Informationssäkerhetsberättelse 2022

Beslutad 2023-03-29 § 32, av: Regionstyrelsen

REGION JÄMTLAND HÄRJEDALEN

Sammanfattning/bakgrund

Regionens arbete med informationssäkerhet syftar till att stödja det övergripande målet att rätt information når rätt person i rätt tid. Detta ska bidra till en välfungerande verksamhet och att regionen kan nå målen med sitt uppdrag till medborgarna.

Den allmänna insikten har under året fördjupats ytterligare om att den information som regionen hanterar har ett mycket stort värde för organisationen och dess medarbetare. Kan den användas på rätt sätt finns en mycket stor potential att dra nytta av för organisationen i form av effektivare arbetsflöden och bättre beslutsunderlag. Därför behöver ökat fokus och resurser läggas på att säkerställa att denna potential kan nyttjas på ett bättre sätt än tidigare varit möjligt. Detta kan ske inte minst genom ökad digitalisering.

Under 2022 har landets säkerhetsläge ytterligare försämrats baserat på alltmer avancerade och allvarliga cyberhot. Konsekvenser av detta är ökade risker för stöld/läckage av känslig information, sabotage, spioneri och utpressning/ekonomisk brottslighet. Tidigare resurser som lagts på proaktiv säkerhet har visat sig otillräckliga utifrån den riskbedömning som sker löpande. Den avvägning som görs mellan insatser för att skydda informationen och de faktiska hoten pekar på att det krävs en relativt sett stor ökning av tilldelade resurser om inte regionens informationstillgångar ska utsättas för oacceptabla risker.

Under 2022 har en ny organisatorisk enhet för informationsförvaltning skapats inom regionstaben. Enheten kommer att ansvara för ledning och stöd inom regionens informationsförsörjning där bland annat informationssäkerhet och dataskydd är ingående delar.

Regionen har gått från att tidigare i egen regi ansvarat för att lokalt drifta IT-lösningar som hanterar informationen till att i allt större grad förlita sig på externa leverantörer av driftlösningar i form av molntjänster. Detta innebär att nya hotbilder behöver kunna hanteras jämfört med tidigare läge.

Digitaliseringen har också ökat i takt, något som bidrar till att ett utökat fokus krävs på att säkra informationen som hanteras i IT-stöden så att den är riktig, tillgänglig när det behövs och att den inte blir åtkomlig för obehöriga. Detta innebär ett i grunden annorlunda arbetssätt jämfört med tidigare för regionens verksamheter. Följder blir bland annat behov av en annan, utökad kompetens jämfört med tidigare för att kunna utföra sitt uppdrag på bästa sätt.

Det allt större beroendet till digitala lösningar/arbetssätt understryker också vikten av fungerande reservrutiner i verksamheten, i händelse av att de digitala stöden inte går att nå.

Informationssäkerhetsberättelse 2022
Dnr RS/38/2023

Handläggare
Lars Christerson
Informationsförvaltning

Region Jämtland Härjedalen
Box 654, 831 27 Östersund
www.regionjh.se

Informationssäkerhetsberättelse 2022
Dnr RS/38/2023

Handläggare
Lars Christerson
Informationsförvaltning

Region Jämtland Härjedalen
Box 654, 831 27 Östersund
www.regionjh.se

INNEHÅLL

1 Informationssäkerhetsberättelse 2022

Informationssäkerhetsberättelsen beskriver Region Jämtland Härjedalens arbete inom områdena informationssäkerhet för det gångna verksamhetsåret.

1.1 Måluppfyllnad 2022 – verksamhetsmål

Följande verksamhetsmål finns kopplade till informationssäkerhet för 2022.

Mål		Utfall 2022-12-31	Målvärde 2022-12-31
E-utbildning medarbetare *Inriktningsmål: Regionens samtliga medarbetare ska ha genomgått grundutbildning i informations-säkerhet och dataskydd* Andel av nu aktiva medarbetare som genomfört e-utbildning med godkänt resultat	Regionen totalt	46%	80%
	Regionstaben	48%	80%
	Hälso- och sjukvårdens förvaltningsområde	41%	80%
	Regional utvecklings förvaltningsområde	57%	80%
Kartläggning och värdering av information *Inriktningsmål: Regionens viktigaste informationstillgångar ska vara kartlagda och informationsklassade* Informationsklassning ska genomföras och vara dokumenterad för samtliga prioriterade informationstillgångar	Hur många verksamheter som genomfört informationskartläggning För identifierade informationstillgångar i respektive kartläggning: hur stor andel av tillgångarna som har informationsklassats	Informations—tillgångar har ännu inte identifierats på strukturerat sätt i styrningen för de flesta verksamheter *Utfall saknas*	50% av prio-riterade tillgångar är klassade
Tydligt ägarskap och styrning *Inriktningsmål: Regionen har ett tydligt och utpekat ägarskap för sina informationstillgångar* Samtliga prioriterade informations-tillgångar har utsedda och dokumenterade informationsägare	Baseras på att verksamhetens viktigaste informationstillgångar har kartlagts (enligt föregående mål) och att dessa informations-tillgångar kopplats till/ tilldelats en namngiven informationsägare	Rollen informations-ägare har ännu inte etablerats i styrningen *Utfall saknas*	100% har utpekat ägarskap

Analys av måluppfyllnad: Måluppfyllnaden visar på att aktiviteter i verksamheten kopplade till informationssäkerhet ännu inte genomförs på ett fullständigt och strukturerat

sätt. Orsaker till detta är flera:

- Oklar ansvarsfördelning och ägande roller kopplade till verksamhetens information.
- Omogen säkerhetskultur – ”säkerhet angår inte mig” alternativt att ”säkerhet sköts av andra i organisationen och inte av mig” – vilket påverkar vilken vikt verksamheterna tillmäter utbildningar i säkerhet.
- Målet att genomföra informationsklassningar kan inte på ett adekvat sätt fördelas ”i linjen” eftersom informationstillgångarnas indelning inte följer linjeorganisationen utan produceras/konsumeras i arbetsflöden och inte strikt efter hur linjeorganisationen för tillfället är utformad. Därmed kan målet inte heller fördelas/följas upp via aktiviteter indelade efter linjen.
- Uppföljning av målet kopplat till genomförandegrad för e-utbildning har försvårats för verksamheterna. Orsaken är att kännedom kring uppföljningsstöd i Kompetensportalen och hur det används ännu inte är känt hos de flesta chefer.
- Bristande metodstöd i det systematiska säkerhetsarbetet – brister i resurstilldelning för stödjande arbetet (med kartläggningar, klassningar).
- Brister i den övergripande styrningen – ”den röda tråden” från övergripande mål till verksamheternas aktiviteter gör att alla mål inte har fördelats ned till aktiviteter till verksamheterna.

Inför 2023: Det behöver till kommande planeringsperiod 2023 bli tydligare till vilka nivåer i organisationen som målen ska fördelas till samt vilka aktiviteter som ska utföras och vilka som ska rapportera i uppföljningen. Det är för 2022 en risk att målen inte har fördelats ned på aktiviteter som ska utföras i verksamheterna i rätt omfattning. Därmed blir styrningen inte helt igenom adekvat och möjlig att följa upp på rätt sätt.

1.2 Uppföljning av aktiviteter prioriterade för 2022

För prioriterade åtgärdsområden inför 2022 (se föregående årsberättelse för år 2021) är status per 2022-12-31 följande.

Prioriterat område för 2022 och framåt	**Status**
1. Tillhandahålla ett adekvat metodstöd för informationskartläggning – informationsklassning	**Pågår.** Metod för kartläggning finns beskriven. Klassningsmodell har uppdaterats. Digitalt stöd för klassning under införande.
2. Förbättra regionens behörighetshantering genom att förbereda för att införa en central behörighetsstyrande källa	**Ännu ej planerad.** Beslut om etablering och införande av central behörighetskälla har inte fattats av regionledningen.
3. Göra det enklare för medarbetarna att göra rätt i den dagliga informationshanteringen – ökat fokus på det användarnära stödet	**Pågår.** Övergripande hanteringsregler för information med olika känslighetsnivåer beslutade och införda 2022. Mer och tydligare stöd som är tillgängligt i situationsanpassad form under utveckling.
4. Tidigare genomförd säkerhetsanalys baserad på ett urval kontroller från ramverket ”CIS Controls” (critical security controls) följs upp – i syfte att minska risker med cyberangrepp	**Ännu ej planerad.** Uppföljning av ”CIS Controls” med åtgärdsbeslut krävs för att ge underlag att bättre kunna hantera cyberhot.

Prioriterat område för 2022 och framåt	Status
5. Det systematiska dataskyddsarbetet för skydd av personuppgifter utökas genom uppföljning av vilka skyddsåtgärder som är införda	**Ej planerad/minskning av resurser.** Heltidstjänst som dataskyddshandläggare har tagits bort under 2022. Detta innebär en minskad ambitionsnivå för dataskydds-arbetet jämfört med tidigare period t o m 2021.
6. Format på underlaget till ledningens genomgång för området informationssäkerhet vidareutvecklas för att få en bättre styrning av säkerhetsarbetet	**Ännu ej infört.** Förslag på förbättringar av redovisning och beslutsgång för ledningens genomgång föreslagna för ledningen (inväntar återkoppling om vidare arbete).
7. Systematisk incidenthantering med rapportering och uppföljning av inträffade säkerhetsincidenter införs	**Ännu ej infört.** Arbetssätt och rutin för systematisk uppföljning av incidenter ännu inte införda.

2 Inträffade säkerhetsincidenter under året

Enstaka säkerhetsincidenter har förekommit då medarbetare klickar på länkar som leder till nedladdning av skadlig kod (phishing). Detta har i vissa fall fått till följd att information har raderats och att serverkonfigurationer har påverkats vilket orsakat felfunktion, något som dock kunnat återställas i rimlig tid.

De flesta rapporterade säkerhetsincidenter avser handhavandefel där information har skickats till fel mottagare eller där pappersbaserad information med känsliga uppgifter förvarats i utrymme där obehöriga kan komma åt den. Det är därför väsentligt att minska riskerna för att sådan exponering/läckage av information sker, exempelvis genom att digitalisera informationsflödena i högre grad för att undvika pappersbaserade informations-bärare. Ökad automation av arbetsuppgifter minskar också, generellt sett, riskerna med felaktigt handhavande av information.

3 Riskanalyser, revisioner och internkontroller

3.1 Uppföljningar och revisioner av informationssäkerheten

Under året har nulägeskartläggningar genomförts av processen för behörighetstilldelning för några centrala verksamhetssystem. Detta arbete visar på behovet av att vidareutveckla behörighetshanteringen inte minst genom högre grad av automation. Förbättringar syftar till att effektivisera och spara tid genom bättre flöden som gör att medarbetarna snabbare kan få tillgång till rätt behörigheter och därmed rätt information i rätt tid. Dessutom pekar resultatet på ett stort behov av att genomföra löpande kontroller och återgodkännanden av

aktuella tilldelade behörigheter så att dessa överensstämmer med gällande behov hos medarbetarna. Detta bedöms kunna höja den totala säkerheten i hög grad.

Medarbetarutbildning: När det gäller regionens grundläggande e-utbildning i informationssäkerhet, obligatorisk för samtliga medarbetare, visar resultatet för 2022 glädjande nog en relativt stor ökning från ca 28% av medarbetarna som slutfört utbildningen med godkänt resultat per 2021 till ca 41% för motsvarande andel per 2022. Detta resultat gäller för medarbetarna inom hälso- och sjukvårdens förvaltningsområde. Motsvarande siffra för hela regionen är 48% av medarbetarna som genomfört utbildningen. Resultatet är dock långt från verksamhetsplanens målvärde 80% genomförandegrad per 2022-12-31.

Denna totalt sett låga genomförandegrad får negativa konsekvenser i slutänden då det gäller medarbetarnas säkerhetsmedvetande och förutsättningar för att uppnå goda arbetssätt i informationshanteringen. Detta påverkar såväl patientsäkerhet som effektivitet och arbetsmiljö.

Extern revision av SITHS-korthanteringen: Under våren 2022 genomfördes en extern revision av regionens SITHS-korthantering (e-tjänstekort) vilken utgör grunden för en tillförlitlig identifiering av våra medarbetare. Revisionen utfördes av Inera AB:s revisionsteam för SITHS och visade på ett antal förbättringsområden, däribland behov av en förbättrad interkontrollprocess för SITHS-kortens utgivning. Denna utgivningsprocess ska säkerställa att regionens medarbetare får tillgång till en nationellt beslutad metod att verifiera sin identitet vilket bidrar till en trygg och robust tillgång till även känsliga uppgifter. Detta tillför värden/tillit för såväl patienter som övriga medborgare då det gäller att deras uppgifter hanteras på rätt sätt och inte läcker till obehöriga.

3.2 Nya riskbedömningar – övergripande riskanalys 2022

Under 2022 har den övergripande riskanalysen för regionens informationssäkerhetsrisker uppdaterats. Den största enskilda risken som identifierats på den övergripande nivån är fortsatt (kvarstår sedan år 2020) bristande medvetenhet hos medarbetarna om hur informationen ska hanteras enligt gällande regelverk (s.k. ”oavsiktligt insiderhot”). Risker i topp är för 2022 samma som för 2021 med den skillnaden att risken för allvarliga cyberangrepp har ökat ytterligare jämfört med föregående år, främst orsakat av det försämrade säkerhetsläget i omvärlden. Regionen behöver höja sin förmåga att motstå cyberhot som riktar sig specifikt mot hälso- och sjukvårdsverksamhet, en sektor som MSB under året pekat ut som särskilt utsatt för denna typ av angrepp.

3.3 Riskarbete i verksamheterna

När det gäller riktade riskanalyser inom informationssäkerhet kopplade till vårdverksamheten så har år 2022 liksom 2021 varit präglat av den vårdskuld som byggts upp under coronapandemin. Konsekvenser av detta har för informationssäkerhetsområdet inneburit att antalet riktande riskanalyser som kunna genomföras inom vårdverksamheten har sjunkit jämfört med perioden innan pandemin. Orsaken är att vårdens medarbetare inte kunnat sätta av tid i den omfattning som hade behövts för att bedriva ett förebyggande arbete för informationssäkerhetsrisker.

Fokus för informationssäkerhetsfunktionen har varit att bistå vid informationsklassningar för den information som hanteras i nya IT-stöd som ska införas. Detta lägger en grund för att senare kunna arbeta mer aktivt med riskbedömningar kopplat till denna information och dess värde (bedömd via klassning).

4 Genomförda förbättringar

4.1 Ny enhet för informationsförvaltning etableras 2022

Den största enskilda förbättringen kopplat till regionens informationssäkerhet för år 2022 är tillkomsten av en ny enhet för informationsförvaltning, placerad under Samordningskansliet (Regionstaben). Denna nya enhet har som uppdrag att ta fram styrning och stöd för hur regionens informationstillgångar ska hanteras på bästa sätt. Det övergripande syftet med enhetens arbete är att bistå med att säkra en robust, effektiv och lagenlig informationsförsörjning för regionens samtliga verksamheter. Detta är helt i linje med de syften som finns för regionens informationssäkerhetsarbete som utgör en del i säkringen av informationsförsörjningen i stort.

4.2 Uppdaterade riktlinjer för IT-säkerhet

Under året har riktlinjer för IT-säkerhet uppdaterat för att återspegla aktuella krav. Detta ger större förutsättningar att motstå vanligt förekommande hot mot vår IT-miljö.

4.3 Vidareutvecklad IT-arkitektur

Utformningen av regionens lokala IT-infrastruktur (nätverk och servermiljö) har vidareutvecklats för att bättre motsvara kraven på en robust IT-arkitektur som kan motstå cyberhot och oavsiktlig spridning av skadlig kod.

4.4 SOC-tjänst övervakar IT-miljön

Under året har en ny s.k. SOC-tjänst (Security Operations Center) anskaffats och aktiverats för regionens IT-miljö. Tjänsten tillhandahåller en löpande övervakning och incidentrespons för säkerhetshot. Den bidrar till en högre förmåga att upptäcka och minimera effekten av cyberangrepp och andra typer av incidenter.

4.5 Etablering av digitalt stöd för informationsklassning och riskanalyser

Under året har ett nytt digitalt stöd (DIGframe) för att dokumentera och följa upp informationsklassningar och riskanalyser börjat etableras inom regionen. Stödet DIGframe används sedan tidigare inom regionen för att hantera regionens centrala registerförteckning för personuppgifter (dataskydd – GDPR) samt, i viss utsträckning, för att dokumentera arbetet med förvaltning av IT-stöd (”objektförvaltning”). Att stödet nu börjar användas även för informationssäkerhet innebär ett viktigt steg framåt för det systematiska arbetet med säkerhet.

4.6 Utveckling av kravkatalog

Under året har en strukturerad kravkatalog med styrande skyddsåtgärder kopplat till klassningsnivåer vidareutvecklats för att stödja ett systematiskt säkerhetsarbete. Kravkatalogen kommer att underlätta en enhetlig och tydlig kravställning gällande vilka typer av skydd som ska finnas införda för att säkra informationsförsörjningen baserat på informationens skyddsbehov.

4.7 Arbete med att kravställa funktioner för ett EDR-skydd

Merparten av de hot och risker som verksamhetens information/IT-miljö utsätts för har sin utgångspunkt från det som händer på klientplattformarna (PC:ar, tunna klienter och mobila enheter). Klienterna är ”ingången” för cyberhot som exempelvis skadlig kod, särskilt *ransomware* som kan spridas vidare till övriga IT-miljön. Hur stora risker (med ev. incidenter som följd) som kan uppstå beror direkt och indirekt på hur regionens medarbetare agerar i sina dagliga arbetsuppgifter då de använder IT-verktygen. Därför behövs ett heltäckande skydd som utgår från om medarbetarna via sina användningssätt ger upphov till säkerhetsrisker.

Ett sätt att upptäcka och förhindra att drabbas av allvarliga cyberhot är att införa s.k. EDR-skydd (Endpoint Detection and Response). Under 2022 har arbetet med att kravställa på ett EDR-skydd påbörjats. Detta skydd syftar till att komplettera de befintliga skydd som redan finns aktiva och för att ta höjd för de cyberhot som hela tiden utvecklas i hög takt och behöver kunna bemötas på ett tillräckligt bra sätt. Moderna EDR-skydd innehåller en kombination av situationsanpassad varningsinformation till användaren om denne försöker utför riskfyllda åtgärder (som att försöka skicka patientinformation via öppen e-post) samt aktivering av larmhändelser vid andra onormala, riskfyllda användningsmönster. Detta ger ökad motståndskraft mot såväl oavsiktliga fel som avsiktliga fel (antagonistiska hot). Effekten av att införa skyddet bedöms vara såväl större medvetenhet hos användarna om vad som är säkra arbetssätt som en större kunskap om hur regionens IT-miljö används i stort och i vilken grad riskfyllda användningsmönster förekommer.

5 Prioriterad inriktning för fortsatt arbete

5.1 Etablering av rollen informationsägare

För att skapa en grund för det systematiska informationssäkerhetsarbetet krävs ett ramverk med tydliga roller och mandat kopplat till regionens informationstillgångar. Den enskilt viktigaste rollen i detta ramverk är *informationsägare*. Till rollen kopplas mandat och ansvar att säkerställa att de informationstillgångar som kopplas till respektive ägande roll hanteras på ett adekvat och säkert sätt. Mandat för rollen behöver införas i regionens delegationsbestämmelser liksom övriga ansvarsroller som fördelas från regionstyrelse/ nämnder. Mycket viktigt för att lyckat med etablering av denna roll är att omvärldsbevaka hur andra organisationer har lyckats införa rollen och vad som ska ingå i dess ansvar.

5.2 Stöd för att genomföra informationskartläggningar

En mycket viktig och grundläggande del i det systematiska säkerhetsarbetet är att kartlägga vilken information som används i regionens verksamheter. Detta görs via en fastslagen metodik, *informationskartläggning*, där informationsklassning är en ingående del. För att komma vidare med detta arbete krävs tillgång till gemensamt metodstöd som ska leda och facilitera kartläggningen inom respektive verksamhet. För att klara arbetet behöver resurser tilldelas som kan bistå med metodstödet. Arbetet bör ses som en viktig del i det totala digitaliseringsarbetet och blir en möjliggörare för att snabbare och säkrare kunna öka graden av digitala arbetssätt.

5.3 Strategi för informationssäkerhet

Det är av största vikt att regionen kan ta fram och besluta om en strategi (på verksamhetsnivå, ej politisk nivå) för informationssäkerhet. Strategin ska vara en del av det övergripande området informationsförsörjning där digitalisering samt informationsförvaltning är andra delar.

5.4 Förbättrat arbete med förebyggande riskbedömningar

För att stärka det förebyggande säkerhetsarbetet krävs att ett mer riskbaserat arbetssätt införs. Detta ska stödja att beslut om skyddsåtgärder tas baserat på bedömda risknivåer i förhållande till vilka risker som kan accepteras. För att fungera är detta inte något som kan införas avgränsat för området informationssäkerhet. Istället krävs att riskbaserad styrning av verksamheten utförs genomgående utifrån olika områden som patientsäkerhet, ekonomi, personal och informationshantering. Genom medvetna beslut om förbättrande åtgärder baserat på risknivåer kan en mer robust, effektiv och säker verksamhet uppnås där god informationssäkerhet bidrar med delar i förbättringarna. Detta kräver god överblick och enkel tolkning av förekommande risker hos regionens beslutsfattare.

Ekonomisk styrning av hur skyddsåtgärder finansieras: I syfte att få till en mer proaktiv hantering/beslut för vilka skyddsåtgärder som ska införas behöver risker kunna kvantifieras tydligare i ekonomiska termer. Först då blir det möjligt att kunna uppnå ett systematiskt och rätt avvägt säkerhetsarbete med vilket vi inte betalar för ”onödiga åtgärder” och inte heller missar att införa ”nödvändiga, rätt anpassade åtgärder”. Detta förbättringsområde kräver att flera olika discipliner och funktionsområden inom regionen samarbetar och där fokus läggs på ekonomi och tillhörande kvalitets-/säkerhetsbristkostnader.

5.5 Införande av säker kommunikation via nationella SDK-tjänsten

Genom att ansluta till den nationella SDK-tjänsten (Säker Digital Kommunikation) för offentlig sektor kan regionen förbättra sina informationsflöden avsevärt. Detta bygger på att en stor del av regioner, kommuner och myndigheter ansluter sig till SDK för att på så sätt kunna utbyta information på ett säkert och snabbt sätt mellan sig. SDK överför meddelanden mellan funktionsadresser som kan nås från samtliga anslutna parter.
I dagsläget saknas en motsvarande tjänst/infrastruktur vilket gör att såväl faxar som papperspost fortfarande behöver användas för överföringen, något som är dyrt, långsamt och osäkert.

5.6 Utbildning, stöd och information

För att stödja medarbetarna i att arbeta på ett säkert sätt och undvika riskfyllda beteenden krävs att ett väl utformat stöd i form av instruktioner, lathundar och utbildningar finns i de situationer de behövs. Utbildning behöver i högre grad än tidigare ges situationsanpassat i ”små portioner” till medarbetare. Då kommer det att upplevas mer relevant och användbart jämfört med om utbildning ges i generell form riktad till samtliga medarbetare i separata ”förebyggande” utbildningar.

5.7 Kontrollerad användning av höga behörigheter

Ett stöd för att systematisera hanteringen av privilegierade, höga behörigheter (för driftpersonal) i IT-miljön har anskaffats och arbetssätt kopplat till detta kommer att vidareutvecklas under det kommande året.

5.8 Kontroll av IT-miljöns komponenter

Fokus kommer under kommande år att läggas på att förbättra inventering och kontroll av såväl hård- som mjukvara i den lokala IT-miljön. Detta innebär automatisk detektering av vilken utrustning som finns ansluten och att inte inaktuell, sårbar mjukvara används i miljön. Detta syftar till att minimera påverkan av kända sårbarheter på den totala säkerhetsnivån.

5.9 Central behörighetskälla

Regionens medarbetare behöver åtkomst till många olika IT-stöd under sin arbetsdag. Varje IT-stöd hanterar roller och behörigheter för att styra denna åtkomst. I dagsläget hanteras merparten av dessa roller/behörigheter manuellt i varje IT-stöd för sig. Detta skapar en mycket stor administrativ arbetsbörda när det gäller att lägga in nya användares behörigheter och hålla befintliga användares behörigheter aktuella mot behoven. Det manuella arbetssättet innebär också långa ledtider innan nödvändiga behörigheter är på plats och en osäker, reaktiv hantering.

Genom att bygga upp en central behörighetskälla där roller uppdateras på ett ställe för varje medarbetare och sedan med automatik kan överföras och uppdatera merparten av IT-stöden kan vi komma bort från den manuella hanteringen. Nästa steg för denna utveckling är att göra en kostnadsuppskattning för nuläget där mycket arbetstid läggs på manuell behörighetshantering. Denna kostnad kan sedan ställas mot vad en automatisering kan spara för belopp årligen för att få underlag till investering i en förbättrad behörighetshantering.

5.10 Förbättrad hantering av säkerhetsincidenter

Regionen har mycket höga krav på sig att hantera säkerhetsincidenter på ett tydligt och systematiskt sätt. Det s.k. NIS-direktivet (med tillhörande lag om informationssäkerhet för samhällsviktiga tjänster) började gälla från 2018 och kommer under 2023 att utökas ytterligare i form av NIS2 med bland annat mer detaljerad tillsyn. Explicita krav på utbildning och övning för ledningsbefattningar kommer också att gälla. För att uppfylla de nya kraven krävs en väl genomtänkt intern hantering av inträffade säkerhetsincidenter i syfte att kunna upptäcka, förebygga/ lära av samt rapportera incidenter (både internt och externt till MSB). Regelverket har ett sanktionssystem där överträdelser kan beläggas med

höga sanktionsavgifter, vilkas belopp också höjs då NIS2 börjar gälla. Förbättringsarbetet kring denna incidenthantering behöver prioriteras under 2023.