätt som bäst tjänar Ludvika kommun och dess invånare. Då bolaget saknar driftverksamhet och därmed anställda (bortsett från VD) är det VD som ansvarar för bolagets informationssäkerhetsarbete.

Ludvika Kommunfastigheter AB

Bolaget uppges inte ha någon särskild person som ansvarar för informationssäkerhetsarbetet, vilket innebär att det är VD som innehar den rollen. Informationssäkerhetsansvaret som följer med linjeansvaret uppges vara känt i organisationen men arbetet har inte varit prioriterat i bolaget.

Västerbergslagens Kraft AB

Västerbergslagens Kraft AB (fortsättningsvis benämnt VBKAB) uppger i intervju att de inte bedriver någon egen verksamhet förutom att VD finns anställd i bolaget. Då bolaget saknar driftverksamhet och därmed anställda (bortsett från VD) är det VD som ansvarar för bolagets informationssäkerhetsarbete.

Drift, underhåll och administration regleras och hanteras enligt avtal med ett av de övriga bolagen i koncernen, Västerbergslagens Energi AB. Västerbergslagens Energi AB ägs till 28,6 % av Ludvika Kommun Stadshus AB. Det avtal som vi tagit del av innehåller inte någon reglering avseende VBKAB:s krav på informationssäkerhet. Avtalet tydliggör inte någon specificering avseende informationssäkerhet. Den återrapportering som avtalet ställer krav på omfattar inte informationssäkerhet.

Då Västerbergslagens Energi AB inte omfattas av granskningen har vi inom ramen för detta arbete inte undersökt förutsättningar och processer för informationssäkerhetsarbetet. Enligt uppgift omfattas Västerbergslagens Energi AB av NIS-direktivet och företrädare från VBKAB har därigenom uppfattat att informationssäkerhetsarbetet mot bakgrund av detta bedrivs systematiskt. Någon uppföljning av om detta stämmer har dock inte genomförts av VBKAB.

Wessman Vatten & Återvinning AB

Wessman Vatten & Återvinning AB (fortsättningsvis benämnt WVÅ) ansvarar för anläggningstillgångar medan bolagets driftverksamhet är organiserad i dotterbolaget WessmanBarken Vatten och Återvinning AB (fortsättningsvis benämt WBAB).

I WVÅ finns en anställd säkerhetschef som beskrivs vara operativt samordnande för alla slags säkerhetsfrågor för WBAB, däribland informationssäkerhet. Intervjuade anger att det inom WBAB finns ett etablerat linjeansvar och struktur för informationssäkerheten.

Intervjuade anger att informationssäkerhetsarbetet som bedrivs inom WBAB har haft utgångspunkt i Ludvika kommuns informationssäkerhetspolicy. Dock uppfattas koncernmodellen leda till svårigheter att tolka vilka styrande dokument som ska följas, vilket har initierat en utredning i syfte att tydliggöra detta.

Som stöd och vid hjälp med hantering av it- och informationssäkerhetsfrågor uppger intervjuade att de vänder sig till It-center, som är den gemensamma it-avdelningen för Ludvika kommun och Smedjebackens kommun.

3.1.3 Samverkan inom kommunkoncernen

Intervjupersoner uppger att det saknas samverkan inom koncernen avseende informationssäkerhetsarbetet.

3.1.4 Bedömning

Vår bedömning är att det saknas styrande dokument som tydliggör ansvar, krav och hur arbetet ska bedrivas.

Vi kan konstatera att kommunfullmäktige i enlighet med MSB:s rekommendationer har beslutat om policy för informationssäkerhet som gäller för kommunens samtliga verksamheter. I nuvarande policy saknas reglering över bolagens ansvar för informationssäkerhet.

Varken kommunstyrelsen eller bolagsstyrelserna har beslutat om riktlinjer eller andra styrande dokument inom informationssäkerhet vilket leder till att det i nuläget saknas ändamålsenliga styrdokument. I avsaknad av verksamhetsanpassade styrdokument bedömer vi att det finns en risk att verksamhetsspecifika förutsättningar inte har beaktats tillräckligt och att ansvarsfördelning och krav för hur arbetet ska bedrivas inte är dokumenterat och etablerat.

Vår bedömning är att kommunstyrelsen samt bolagsstyrelserna i Ludvika Kommunfastigheter AB och Västerbergslagens Kraft AB inte har säkerställt att det finns en ändamålsenlig organisation för informationssäkerhetsarbetet.

I avsaknad av styrande dokument saknas en tydliggjord ansvarsfördelning och krav på hur arbetet ska bedrivas inom både förvaltningar och bolag. Vi ser det som väsentligt att kompletterande styrdokument tydliggör det ansvar som ingår i verksamhetsansvaret och för ytterligare nyckelfunktioner i arbetet.

Vi bedömer därtill att det saknas ett ansvarstagande för informationssäkerhet inom kommunen och ovan nämnda bolag där linjeansvaret inte fullföljs i nuläget. Det arbete

som utförs av enskilda funktioner kan i delar bidra till informationssäkerhet men sker inte i enlighet med en systematik och struktur.

Vi uppfattar att varken kommunstyrelsen eller Ludvika kommun Stadshus AB i tillräcklig utsträckning har beaktat de effektiviserings- och kvalitetsvinster som en utvecklad koncernsamverkan i informationssäkerhetsarbetet skulle kunna bidra till.

Vi kan konstatera att kommunen har tillsatt en informationssäkerhetssamordnare i enlighet med MSBs rekommendationer. Vi ser dock behov av att rollen stärks med ett tydligt uppdrag att leda, stödja, samordna och följa upp det kommun- eller koncernövergripande informationssäkerhetsarbetet.

Vår bedömning är att Västerbergslagens Kraft AB har behov av att utreda sitt ansvar för informationssäkerhet då detta inte kan delegeras till andra. Om vissa uppgifter i arbetet ska genomföras av extern part behöver detta regleras tydligt med kravställning på säkerhetsnivåer och aktiviteter tillsammans med former för uppföljning.

Vår bedömning att Wessman Vatten & Återvinning AB i allt väsentligt har en ändamålsenlig organisation för informationssäkerhet.

Vi bedömer att linjeansvaret är etablerat och det finns en utsedd informationssäkerhetssamordnare som samordnar arbetet och vissa uppgifter inom bolaget.

I avsaknad av styrande dokument saknas dock en tydliggjord ansvarsfördelning och krav på hur arbetet ska bedrivas inom bolaget. Vi ser det som väsentligt att kompletterande styrdokument tydliggör det ansvar som ingår i verksamhetsansvaret och för ytterligare nyckelfunktioner i arbetet. Vi ser även behov av att ansvarsfördelning mellan bolaget och WessmanBarken Vatten & Återvinning AB regleras tydligare och att detta dokumenteras.

3.2 Riskbedömning och informationsklassning

Av lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster framgår att leverantör av samhällsviktiga tjänster ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Utifrån detta har MSB rekommendationer avseende säkerhetsåtgärder i syfte att öka skyddet mot angrepp eller minimera eventuell skada. Rekommendationerna omfattar bland annat säkerhetsuppdateringar, säkerhetskopiering samt förmågan att upptäcka säkerhetshändelser.

3.2.1 Riskanalyser och informationsklassning inom kommunstyrelsen och nämnder

Enligt intervju genomförs inga kommunövergripande riskanalyser avseende informationssäkerhet. Det uppges inte heller finnas någon beslutad modell för riskbedömning eller informationsklassning. I de fall klassning genomförs uppges det ske på initiativ från enskilda personer utifrån kompetens och engagemang.

Vid upphandling av ett nytt system genomförs upphandlingen av Upphandlingscentra som är gemensam samverkan mellan flera kommuner[3] i Dalarna. för Faluns och Borlänges kommuner. Som del i upphandlingsprocessen av ett nytt verksamhetssystem anges i intervju att informationsklassning ska genomföras.

Vi har tagit del av internkontrollplaner för år 2022 för styrelse och de nämnder som granskningen omfattar. I dessa planer finns inga kontrollmoment som berör informationssäkerhet.

Kommunstyrelsen

Intervjuade anger att det inte har genomförts någon verksamhetsövergripande riskbedömning inom kommunstyrelseförvaltningen. Vidare anges att det även saknas genomförda informationsklassningar av de informationstillgångar som nyttjas inom förvaltningen.

Social- och utbildningsnämnden

Förvaltningen har enligt intervjuade inte klassat information som hanteras inom förvaltningen, men beskriver att verksamhetssystem där känsliga uppgifter om enskilda individer hanteras, till exempel elevhälsans journalsystem, kräver säkerhetsinloggning genom tvåfaktorsautentisering.

Vidare lyfts att det finns en medvetenhet angående riskerna med att information som hanteras inom förvaltningen sparas i tredje land. Socialnämnden har enligt uppgift inte vidtagit särskilda åtgärder med anledning av detta.

[3] Ludvika kommun, Falu kommun, Borlänge kommun, Gagnefs kommun, Säters kommun, Avesta kommun samt Hedemora kommun.

Kultur- och samhällsutvecklingsnämnden

Enligt vad som uppges i intervju genomförde förvaltningen för något år sedan en scenariobaserad riskbedömning kring möjliga avbrott, där avbrott i verksamhetssystem identifierades som en risk. Riskbedömningen resulterade i ett antal rutiner som togs fram tillsammans med personal från säkerhetsenheten.

Vidare framförs att verksamhetssystemen prioriterats utifrån hur kritiska dessa är, och att förvaltningen endast ansågs ha något enstaka system som bedömdes som kritiskt. Därtill delges att det finns ett arbetssätt för informationsklassning av dokument, men utifrån intervju uppfattar vi att det rör dokumenthanteringsplaner snarare än rutiner för klassning av information.

Vård- och omsorgsnämnden

Förvaltningsföreträdare anger att varken riskbedömningar eller informationsklassningar genomförs regelbundet. I och med att förvaltningen hanterar stor volym känslig information beskrivs att arbetssätt utgår från äldre rutiner och sekretessbestämmelser, liksom att klassning av system genomförs vid upphandling av nya system.

Vid upphandling av nya system genomförs klassning av vård- och socialförvaltningens personal. Som klassningsmodell används Sveriges kommuner och regioners verktyg *Klassa*[4]. Intervjuade beskriver att verktyget är komplicerat då det nyligen genomgått en större uppdatering, och att stöd från informationssäkerhetssamordnare hade önskats. Över lag anges att förvaltningen står ensam och hanterar informationsklassning utan stöd från upphandlings- eller it-personal, som beskrivs sakna tillräcklig kompetens för informationsklassning av den typen av system som används inom förvaltningen.

3.2.2 Riskanalyser och informationsklassning inom bolagsstyrelser

Ludvika kommun Stadshus AB

Bolaget har inte genomfört någon koncernövergripande riskbedömning på verksamhetsnivå. Då bolaget saknar driftverksamhet genomförs inget riskanalys- eller klassningsarbete.

Ludvika Kommunfastigheter AB

Ludvika Kommunfastigheter AB har inte genomfört riskbedömning eller informationsklassning av bolagets informationstillgångar. Av intervju framgår att det saknas ett avtal avseende kravställning på specifika säkerhetsnivåer för it-leveransen mellan bolaget och It-center.

Västerbergslagens Kraft AB

Representanter från VBKAB uppger att de inte har insyn i om riskbedömningar eller informationsklassning har genomförts. Detta utifrån att de anser att Västerbergslagens Energi AB har helhetsansvar för informationssäkerhetsarbetet.

[4] Ett verktyg som SKR tagit fram för att förenkla kommuners och regioners genomförande av informationsklassning. Källa: skr.se

Wessman Vatten & Återvinning AB

Intervjuade anger att verksamheten genomfört riskbedömning enligt en egenkonstruerad modell anpassad för koncernens verksamhet inom dricksvatten och avlopp, vilket omfattas av NIS-direktivet. Härvid värderades olika slags informationssäkerhetrisker, som sabotage och brand, utifrån påverkan på verksamheten. Detta beskrivs ha legat till grund för en åtgärdslista som lämnats in till aktuell tillsynsmyndighet (Livsmedelsverket). Vi har i granskningen efterfrågat att få ta del av rapporten men inte erhållit detta. Informationsklassningen uppges ha genomförts av verksamhetsrepresentanter tillsammans med it-personal samt säkerhetschef för Ludvika kommun.

Vi delges att koncernen påbörjat en systeminventering för att kartlägga olika roller kopplade till systemförvaltning. Utifrån inventeringen avses en riskanalys genomföras, vilken ska utgöra grund för exempelvis behörighetstilldelning och informationsklassning. Anledningen till genomlysningen beskrivs vara att det finns en befintlig rollista med namn på olika funktioner, men att den i vissa avseenden är inaktuell. Genom inventeringen uppges att klassning kommer att genomföras för system som ännu inte klassats.

3.2.3 Åtgärdsplan

Då informationsklassning och riskbedömning av informationstillgångar inte har genomförts mer än vid enstaka tillfällen saknas upprättade åtgärdsplaner som visar behov av säkerhetsåtgärder för att skydda information och system. Detta gäller för samtliga revisionsobjekt.

Wessman Vatten & Återvinning AB har utifrån krav från tillsynsmyndighet för NIS-direktivet en åtgärdslista utifrån risker. Då vi inte har tagit del av denna kan vi inte uttala oss om den är tillräcklig i förhållande till verksamhetens behov eller krav.

3.2.4 Bedömning

Vår bedömning är att kommunstyrelsen, de nämnder som omfattas av granskningen, bolagsstyrelserna i Wessman Vatten & Återvinning AB, Västerbergslagens Kraft AB och Ludvika Kommunfastigheter AB inte har genomfört informationsklassning eller riskbedömning i tillräcklig utsträckning av de informationstillgångar som verksamheten ansvarar för.

Arbetet som bedrivs är inte tillräckligt i syfte att kunna identifiera eventuella hot och oönskade händelser som kan påverka kommunen och bolagens verksamheter negativt. I avsaknad av tillräckliga riskanalyser och klassningar finns inte underlag för åtgärdsplaner i syfte att stärka informationssäkerheten. Detta gäller samtliga revisionsobjekt.

Vidare bedömer vi att Ludvika kommun Stadshus AB och kommunstyrelsen har brustit i sitt övergripande säkerhetsansvar då inte informationssäkerhetsrisker har beaktats i dokumenterade riskanalyser. Detta behöver genomföras på både koncern- och kommunövergripande nivå i syfte att identifiera hot och risker som kan påverka hela

koncernen negativt då konsekvenser av informationssäkerhetsincidenter ofta är allvarliga med både ekonomiska följder och förtroendeskada.

3.3 Säkerhetskultur

3.3.1 Säkerhetskultur inom kommunstyrelsen och nämnderna

Vid tidpunkten för granskningens genomförande framkommer att kommunen nyligen köpt in ett paket med nano-learning inom informations- och it-säkerhet. Utbildningen består av korta digitala utbildningssessioner och kommer att genomföras ett par gånger om året med start hösten 2023. Utbildningen är obligatorisk för samtliga anställda som innehar en egen dator. Vi delges att informationssäkerhetssamordnaren utöver detta ser över möjligheten att genomföra en grundläggande, kommungemensam informationssäkerhetsutbildning, men uppger att det kan finnas svårigheter att genomföra en sådan på grund av resursbrist.

Generellt uppfattar intervjuade att avsaknad av utbildning har genererat en låg kunskapsnivå hos anställda såväl som förtroendevalda. Samtidigt framhålls, mot bakgrund av omvärldsläget, att säkerhetsmedvetenheten höjts och att mottagligheten för kunskap inom informationssäkerhet är högre nu än tidigare.

Samtliga intervjuade förvaltningsföreträdare framför att kunskap om personuppgiftshantering är förhållandevis god bland medarbetare, men att kännedom om informationssäkerhet är mindre. Inom samtliga granskade nämnder uppfattas kunskap åvila ett begränsat antal enskilda individer, vilka utpekas som särskilt betydelsefulla för varje nämnds informationssäkerhetsarbete.

3.3.2 Säkerhetskultur inom bolagsstyrelserna

Utbildning uppges inte ha genomförts inom något av bolagen.

3.3.3 Bedömning

Vår bedömning är att kommunstyrelsen, granskade nämnder samt bolagsstyrelser inte tillsett en god säkerhetskultur.

De kommunövergripande insatserna i syfte att stärka säkerhetskulturen behöver utvecklas ytterligare med att omfatta riktade utbildningsinsatser. Utbildningsinsatser bidrar till att öka kunskap och medvetenhet hos medarbetare och förtroendevalda, vilket i sin tur kan leda till att risken för att incidenter inträffar minskar.

Vi anser att kommunstyrelsen och bolagen bör säkerställa att samtliga medarbetare omfattas av utbildningsinsatserna då flertalet i kommunens och bolagens organisation inte har tillgång till en egen dator.

Utbildningarna bör även omfatta förtroendevalda samt vara obligatoriska, både för att säkerställa samtligas deltagande och för att kommunstyrelsen genom detta påvisar vikten av att kunskapen kring informationssäkerhet ökas.

3.4 Hantering av informationssäkerhetsincidenter

Av lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster framgår att leverantör av samhällsviktiga tjänster ska vidta lämpliga åtgärder för att förebygga och minimera verkningar av incidenter som påverkar nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Åtgärderna ska syfta till att säkerställa kontinuiteten i tjänsterna.

Av *informationssäkerhetspolicyn* framgår att alla anställda är skyldiga att uppmärksamma och rapportera säkerhetspåverkande händelser.

3.4.1 Rutiner

Rutin för incidentrapportering[5] redovisar hur personuppgiftsincidenter samt it- och informationssäkerhetsincidenter ska anmälas och hanteras. Incidentanmälan ska göras via kommunens intranät, till vilket en länk finns i rutinen. Ansvarig för att vidta de åtgärder som rutinen beskriver är ansvarig chef eller den som delegerats uppgiften. Rutinen omfattar såväl nämnder som helägda bolag. I rutinen saknas en beskrivning av vad som avses med en informationssäkerhetsrelaterad incident.

WVÅ hänvisar till rutiner upprättade av Smedjebackens kommun[6]. Rutinerna innehåller tydliga eskaleringsvägar samt en beskrivning av hur incidenten ska utredas.

3.4.2 Arbetssätt inom revisionsobjekten

Det förs fram att *rutin för incidentrapportering*, som beskrivs ovan, togs fram nyligen som ett första steg mot en mer central samordning och styrning av incidenthantering. Av intervjuer framgår att rutinerna ännu inte är implementerade inom samtliga revisionsobjekt, vilket uppges ha resulterat i egna rutiner för anmälan av incident. En vanlig hantering uppges vara att kontakta närmaste chef.

Intervjuade anger att rutinerna inom WVÅ är etablerade inom bolaget och används i händelse av att en incident inträffar.

Intervjuade uppger att antalet anmälningar upplevs som för få i förhållande till organisationens storlek, vilket förvaltningsrepresentanter uppfattar beror på den begränsade kunskapen om vad en informationssäkerhetsincident är.

Att anmälan ska ske via intranätet uppges vara ett sätt för att vid årets slut kunna följa upp incidenterna.

[5] Beslutad 2023-07-07

[6] Övergripande rutin för incidenthantering, kommunchef

3.4.3 Bedömning

Vi bedömer att det finns en incidenthanteringsrutin som inkluderar krav på hur incidenter ska dokumenteras och följas upp samt vilka eskaleringsvägar som ska användas.

Vår bedömning är dock att rutinen inte i tillräcklig utsträckning är etablerad inom kommunstyrelsen, de nämnder som omfattas av granskningen samt bolagsstyrelserna i Ludvika kommun Stadshus AB, Västerbergslagens Kraft AB och Ludvika Kommunfastigheter AB.

Vi bedömer att Wessman Vatten & Återvinning AB har upprättade och implementerade rutiner för incidenter som inkluderar krav på hur incidenter ska dokumenteras och följas upp samt vilka eskaleringsvägar som ska användas.

Vi ser ett behov av att tydliggöra vad som är en informationssäkerhetsincident, både i rutinen samt genom kompetenshöjande insatser som utbildning. Syftet är att minska risken för att incidenter inträffar samt att säkerställa att kunskap finns om vad en incident är vilket ökar chansen för att dessa anmäls.

Utöver detta är vår bedömning att samtliga revisionsobjekt kan stärka arbetet med att analysera inträffade incidenter i syfte att identifiera eventuella åtgärder som behöver vidtas för att minska risken för att incidenten inträffar igen.

3.5 Uppföljning och återrapportering

Av 6 kap. 6 § Kommunallagen (2017:725) framgår att nämnder inom sitt område ska se till att verksamheten bedrivs i enlighet med de mål och riktlinjer som fullmäktige har bestämt samt de bestämmelser i lag eller annan författning som gäller för verksamheten. De ska även se till att den interna kontrollen är tillräcklig och att verksamheten bedrivs på ett i övrigt tillfredsställande sätt.

Vidare framgår av MSB:s metodstöd att för att ledningen på en strategisk nivå ska få en samlad bild och kunskap om informationssäkerhetsarbetet i kommunen behöver det ske en kommunövergripande uppföljning av arbetet som sedan rapporteras under ledningens genomgång. Uppföljningen utgör även underlag för eventuella beslut på strategisk nivå angående åtgärder och resursfördelning. Resultatet från ledningens genomgång ska dokumenteras och bevaras.

Enligt kommunens informationssäkerhetspolicy ska styrelse och nämnder följa upp informationssäkerhet inom respektive verksamhet. Policyn i sig ska följas upp och, vid behov, revideras en gång om året, samt att efterlevnad till denna också ska följas upp. Vidare ska informationssäkerhetssamordnare, i början på året, återrapportera föregående års och kommande års informationssäkerhetsarbete till kommundirektör och kommunstyrelsen. Extraordinära händelser kan, enligt policyn, motivera ytterligare uppföljning.

3.5.1 Uppföljning inom kommunstyrelse och nämnder

Utifrån intervjuer konstaterar vi att ingen regelbunden uppföljning avseende informationssäkerhet görs inom kommunstyrelsen eller granskade nämnder. Vidare

anges att det saknas tydlighet avseende hur uppföljningsarbetet ska genomföras och att avsaknaden av riktlinjer utgör en bidragande orsak till ett uteblivet uppföljningsarbete.

Informationssäkerhetssamordnaren tillika säkerhetskyddschef medverkar vid ledningsgruppens träffar och informerar angående samtliga säkerhetsfrågor. Vidare uppges att kommunstyrelsen innehar ett intresse angående säkerhetsfrågor med anledning av omvärldsförändringar.

3.5.2 Uppföljning inom bolagsstyrelser

Utifrån intervjuer konstaterar vi att ingen regelbunden uppföljning avseende informationssäkerhet görs inom bolagen och det finns i nuläget ingen systematisk rapportering eller uppföljning av informationssäkerhet mot respektive bolagsstyrelse.

Den enda uppföljning som nämnts är Wessman Vatten & Återvinning samt Västerbergslagens Kraft AB som uppges återrapportera incidenter till respektive bolagsstyrelse i de fall sådana har inträffat.

3.5.3 Beslut om förbättringar

Kommunen samt bolagen saknar mål- och handlingsplaner för informationssäkerhetsarbetet.

3.5.4 Bedömning

Vår bedömning är att kommunstyrelsen, nämnder och bolagsstyrelser saknar ett etablerat uppföljningsarbete samt mål- och handlingsplaner för arbetet.

Vi anser därför att kommunstyrelsen, nämnder samt bolagsstyrelser inte har säkerställt en tillräcklig återrapportering i syfte att kunna besluta om erforderliga åtgärder för att stärka informationssäkerheten inom koncernen.

4 Slutsats och rekommendationer

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen, nämnder och bolagsstyrelser inte bedriver ett systematiskt informationssäkerhetsarbete så att det sker på ett ändamålsenligt sätt.

Vi bedömer att ledningssystemets omfattning inte är i paritet med varken de informationstillgångar som hanteras av kommunkoncernen, eller med vad som rekommenderas av MSBs metodstöd.

Det riskanalysarbete som genomförs anser vi inte vara tillräckligt, vilket utgör en risk för att säkerhetsåtgärder inte identifieras i den utsträckning som behövs för att skydda informationstillgångarna.

Utöver detta saknas ett etablerat uppföljningsarbete inom samtliga revisionsobjekt som kan ligga till grund för beslut om åtgärder i syfte att stärka kommunens informationssäkerhet.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Revidera policyn med reglering avseende de helägda bolagen.
- Upprätta styrande dokument som tydliggör ansvar, krav och hur informationssäkerhetsarbetet ska bedrivas samt säkerställa att de implementeras i kommunkoncernens organisation.
- Säkerställa att en ändamålsenlig organisation etableras i kommunen i enlighet med ansvar och krav där en del är att etablera linjeansvaret och en annan är att tydliggöra informationssäkerhetssamordnarens roll och mandat.
- Fastställa en kommun/koncerngemensam modell för riskbedömning och informationsklassning samt säkerställa att informationsklassning och riskbedömning av kommunens informationstillgångar genomförs.
- Säkerställa att obligatoriska utbildningsinsatser genomförs samt att medarbetarnas samt förtroendevaldas medverkan följs upp.
- Säkerställa att incidenthanteringsrutinen implementeras i hela organisationen.
- Etablera ett uppföljningsarbete för informationssäkerhet samt säkerställa att en informationssäkerhetsberättelse upprättas.
- Utifrån eget verksamhetsansvar samt uppsiktsplikt över andra nämnder samt bolag följa upp det informationssäkerhetsarbetet som bedrivs i syfte att erhålla en nulägesbild för beslut om eventuella insatser.
- Överväga på vilka sätt koncernsamverkan kan utvecklas avseende informationssäkerhetsarbetet.

Utifrån vår bedömning och slutsats rekommenderar vi kultur- och samhällsutvecklingsnämnden, social- och utbildningsnämnden samt vård- och omsorgsnämnden att:

- Säkerställa att kommunövergripande styrdokument implementeras i organisationen.
- Säkerställ att en ändamålsenlig organisation upprättas i enlighet med ansvar och krav.
- Säkerställa att informationsklassning och riskbedömning av nämndens informationstillgångar genomförs.
- Säkerställa att obligatoriska utbildningsinsatser genomförs samt att medarbetarnas samt förtroendevaldas medverkan följs upp.
- Säkerställa att incidenthanteringsrutinen implementeras i organisationen samt att inträffade incidenter analyseras i syfte att utgöra underlag för förbättringar.
- Följa upp det nämndspecifika informationssäkerhetsarbetet som bedrivs i syfte att erhålla en nulägesbild för beslut om eventuella insatser i syfte att stärka informationssäkerheten.

Utifrån vår bedömning och slutsats rekommenderar vi Ludvika kommun Stadshus AB att:

- Överväg på vilka sätt koncernsamverkan kan utvecklas avseende informationssäkerhetsarbetet.
- Säkerställ att koncernövergripande dokument implementeras i de helägda bolagen.
- Årligen värdera informationssäkerhetsrisker och konsekvenser för koncernen.
- Säkerställa att styrelsen erhåller regelbunden information om informationssäkerhetsarbetet hos kommunen och dotterbolagen för att vid behov kunna besluta om åtgärder för att stärka säkerheten i koncernen.

Utifrån vår bedömning och slutsats rekommenderar vi Ludvika Kommunfastigheter AB att:

- Säkerställa att bolaget efterlever koncernövergripande styrdokument.
- Säkerställ att en ändamålsenlig organisation upprättas i enlighet med ansvar och krav.
- Säkerställa att informationsklassning och riskbedömning av bolagets informationstillgångar genomförs.
- Säkerställa att incidenthanteringsrutinen implementeras i organisationen samt att inträffade incidenter analyseras i syfte att utgöra underlag för förbättringar.

— Följa upp det informationssäkerhetsarbetet som bedrivs i bolaget i syfte att erhålla en nulägesbild och kunna besluta om eventuella insatser i syfte att stärka informationssäkerheten.

Utifrån vår bedömning och slutsats rekommenderar vi Västerbergslagen Kraft AB att:

— Säkerställa att bolaget efterlever koncernövergripande styrdokument.

— Säkerställ att det finns en ändamålsenlig organisation upprättad i enlighet med ansvar och krav samt att ansvarsfördelning avseende informationssäkerhetsarbetet tydliggörs i avtal med Västerbergslagen Energi AB.

— Säkerställa att informationsklassning och riskbedömning av bolagets informationstillgångar genomförs.

— Säkerställa att incidenthanteringsrutinen implementeras i organisationen samt att inträffade incidenter analyseras i syfte att utgöra underlag för förbättringar.

— Följa upp det informationssäkerhetsarbetet som bedrivs i bolaget i syfte att erhålla en nulägesbild och kunna besluta om eventuella insatser i syfte att stärka informationssäkerheten.

Utifrån vår bedömning och slutsats rekommenderar vi Wessman Vatten & Återvinning AB att:

— Säkerställa att koncernövergripande styrdokument implementeras i organisationen.

— Säkerställ att ansvarsfördelning avseende informationssäkerhetsarbetet tydliggörs i avtal med WessmanBarken Vatten & Återvinning AB.

— Säkerställa att informationsklassning och riskbedömning av bolagets informationstillgångar genomförs.

— Säkerställa att incidenthanteringsrutinen implementeras i organisationen samt att inträffade incidenter analyseras i syfte att utgöra underlag för förbättringar.

— Följa upp det informationssäkerhetsarbetet som bedrivs i bolaget i syfte att erhålla en nulägesbild och kunna besluta om eventuella insatser i syfte att stärka informationssäkerheten.

Ludvika kommun och kommunala bolag
Granskning av informationssäkerhet

2023-10-20

Datum som ovan
KPMG AB

Jenny Thörn
Kommunal revisor

Ida Larsson
Kommunal revisor

Sofie Ernerudh
Kommunal revisor

Magnus Larsson
Certifierad kommunal revisor

A Metodstöd för systematiskt informations-säkerhetsarbete och säkerhetsåtgärder

Som revisionskriterium i granskningen utgår vi från MSB:s metodstöd och rekommendationer för ett systematiskt informationssäkerhetsarbete och säkerhetsåtgärder med fokus på nedanstående områden.

Standard och krav

Metodstödet bygger på de internationella standarderna för informationssäkerhet i ISO/IEC 27000-serien och då främst på SS-EN ISO/IEC 27001 och SS-EN ISO/IEC 27002 om ledningssystem för informationssäkerhet.

Ledningssystem för informationssäkerhet

Ett ledningssystem för informationssäkerhet (ofta förkortat LIS) är den del av ledningssystemet som styr verksamhetens informationssäkerhet. För att informationssäkerhetsarbetet ska lyckas och vara framgångsrikt är det viktigt att informationssäkerheten integreras med de olika styrformerna, som planering och uppföljning. Det innebär till exempel att ledningen löpande informerar sig om informationssäkerhetsarbetet, gör regelbundna verksamhetsplaneringar och kontroller samt ser över styrdokumenten med jämna mellanrum.

Ledningen bör också se till att organisationen antar en policy för informationssäkerhetsarbetet. I ytterligare styrdokument, riktlinjer och liknande kan sedan den högsta ledningen ge vägledning till chefer och övriga medarbetare om vilka krav som ställs i arbetet. Det är viktigt att alla i en organisation känner till och förstår innehållet i policys och riktlinjer.

Ansvar och organisation

Metodstödet beskriver hur ansvaret för arbetet med informationssäkerhet bör fördelas i organisationen samt tydliggör betydelsen av ledningens förståelse och engagemang i informationssäkerhetsarbetet för att det ska lyckas. Det bör finnas en person inom organisationen med ansvar för att samordna informationssäkerhetsarbetet. Grundprincipen är att ansvaret för informationssäkerhetsarbete ska följa det ordinarie verksamhetsansvaret från ledning ner till enskilda medarbetare. Informationssäkerhetssamordnaren har därmed inget formellt ansvar för informationssäkerheten utan ska verka som ett stöd för att den övriga organisationen innefattande ledning, chefer och medarbetare tar sitt ansvar för informationssäkerhet i verksamheten. Det är viktigt att tydligt klargöra informationssäkerhetssamordnarens roll och vilket mandat och rapporteringsplikt som ska ingå i rollen.

Utbildning och kommunikation

MSB:s metodstöd ställer krav om ständig utbildning och kommunikation för att höja medvetenheten och kunskapen om informationssäkerhet. Utbildning och kommunikation ökar också acceptansen av och förståelsen för de säkerhetsåtgärder som implementeras.

Riskanalys och informationsklassning

Genom en riskanalys ska verksamheten identifiera de hot och oönskade händelser som kan leda till negativa konsekvenser för organisationen. Riskanalyser kan göras verksamhetsövergripande, för en process eller för ett enskilt objekt. Risker och potentiella händelser som kan leda till negativa konsekvenser beskrivs och bedöms sedan avseende sannolikheten att de inträffar samt potentiella konsekvenser.

Metodstödet anger vidare att informationsklassning är en förutsättning för att skapa rätt skydd för informationen som hanteras i respektive verksamhet. Med en gemensam klassningsmodell kan organisationens informationstillgångar skyddas utifrån interna och externa krav på informationens konfidentialitet, riktighet och tillgänglighet. Skyddsnivåerna beskriver säkerhetsåtgärder som informationens värde kräver. Identifierat behov av säkerhetsåtgärder utgör ett viktigt underlag vid exempelvis kravställning av tjänster, som interna och externa it-tjänster. De identifierade behoven av säkerhetsåtgärder bör dokumenteras i en åtgärdsplan. It-säkerhetsåtgärder rent tekniskt kan vara en del men klassningen kan även ha identifierat behov av kompletterande risk- och konsekvensanalyser, förbättrade rutiner eller andra åtgärder som bedöms nödvändiga för att säkerställa säkerheten för informationstillgångarna.

Skyddsåtgärder

Informationstillgångar består av information och resurser som används för att hantera information. Själva informationen är den primära tillgången som ska klassas. Resurser som används för att hantera informationen, till exempel it-system och fysiska tillgångar, samt rutiner i verksamheten ska sedan utformas enligt skyddsnivåer som matchar klassningens resultat. De resurser som hanterar informationen behöver därför skyddas på lägst den nivå som högst klassad information har.

I MSB:s föreskrift för säkerhetsåtgärder i informationssystem framgår att systemägaren behöver ha en dialog med berörda informationsägare inom organisationens olika verksamheter för att införa de säkerhetsåtgärder som ger rätt nivå av skydd för informationssystemet. Behovet av säkerhetsåtgärder identifieras utifrån de informationsklassningar och riskbedömningar som informationsägaren har genomfört, samt systemägarens egna riskbedömningar för informationssystemet.

MSB:s metodstöd beskriver att övervakning anger status för ett system, en process eller en aktivitet. Övervakning sker ofta kontinuerligt genom exempelvis att loggar i ett it-system övervakas och avvikelser automatiskt rapporteras. Övervakning och mätning görs för att bedöma om implementerade säkerhetsåtgärder har avsedd verkan och fungerar tillfredsställande.

Uppföljning och förbättringsarbete

För att ledningen på strategisk nivå ska få en samlad bild och kunskap om informationssäkerhetsarbetet i organisationen behöver det ske en övergripande uppföljning av arbetet som sedan rapporteras under ledningens genomgång. Uppföljningen utgör även underlag för eventuella beslut på strategisk nivå angående åtgärder och resursfördelning.

Resultatet från ledningens genomgång ska dokumenteras och bevaras.

Interna styrdokument

Enligt MSB bör ledningen se till att organisationen antar en policy för informationssäkerhetsarbetet. I ytterligare styrdokument, riktlinjer och liknande kan ledningen ge vägledning till chefer och övriga medarbetare över de krav och förhållningssätt som gäller i informationssäkerhetsarbetet.

I riktlinjer är det vanligt att det förs in bestämmelser om till exempel:

- användning av internet och e-post
- åtgärder till skydd mot skadlig kod
- fysisk säkerhet
- incidenthantering
- kontinuitetsplanering
- mobilt arbete
- inventarier och licenser
- behörighetsadministration
- loggning

Det är viktigt att alla i en organisation känner till och förstår innehållet i policys och riktlinjer. Erfarenheten visar tydligt vikten av att anställda uppvisar ett säkert beteende i sitt dagliga arbete.