www.pwc.se

Revisionsrapport

Samlad bedömning Informations- och cybersäkerhet

Region Gävleborg

Karin Magnusson
Carl Thorn
Gabrielle Stööp
Viktor Persson

Maj/2019

pwc

Innehåll

Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Region Gävleborg genomfört en granskning av informations- och cybersäkerhetsarbetet i regionen. Denna granskning har innefattat en inledande dokumentgranskning samt intervjuer med intressenter inom regionen.

Dokumentgranskningen har omfattat relevanta styrande dokument som berör områdena informations- och cybersäkerhet. Inom ramen för granskningen har intervjuer genomförts med tjänstemän inom huvudsakligen it[1]-förvaltningen, funktionen för informationssäkerhet och funktionen för fysisk säkerhet.

Revisionsfrågan som besvaras lyder:

- *Har Regionstyrelsen säkerställt att Region Gävleborg har ett ändamålsenligt arbete med att identifiera, prioritera och hantera säkerhetshot och incidenter som kan påverka regionens informations- och cybersäkerhet?*

Den **sammantagna revisionella bedömningen** är att regionstyrelsen, *i begränsad utsträckning*, har säkerställt att Region Gävleborg har ett ändamålsenligt arbete med att identifiera, prioritera och hantera säkerhetshot och incidenter som kan påverka regionens informations- och cybersäkerhet.

Den sammanfattande bedömningen baseras på en sammanvägning av bedömningarna för nedanstående kontrollmål.

Revisionell bedömning har skett utifrån följande skala/gradering:

Ej uppfyllt
I begränsad utsträckning
Till övervägande del
Helt uppfyllt

Kontrollmål	Revisionell bedömning
Har regionen förmåga att styra och följa upp risk- och säkerhetsarbetet på ett sätt som förutsättningar, interna och externa regler kräver?	**I begränsad utsträckning** Det finns ett aktivt arbete med informations- och cybersäkerhet. Informationssäkerhetsansvarig och it-ansvarig är nya på sina positioner och har inlett ett förbättringsarbete i sina respektive områden. Det saknas dock styrande dokumentation inom båda områdena. Utan styrande dokumentation och aktiv uppföljning är det

[1] Informationsteknik: *system för att samla in, lagra och bearbeta presentera och överföra data*

	svårt att säkerställa ändamålsenlig hantering. Vidare finns brister inom styrningen av informationssäkerhet då funktionen inte har en egen budget samt informationssäkerhetsansvarig inte har tillräckligt mandat för att säkerställa ett systematiskt arbete över hela regionen. Det finns ingen systematisk, dokumenterad måluppföljning inom informationssäkerhet och därmed inget sätt att följa upp det arbete som bedrivs. Det pågår ett arbete med att kartlägga samtliga processer i regionen för att ha översyn över regionens samtliga informationstillgångar men detta arbete är ännu inte klart. I leverantörshanteringen ingår informationssäkerhet idag till viss del men det behöver säkerställas genom en kravställande dokumenterad process.
Har regionen förmåga att utveckla och genomföra lämpliga skyddsåtgärder för att säkerställa leverans av kritiska tjänster samt skydda system och information?	**I begränsad utsträckning** Region Gävleborg har flera mekanismer på plats för att för att säkerställa leverans av kritiska tjänster samt skydda system och information. Tekniska lösningar vars syfte är att garantera detta används utbrett i inom it-miljön. Vidare verkar säkerhetsansvarig personal vara väl införstådd i relevanta, gängse skyddsprinciper såsom “lägsta behövda behörighet”. Fastän skydden i stort tycks fungerar bra finns tillkortakommanden i arbetet. Det mest märkbara är att det i många fall saknas dokumenterade, etablerade rutiner. Ofta förlitar sig personal på gruppöverenskomna “best practices”. Detta skapar ett personberoende. Ett annat övergripande tillkortakommande som framgick av intervjuerna är att det saknas systematiskt arbete för att höja chefers och andra medarbetares förståelse för säkerhetsfrågor. För flera lösningar saknas vissa tillämpningar som skulle göra lösningarna än mer effektiva. Vissa system är särskilt konfigurerade, medan andra utgår ifrån standardiserade bas-

	konfigurationer som skulle kunna anpassas.
Har regionen förmåga att utveckla och genomföra lämpliga aktiviteter för att identifiera förekomsten av informations- och cybersäkerhetshändelser?	**I begränsad utsträckning** Region Gävleborg har flera lösningar på plats för att förhindra angrepp och flagga suspekta avvikelser på klient- och serversystem och i nätverkstrafik. Dessutom genomförs omfattande loggning. Ett genomgående tema är att det saknas dokumenterade, etablerade rutiner. Detta får konsekvenser för arbetet då det riskerar att bli bristfällig systematik i arbetssätt, frekvens och ansvarsfördelning. Vidare är personalen som i nuläget tar emot och hanterar avvikelser inte tränad i cybersäkerhet, och därav hämmas regionens förmåga att agera tillfredsställande på avvikelser.
Har regionen förmåga att utveckla och genomföra aktiviteter för att vidta lämpliga åtgärder avseende en upptäck informations- eller cybersäkerhetsincident?	**I begränsad utsträckning** It-incidenter och informationssäkerhetsincidenter rapporteras och hanteras på två olika sätt. Det finns ingen övergripande bild över samtliga informationssäkerhetsincidenter. Vidare är samordningen mellan it-avdelningen och informationssäkerhetavdelningen bristfällig vad det gäller incidenthantering. Det har inletts ett arbete för att förbättra detta men i dagsläget finns det brister. En ytterligare orsak är bristande styrande dokumentation kring incidenthantering inom informationssäkerhetsområdet. Det finns ett utkast till ny rutin för incidenthantering men denna är ännu inte antagen.
Finns ändamålsenliga planer för att återställa IT-driften vid incidenter och kriser t.ex. IT-haveri?	**I begränsad utsträckning** Funktionen för informationssäkerhet ska tillhandahålla en övergripande kontinuitetsplan som verksamheten sedan ska använda för att skapa egna, specifika planer. Detta finns inte på plats i dagsläget och det finns därmed en brist i kontinuietsplanering inom informationssäkerhetsområdet. It arbetar med kontinuitetsplanering i sina tillgångar. Det genomförs tester av kontinuitet i it-miljön. Arbetet med kontinuitetshantering på it-förvaltningen sker dock inte på ett systematiskt sätt och det fattas en stor del dokumenterade processer för detta.

Sammanfattande rekommendationer

Baserat på ovan bedömning är granskningens övergripande rekommendationer:

- Att styrande dokument inom både informations- och cybersäkerhet fastställs
- Att dokumenterade processer för arbetet med informations- och cybersäkerhet fastställs
- Att arbetet med informationssäkerhetsrisker formaliseras och systematiseras
- Att incidenthanteringsprocessen samordnas genom samverkan mellan informationssäkerhetsavdelningen och it-avdelningen
- Att det säkerställs att funktionen för informationssäkerhet har tillräckligt med mandat för att bedriva sitt uppdrag samt förvaltar sin egen budget
- Att utbildningar och kompetenshöjande aktiviteter genomförs inom området cybersäkerhet

Detaljerade rekommendationer finns under respektive kontrollmål.

1. Inledning

1.1. Bakgrund

Den pågående digitaliseringen ger möjligheter att höja kvalitet, säkerhet och effektivitet i regionens olika verksamheter och förbättra service till medborgare, organisationer och företagare. Den andra sidan av myntet målar dock en annan bild, nämligen att allt fler inom privat- som offentlig sektor drabbas av allvarliga attacker, intrång, läckage och avbrott. Årliga rapporter från bl.a. Försvarets Radioanstalt (FRA), Säkerhetspolisen (SÄPO), Militära underrättelse- och säkerhetstjänsten (MUST) och Myndigheten för samhällsskydd och Beredskap (MSB) beskriver sammantaget att hotbilden blir allt mer påtaglig, komplex och allvarlig.

I oktober 2018 publicerades MSB:s rapport *En bild av landstingens informationssäkerhetsarbete 2018* och där konstateras att det råder brist på strategier, åtgärder resurser och kompetens inom informationssäkerhetsområdet.

2017 beslutade regeringen om en ny nationell informations- och cybersäkerhetsstrategi. I denna strategi ingår att säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet på alla nivåer i samhället. Regioner berörs i allra högsta grad av denna strategi och ska inneha ett systematiskt och riskbaserat informations- och cybersäkerhetsarbete. Detta aktualiseras med EU:s NIS-direktiv (2016/1148) och Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174) med förordning (2018:1175), som är införlivningen i den svenska rättsordningen. Övergripande med NIS-direktivet är ett mål om att uppnå en hög gemensam lägstanivå inom cybersäkerhet i EU. Regioner levererar ett antal samhällsviktiga tjänster såsom hälso- och sjukvård samt transport och påverkas därmed av lagarna. Vidare, en rad andra regelverk berör informationssäkerhet, inte minst GDPR.

Regionens revisorer har med hänsyn till risk och väsentlighet bedömt det angeläget att göra en granskning inom ovan rubricerat område. Granskningen inleddes med en hotbildsanalys. Resultatet från denna finns dokumenterat i rapporten ”Region Gävleborg Hotprofil”. Hotprofilen har legat till grund för denna mognadsbedömning av regionens informations- och cybersäkerhetsarbete. Hotprofilen är en slags analys av regionens verksamhet och hotbild som finns gentemot verksamheten. Denna analys har därför använts för att avgränsa granskningen och inrikta den på delar i verksamheten som anses vara mest kritiska ur ett informations- och cyberssäkerhetsperspektiv.

1.2. Syfte och Revisionsfråga

Utifrån genomförd riskanalys har revisorerna beslutat att ge PwC i uppdrag att utföra en granskning avseende Regionens informations- och cybersäkerhet. Syftet är att ge revisorerna ett underlag för bedömning av ändamålsenligheten i Region Gävleborgs informations- och cybersäkerhetsarbete i förhållande till de risker som regionen utsätts för.

Den revisionsfråga som denna granskning ska svara på är:

Har Regionstyrelsen säkerställt att Region Gävleborg har ett ändamålsenligt arbete med att identifiera, prioritera och hantera säkerhetshot och incidenter som kan påverka regionens informations- och cybersäkerhet?

1.3. Revisionskriterier

Revisionskriterierna utgörs i huvudsak av:

- Hälso- och sjukvårdslag
- Patientdatalag
- Patientsäkerhetslagen
- Regioninterna styrdokument som rör granskningsområdet

1.4. Kontrollmål

Följande kontrollmål bildar underlag för bedömning:

- Finns en bild av vilka huvudsakliga hotaktörer och hothändelser som utsätter regionen för risk?
- Har styrelsen fastställt vilka risknivåer som är acceptabla?
- Finns ett effektivt informations- och cybersäkerhetsarbete i linje med accepterade risknivåer?
- Finns det hos ledande befattningshavare en god kunskap och förståelse för informations- och cybersäkerhetsarbetet?
- Finns det upprättade policyer och riktlinjer avseende regionens arbete med informations- och cybersäkerhet?
- Är regionens investeringar i informations- och cybersäkerhetsarbete i linje med de brister och den hotbild som föreligger?
- Har regionen förmåga att hantera cybersäkerhetsrisker kopplat till system, personer, information och leverantörer?
- Har regionen förmåga att styra och följa upp risk- och säkerhetsarbetet på ett sätt som förutsättningar, interna och externa regler kräver?
- Har regionen förmåga att utveckla och genomföra lämpliga skyddsåtgärder för att säkerställa leverans av kritiska tjänster samt skydda system och information?
- Har regionen förmåga att utveckla och genomföra lämpliga aktiviteter för att identifiera förekomsten av informations- och cybersäkerhetshändelser?
- Har regionen förmåga att utveckla och genomföra aktiviteter för att vidta lämpliga åtgärder avseende en upptäckt informations- eller cybersäkerhetsincident (incident- och krishantering)?
- Finns ändamålsenliga planer för att återställa it-driften vid incidenter och kriser såsom t.ex. it-haveri (kontinuitetshanteringsplan)?

I granskningen har dessa kontrollmål klustrats för att skapa en rapportstruktur som är lättöverskådlig och relevant för läsaren. Rapporten är därför uppbyggd utefter fem huvudsakliga kontrollmål, där det i inledningen klargörs vilka ytterligare kontrollmål som berörs under respektive avsnitt.

1.5. Avgränsning

Granskningen betonar regionens övergripande informations- och cybersäkerhetsarbete på koncernnivå.

I tid avgränsas granskningen till år 2019 och till granskningens kontrollfrågor.

1.6. Metod[2]

Inför denna granskning har PwC genomfört en hotbildsanalys av Region Gävleborg. Hotbildsanalysen har baserats på en sammanvägning av tillhandahållen dokumentation samt intervjuer med nyckelpersoner inom Region Gävleborgs it- och säkerhetsverksamhet. Telefonintervjuer har genomförts med informationssäkerhetsansvarig, säkerhetschef, it-avdelningschef samt enhetschef för serverdrift och infrastruktur. I övrigt har även PwC:s samlade kunskap kring hotaktörer och den hotbild som finns gentemot hälso- och sjukvårdssektorn använts för att skapa hotbildsanalysen.

Hotbildsanalysen har använts som utgångspunkt till denna granskning av informations- och cybersäkerhet. Hotbilden har används för att skapa en förståelse för de hot och risker som regionen står inför och därmed har granskningen kunnat lägga fokus på sådana delar som är särskilt kritiska.

Granskningen har genomförts genom dokumentgranskning och intervjuer.

Inom ramen för granskningen har vi genomfört två workshops med deltagare från it-förvaltningen och funktionen för informationssäkerhet samt uppföljande intervjuer med ytterligare intressenter bland annat säkerhets- och beredskapschef. Deltagare i respektive workshop var bland annat:

Representanter från informationssäkerhetsavdelningen
- Informationssäkerhetsansvarig
- Informationssäkerhetssamordnare
- Sakkunnig samordnare informationssäkerhet

Representanter från it-avdelningen
- It-säkerhetsansvarig
- Enhetschef Server och Drift
- Objektsförvaltare för diagnostiksystem, förvaltare av incidentprocessen
- Enhetschef för it-support, processägare incident
- Objektsförvaltare för arbetsplats
- Objektsförvaltare för kommunikationsverktyg
- Objektsförvaltare för teknisk plattform

Den dokumentation som ingick i dokumentgranskningen var bland annat:
- Informationssäkerhet, Övergripande direktiv
- Informationssäkerhet, Direktiv för styrande dokument i LIS
- Informationssäkerhet, Direktiv för ansvar och roller
- Informationssäkerhet, Direktiv för molntjänster
- Informationssäkerhet, Direktiv för lagring och kommunikation i digitala kanaler
- Informationssäkerhet, Direktiv för incidenthantering (utkast)
- Informationssäkerhet, Direktiv för systematiskt och riskbaserad informationssäkerhetsarbete (utkast)

[2] För definitioner av begreppen informationssäkerhet, cyberssäkerhet, cyberhot m.m. se http://www.fsb.org/2018/11/cyber-lexicon/

- Informationssäkerhet, Rutin för systematisk och riskbaserat informationssäkerhetsarbete (utkast)
- E-postdirektiv
- It-strategi
- Beslut ny IT-funktion, rutin
- Beslutsunderlag ny IT-funktion, mall
- Risk- och sårbarhetsanalys
- Rutin, Incidenthantering it-avdelningen

Metoden för analys av dokumentation och genomförande av intervjuer har baserats på NIST Framework for Improving Critical Infrastructure Cybersecurity V1.1[3] (”Cybersecurity Framework”, ”CSF”. Detta är en standard som har tagits fram för att stärka informationssäkerheten i samhällskritisk infrastruktur och är heltäckande och mappad mot andra erkända standarder som Center for Internet Security (CIS) Top 20 och ISO 27001.

NIST CSF innehåller en mognadsskala från 1-5. Vi har använt denna skala för att ge regionen en initial mognadsbedömning. Denna bedömning har sedan översatts till revisionens bedömningskriterier som består av en skala från 1-4 (ej uppfyllt, i begränsad utsträckning, till övervägande del, helt uppfyllt).

NIST CSF innehåller höga krav och att uppnå högsta nivån enligt detta ramverk kräver en organisation som har en hög mognadsgrad i sitt informations- och cybersäkerhetsarbete. Vi har således anpassat de krav som finns i NIST-ramverket efter regionens särskilda behov och förutsättningar och givit en bedömning baserat på detta.

NIST CSF beskriver informations- och cybersäkerhetsförmåga i termer av fem funktioner, med ett antal kategorier om total drygt 200 kontroller. Vi har utifrån hotprofil, vår erfarenhet från tidigare granskningar samt dokumentgranskning valt ut de kontroller och frågor som vi anser vara mest relevanta och kritiska för regionen.

NIST CSF-funktionerna är:

- **Identifiera**, vilket innebär att man analyserar organisationens förmåga att identifiera det skyddsvärda, förmågan till riskanalys, tredjepartsrisk och riskhantering samt förmågan till styrning av informationssäkerheten.

- **Skydda**, vilket innebär att man värderar organisationen förmåga till behörighetskontroller, utbildning av personal, skyddsmekanismer som brandväggar med mera.

- **Upptäcka,** vilket innebär en bedömning av organisationens förmåga att upptäcka eventuella avvikelser från normalbilden, övervakningsprocesser, logghantering med mera.

- **Hantera**, vilket handlar om organisationen förmåga till incidenthantering, kommunikationsplaner, avhjälpande åtgärder samt utveckling

- **Återhämta**, vilket handlar om organisationens förmåga att så snart som möjligt efter en incident återgå till normaldrift samt förmågan till att göra analyser av det inträffade och förbättra/förändra rutiner samt upprätta en kontinuitetsplan.

[3] För mer information om NIST CSF se https://www.nist.gov/cyberframework

Granskningen har genomförts av Carl Thorn, Gabrielle Stööp och Viktor Persson, samtliga från PwC. Granskningsrapporten har faktagranskats av berörda tjänstemän.

2. Iakttagelser och bedömningar

2.1. Kontrollmål 1 – Har regionen förmåga att styra och följa upp risk- och säkerhetsarbetet på ett sätt som förutsättningar, interna och externa regler kräver?

2.1.1. Inledning

Detta kontrollmål berör den förmåga i NIST CSF som kallas ”identifiera”. Detta innebär att organisationen ska ha en organisatorisk förståelse för sina behov och försättningar att hantera informations- och cyberssäkerhetsrisker. Förmågan innefattar således riskhantering samt ledning och styrning av informations- och cybersäkerhetsarbetet.

Utöver det övergripande kontrollmålet har även ett antal ytterligare kontrollmål tagits i beaktning i förhållande till denna förmåga. Dessa kontrollmål är:

- Finns en bild av vilka huvudsakliga hotaktörer och hothändelser som utsätter regionen för risk?
- Har styrelsen fastställt vilka risknivåer som är acceptabla?
- Finns ett effektivt informations- och cybersäkerhetsarbete i linje med accepterade risknivåer?
- Finns det hos ledande befattningshavare en god kunskap och förståelse för informations- och cybersäkerhetsarbetet?
- Finns det upprättade policyer och riktlinjer avseende regionens arbete med informations- och cybersäkerhet?
- Är regionens investeringar i informations- och cybersäkerhetsarbete i linje med de brister och den hotbild som föreligger?

Iakttagelser och bedömning i förhållande till dessa kontrollmål sammanvägs tillsammans med det övergripande kontrollmålet.

2.1.2. Iakttagelser

It genomför kontinuerlig inventering av den hårdvara och mjukvara som de ansvarar för. Det finns en konfigurationsdatabas som ger en översiktlig bild av de it-tillgångar som finns. Inventeringen sker dock separat i respektive område, exempelvis finns en separat inventering av serversystem och en separat för klientsystem. Det finns ett antal olika applikationer där inventering dokumenteras. Ansvaret för att föra inventering ligger i respektive område, i respektive objektsfamilj. Det finns en huvudsaklig ansvarig för varje objektsfamilj.

Funktionen för informationssäkerhet genomför för tillfället en processkartläggning där samtlig information som regionen behandlar samt var informationen lagras ska kartläggas. Detta är någonting som kräver mycket tid och resurser och arbetet beräknas vara klart om ca 2,5 år. Det inledande arbetet har inneburit att kartlägga sådana processer som är omfattande och kritiska, exempelvis sådana processer som kan beröras av NIS-direktivet. Denna process-/informationskartläggning används som grund vid informat-

ionsklassning och riskanalys. Kartläggning och klassning sparas på en gemensam Sharepoint-sida.

Det finns ingen informationssäkerhetspolicy. Detta förklaras enligt att regionen antar ett begränsat antal policydokument. Arbetet med informationssäkerhet styrs istället av ett antal direktiv: Direktiv Informationssäkerhet, Direktiv styrande dokument i LIS och Direktiv för ansvar och roller. Därtill finns ett antal rutiner som ytterligare beskriver arbetet med informationssäkerhet. Vidare har informationssäkerhetansvarig tagit fram utkast till ytterligare ett direktiv samt en rutin (Direktiv och rutin för systematiskt och riskbaserat informationssäkerhetsarbete). Dessa dokument har ännu inte antagits men innehåller ytterligare beskrivning av hur regionen ska arbeta med informationssäkerhet däribland hur regionen ska bedöma och hantera informationssäkerhetsrisker. Det finns således i nuläget inte något styrande dokument för hur regionen ska arbeta med informationssäkerhetsrisker. Det finns inte dokumenterat hur risker ska bedömas, vilken risktolerans som finns eller hur risker ska prioriteras och hanteras. Regionen arbetar dock med att identifiera och bedöma informationssäkerhetsrisker i praktiken, men i dagsläget sker detta utan en dokumenterad process och med de styrande dokument som intern styrning och kontroll tillhandahåller.

Funktionen för informationssäkerhet har det övergripande ansvaret för att styra arbetet med informationssäkerhet i regionen. Denna funktion har det strategiska ansvaret och sköter framtagandet av styrande dokument samt den övergripande övervakningen av området. Det har nyligen skett en organisationsförändring i regionen vilket har resulterat i att funktionen nu är placerade under enheten för informationsförvaltning som i sin tur är placerade under kansliavdelningen som är organiserad i stabsförvaltningen. Funktionen för informationssäkerhet har ingen egen budget.

Ansvaret för implementering och genomförande ligger hos respektive verksamhet. I varje förvaltning finns en informationsförvaltningssamordnare. Detta är funktionen för informationssäkerhets kontaktpunkter ute i verksamheten. Vidare finns ett informationssäkerhetsråd som informationssäkerhetsansvarig kallar samman åtta gånger om året och som består av bland annat representanter från samtliga förvaltningar, it-chef, it-säkerhetsansvarig, chefsjurist och säkerhetschef.

Kanslidirektören är ansvarig för investeringar i regionens informationssäkerhetsarbete. Funktionen för informationssäkerhet kan dock vara med och påverka vad dessa investeringar ska vara. Det finns ett arbete med att ta fram kvalitetskrav för informationssäkerhet. Från kraven kan man sedan avgöra vad som är mest prioriterat och vilka verktyg som krävs för nå detta. Kopplat till detta vill även funktionen för informationssäkerhet ta fram en detaljerad plan för måluppföljning inom informationssäkerhet. Det finns i nuläget ett antal mål listade i det övergripande direktivet för informationssäkerhet men det finns ingen plan för hur dessa mål ska uppnås eller mätas.

Funktionen för informationssäkerhet deltar i ett antal externa nätverk i syfte att hålla sig uppdaterad på vad som händer inom området samt ta del av information i hur andra organisationer hanterar de utmaningar som regionen står inför. Funktionen ansvarar för att övervaka ny lagstiftning som berör området informationssäkerhet. För tillfället är NIS-direktivet i fokus och det pågår ett arbete för att säkerställa att organisationen efterlever lagstiftningen. Regionen använder sig inte av något compliance-verktyg. Det finns en Sha-

repoint-sida (se beskrivning tidigare i detta avsnitt) där all information som regionen har ska dokumenteras och därefter kopplas till de olika lagkrav som styr denna information (exempelvis NIS och Dataskyddsförordningen).

Det finns inget systematiskt arbete inom regionen för att identifiera och analysera cyberhot. Ansvaret ligger enligt uppgift på Säkerhetschefen och denne genomför omvärldsbevakning som i sin tur i viss mån innehåller allmänna hotbildsanalyser från svenska myndigheter såsom Säkerhetspolisen och Myndigheten för samhällsskydd och beredskap. Det finns en dokumenterad risk- och sårbarhetsanalys från 2015, i övrigt har regionen inga egna dokumenterade hotanalyser.

Regionen anser sig vara beroende av leverantörer och tredje part i stor utsträckning. Informationssäkerhetsansvarig är delaktig i arbetet med att sälla krav på leverantörer i upphandling. Det finns dock en dokumenterad process för beslut om nya it-funktioner. I denna ingår att informationssäkerhet ska tas i beaktning. Vid övriga inköp inkluderas informationssäkerhet sporadiskt, då det anses att ett behov finns. SKL:s metod Klassa används som inspiration för att upprätta informationssäkerhetskrav. Det finns enligt uppgift en plan att upprätta en mall som ska användas vid upprättandet av informationssäkerhetskrav och i kontakt med leverantörer men denna finns ännu inte på plats. Vidare finns en rutin för att genomföra granskning av personuppgiftsbiträden. Det finns en plan att ta fram en liknande rutin för att kunna granska samtliga leverantörer och de informationssäkerhetskrav som ställs på dem, men detta har ännu inte fastställts.

2.1.3. Bedömning

Kontrollmål 1 – Har regionen förmåga att styra och följa upp risk- och säkerhetsarbetet på ett sätt som förutsättningar, interna och externa regler kräver?

Vår bedömning är att kontrollmålet i begränsad utsträckning är uppfyllt.

Den processkartläggning som funktionen för informationssäkerhet för närvarande genomför kommer leda till att regionen har en bättre kontroll och översikt över sina informationstillgångar och hur dessa hanteras. I nuläget anser vi inte att denna kontroll och översikt finns.

I samband med i ovan nämnda processkartläggning sker riskidentifiering och riskbedömning. Det finns således ett pågående arbete med informationssäkerhetsrisker. Det finns dock ingen dokumenterad process för hur detta ska gå till. Vår bedömning är därför att arbetet inte sker på ett systematiskt sätt. Styrande dokument som Direktiv och Rutin för systematisk och riskbaserat informationssäkerhetsarbete bör antas för att säkerställa att det finns en enhetlig hantering av informationssäkerhetsrisker i regionen.

Regionen har idag inte en dokumenterad process för arbetet med att identifiera och bedöma hot. Vår bedömning är att regionen bör ha en gemensam process för att värdera omvärlden på strategisk nivå inom vilken regelverk, hotbild, nationella strategier och målsättningar formar säkerhetsarbetet. Vi har som en del av denna granskning tagit fram en hotbildsanalys åt regionen. Denna bör regionen förvalta och arbeta med för att säkerställa att regionens säkerhetsarbete är i linje med den hotbild som finns.

Den organisatoriska placeringen av funktionen för informationssäkerhet samt det faktum att funktionen inte har en egen budget innebär en risk. Avståndet till högsta ledning kan medföra svårigheter att på ett effektivt sätt ha möjligheten att styra arbetet med informationssäkerhet i regionen. Detta förstärks ytterligare genom att funktionen för informationssäkerhet inte råder över en egen budget. Informationssäkerhet är beroende av andra delar av organisationen och det finns en risk att det blir bortprioriterat samt att ett kontinuerligt arbete inte kan upprätthållas.

Det framhålls under intervjun att det finns ett behov av mer engagemang och kunskap kring säkerhetsfrågor hos högsta ledningen i regionen. Ledningens engagemang är kritiskt och krävs för att informationssäkerhet ska vara en prioriterad fråga i regionen. Detta avspeglar sig även i frågor om budget, mandat och resurser.

Det finns ingen informationssäkerhetspolicy. Regionen har endast direktiv och rutiner för informationssäkerhet. En policy är det högst styrande dokumentet i regionen och en informationssäkerhetspolicy skulle därmed ha ett högt symboliskt värde och skulle påvisa vikten av informationssäkerhet på samtliga nivåer i regionen. Vår bedömning är således att en policy skulle förbättra styrningen av informationssäkerhet i regionen.

Funktionen för informationssäkerhet har ingen måluppföljning eller detaljerad plan för hur arbetet med informationssäkerhet ska följas upp. Detta ska enligt uppgift införas men i nuläget brister arbetet med uppföljning av informationssäkerhetsarbetet i regionen.

Informationssäkerhet är ofta med i kravställning i inköpsprocessen och det finns en dokumenterad process för detta gällande beslut om nya it-funktioner. Vår bedömning är dock att det fortfarande finns arbete att göra kring inköpsprocessen och att det bör säkerställas att informationssäkerhet tas i beaktning i samtliga inköp där det är relevant. Det bör även finnas en rutin för granskning och uppföljning informationssäkerhetskrav, någonting som inte genomförs i dagsläget.

2.1.4. Rekommendationer

- Anta och implementera en informationssäkerhetspolicy som revideras på årsbasis
- Säkerställ att den processkartläggning som genomförs, prioriteras och slutförs enligt plan
- Anta och implementera styrande dokument för hantering av informationssäkerhetsrisker och fastställ vilka risknivåer som är acceptabla
- Se över den organisatoriska placeringen av funktionen för informationssäkerhet i organisationen och säkerställ att informationssäkerhetsansvarig har rätt mandat för att bedriva ett effektivt informationssäkerhetsarbete över hela regionen
- Säkerställ att högsta ledning har engagemang i och kunskap om informationssäkerhetsarbetet
- Överväg att införa en egen budget för funktionen för informationssäkerhet
- Inför måluppföljning och mätning av informationssäkerhetsarbetet
- Inför ett systematiskt arbete med att identifiera och analysera hot, använd med fördel den hotbildsanalys som PwC har tagit fram och förvalta denna framåt
- Säkerställ att informationssäkerhet inkluderas i inköpsprocessen genom en dokumenterad process som är riskbaserad och inkluderar behovsanalys, kravställning, upphandling, kontraktering, uppföljning och avslut

2.2. Kontrollmål 2 – Har regionen förmåga att utveckla och genomföra lämpliga skyddsåtgärder för att säkerställa leverans av kritiska tjänster samt skydda system och information?

2.2.1. Inledning

Detta kontrollmål berör den förmåga i NIST CSF som kallas ”skydda”. Detta innebär att organisationen ska inneha lämpliga skyddsåtgärder för att minska eller begränsa en potentiell cyberattack.

Utöver det övergripande kontrollmålet har även ett ytterligare kontrollmål tagits i beaktning i förhållande till denna förmåga. Detta kontrollmål är:

- Har regionen förmåga att hantera cybersäkerhetsrisker kopplat till system, personer, information och leverantörer?

Iakttagelser och bedömning i förhållande till detta kontrollmål sammanvägs tillsammans med det övergripande kontrollmålet.

2.2.2. Iakttagelser

Det finns en dokumenterad, etablerad rutin för tilldelning av behörigheter till system i Region Gävleborgs it-miljö. Enligt uppgift har verksamheten tagit fram en behovsanalys som grundar sig i principen “lägsta behövda behörighet”. Chefer skickar in förfrågningar till särskild personal för medarbetare som de ansvarar för, varpå förfrågningarna bedöms utefter en mall som resulterat från analysen. Via ett ärendesystem finns det spårbarhet i vem som lagt till behörigheter och när. Vid ändring av behörigheter åligger det respektive chef att rapportera behovet av ändring. Det görs ingen kontinuerlig, automatiserad uppföljning som ser till att behörigheter tas bort när de inte längre behövs.

Systemet som styr it-behörigheter är integrerat med organisationens HR-system. När en anställd slutar stängs motsvarande konto ned via en automatiserad process.

Ansvarig personal försöker välja lämpliga autentiseringsmetoder för sina it-system. Vilken autentiseringsmetod som ska användas baseras på en klassning av informationen i respektive system. Intervjuad personal berättar att processen för hur klassningen ska gå till inte är genomarbetad, sådant att det finns risk att flera system i nuläget saknar tillfredsställande autentisering.

Region Gävleborg tillämpar flera lösningar för att möjliggöra fjärråtkomst till interna nätverk. För att få behörighet behöver man göra en förfrågan via sin chef enligt rutinen som beskrivits ovan. Fjärråtkomstlösningarna är konfigurerade sådant att man bara kan fjärransluta till det interna nätverket med en dator som har tillhandahållits av Region Gävleborg. Vad man har tillgång till på det interna nätverket är behörighetsstyrt. Samtliga tillämpade lösningar använder flerfaktorsautentisering.

Region Gävleborgs organisation är sådan att det finns behov att segmentera dess datornätverk. Det finns en grupp som i stort ansvarar för att hantera sådant arbete, men hur

den ska gå tillväga finns inte kravställt eller beskrivet i rutiner. Intervjuad personal menar att det uppkommer diskussioner från fall till fall, och att bedömningar görs utefter en överenskommen "best practice". Det har inte gjorts något aktivt arbete att se över behovet av nätverkssegmentering i hela organisationen, utan bara delar som anses mer kritiska. Vilka system som finns i respektive nätverkssegment är dokumenterat.

Klientdatorer i Region Gävleborgs it-miljö får sina hårddiskar krypterade med Bitlocker. Även mobiltelefoner är krypterade, men inte serverdatorer. Intervjuad personal kunde inte erinra sig om att kryptering tillämpas på en applikationsnivå eller vid lagring i databaser. Gällande graden av kryptering som tillämpas för data vid överföring i datornätverket berättar intervjuad personal att det inte är något som arbetas med specifikt, och att det inte finns kravställande dokument.

Det är ett pågående arbete att öka medvetenheten om dataläckor och att se över klassningen av information i regionens system. Hur it-ansvariga och informationssäkerhetsansvariga ska samverka är inte utarbetat.

På både klient- och serversystem görs kontinuerliga backuper. På dessa görs dagligen s.k. snapshots av filsystemen. Intervjuad personal menar att detta är helt automatiserat. För databasbackuper beror frekvensen på krav från respektive systemägare. Backupdatan skrivs till två separata diskar – inte magnetband. Tidslängden som en backup sparas är 90 dagar. Att backuphårddiskarna inte blivit defekta kontrolleras kontinuerligt. Att datan som skrivs till backuphårdiskarna faktiskt är den som avses kontrolleras enligt uppgift inte, och alltså görs inte heller återläsningstester.

Region Gävleborg har rutiner på plats för att hantera förflyttning och destruktion av system. Varje månad görs en översyn över vilka system som brukas av en viss gruppering. För att ett system ska flyttas mellan grupperingar krävs ett beslut från en i respektive gruppering ansvarig person. Vid destruktioner omfattas enligt uppgift samtliga system av en process där data i systemen skrivs över, och respektive system sedan destrueras fysiskt.

Region Gävleborg arbetar med fysisk säkerhet på flera sätt. Väktare används utefter behov. Intervjuad personal menar att bestämning av åtkomst till fysiska utrymmen i stort är en it-fråga. Åtkomst tilldelas till personalens e-tjänstekort. Tilldelning av behörigheter sker enligt samma rutin som för it-system.

Programvara som används inom Region Gävleborgs it-miljö är främst inköpt, men det utförs också viss egenutveckling. Att produktionsmiljön och utvecklingsmiljön ska vara separata är välförstått, men efterlevnaden upplevs inte vara helt riktig. Intervjuad personal menar att miljöerna inte är så pass separerade att man inte kan nå produktionssystem från utvecklingssystem. Vid egenutveckling är vidare utvecklarna typiskt desamma som ansvarar för drift, sådant att de kan ha tillgång i stort sett alla system. De som utvecklar besitter inte nödvändigtvis kunskap om hur man skriver säker kod. Testning av utvecklade program görs ur ett funktionellt perspektiv, inte ur ett säkerhetsperspektiv. Att testdatan som används under utveckling bör vara maskerad är också välförstått, men även här antyder intervjuad personal att efterlevnaden inte är helt konsekvent. Vid nyttjande av externa utvecklare upprättas enligt rutin sekretessavtal.

Både klientsystem och serversystem är konfigurerade utifrån en baskonfiguration i vilken säkerhet har tagits i beaktning. Baskonfigurationen återfinns på s.k. images som skrivs till systemen när de installeras upp. Vilka program som får finnas och köras på systemen styrs av programvaran Applocker. Både klient- och serversystem har antivirusprogramvara. Vissa program kräver att användare måste kunna agera lokal administratör, och intervjuad personal ser detta som ett problem. Som lokal administratör har man bl.a. möjlighet att ändra konfigurationer på systemen som man vanligtvis inte kan. Personal som behöver kunna agera lokal administrator ska enligt rutin använda separata konton för detta ändamål som enbart används vid behov. Det finns inget system på plats som upptäcker om ett systems konfiguration avviker från den bestämda.

Region Gävleborg har ett utarbetat system för patchning av klient- och serversystem. Att hantera patchning är en av huvudsysslorna för de driftansvariga. Patchning sker rutinmässigt varje månad. Innan patchning sker på samtliga system görs de på ett urval, för att erfara om patcharna orsakar problem. Via en programvara som samlar in diagnostik från system i it-miljön kan driftansvariga se systems patchnivå och erfara huruvida patchning misslyckats. Intervjuad personal berättar att det finns ett litet antal gamla system i it-miljön som inte längre stöds av leverantören (Microsoft), och som därför utgör en viss säkerhetsrisk. Intervjuad personal menar att de kompenserar för detta genom att begränsa deras exponering. Det finns inga rutiner för att snabbt adressera plötsligt offentliggjorda sårbarheter i programvara.

Det finns initiativ att utbilda personal i säkerhet. Gällande informationssäkerhet finns en obligatorisk introduktionsutbildning som samtliga på regionen ska gå. Detta är en e-learning och är ett minimikrav som alla måste uppnå. Det finns även listat på det gemensamma intranätet vilka styrande dokument som varje roll måste läsa. Informationssäkerhetsansvarig följer upp och säkerställer att samtliga informationsförvaltningssamordnare har läst den dokumentation som de ska läsa. Det är i sin tur respektive samordnares ansvar att föra vidare detta i sin förvaltning och säkerställa att detta efterlevs. Funktionen för informationssäkerhet ansvarar för att verksamheten ska ha kunskap om informationssäkerhet och det ansvar som verksamheten själva har kopplat till informationssäkerhet. Informationssäkerhetsansvarig håller i ett stort antal utbildningar kontinuerligt. Dessa utbildningar anpassas utefter verksamheten och de roller som utbildas. Utbildningar sker dels då ett behov identifieras eller då verksamheten själv kontaktar informationssäkerhetsansvarig med förfrågan om utbildning. Det finns ingen övergripande utbildningsplan.

Medarbetare utbildas inte specifikt i cybersäkerhet. De it-säkerhetsansvariga har inte som uttalad uppgift att utbilda medarbetare. Det utbildningsmaterial som medarbetare enligt rutin tar del av är systemintroducerande, utan särskilt fokus på säkerhet.

2.2.3. Bedömning

Kontrollmål 2 – Har regionen förmåga att utveckla och genomföra lämpliga skyddsåtgärder för att säkerställa leverans av kritiska tjänster samt skydda system och information?

Vår bedömning är att kontrollmålet i begränsad utsträckning är uppfyllt.

Region Gävleborg har flera mekanismer på plats för att för att säkerställa leverans av kritiska tjänster samt skydda system och information. Tekniska lösningar vars syfte är att

garantera detta används utbrett i it-miljön. Vidare verkar säkerhetsansvarig personal vara väl införstådd i relevanta, gängse skyddsprinciper såsom "lägsta behövda behörighet".

Fastän skydden i stort tycks fungerar bra finns tillkortakommanden i arbetet. Det mest märkbara är att det i många fall saknas dokumenterade, etablerade rutiner. Ofta förlitar sig personal på gruppöverenskomna "best practices". Ett annat övergripande tillkortakommande som framgick av intervjuerna är att det saknas systematiskt arbete för att höja chefers och andra medarbetares förståelse för säkerhetsfrågor.

Gällande tekniska skyddsmekanismer finns många lösningar på plats som bidrar till ett omfattande skydd. För flera lösningar saknas vissa tillämpningar som skulle som skulle göra lösningarna än mer effektiva. Vissa system är särskilt konfigurerade, medan andra utgår ifrån standardiserade baskonfigurationer. I flera fall kan det finnas fog för att se över konfigurationerna och anpassa dem mer utefter behov.

Det finns dock ingen övergripande plan för utbildning av anställda utan utbildningar görs sporadiskt vid behov. Vår bedömning är att en plan bör finnas för att säkerställa att samtliga personer får rätt utbildning för sin roll.

2.2.4. Rekommendationer

- Etablera rutiner för
  - vilka autentiseringskrav som ska finnas på system
  - hur och i vilka fall nätverk ska segmenteras
  - hur skyddssystem ska vara konfigurerade
  - hur regionen ska arbeta för att försöka förhindra dataläckage
  - hur utvecklingsmiljön ska separeras vid egenutveckling
  - hur testdata får användas vid egenutveckling, bl.a. gällande anonymisering
  - hur säkerhetstestning ska genomföras vid egenutveckling
  - hur man ska hantera plötsligt offentliggjorda sårbarheter i programvara (s.k. zero-days)
- Utvärdera effektiviteten av skyddsmekanismerna genom kontrollerade, kontinuerliga tester, fördelaktigen penetrationstester
- Se över tidsramen för nedstängningen av konton för timanställd och extern personal
- Använd kryptering i databaser
- Använd magnetband för långtidsbackuper
- Överväg att anpassa nuvarande standardkonfigurationer
- Fastställ en utbildningsplan för informationssäkerhet som berör hela regionen och är målgruppsanpassad där ledningspersoner, personer med särskilda behörigheter eller har tillgång till särskilt känsliga system/information får ytterligare utbildning

2.3. Kontrollmål 3 – Har regionen förmåga att utveckla och genomföra lämpliga aktiviteter för att identifiera förekomsten av informations- och cybersäkerhetshändelser?

2.3.1. Inledning

Detta kontrollmål berör den förmåga i NIST CSF som kallas ”upptäcka”. Detta innebär att organisationen ska ha förmågan att upptäcka potentiella eller redan inträffade informations- och cybersäkerhetsincidenter.

2.3.2. Iakttagelser

Region Gävleborg har enligt uppgift inte system eller rutiner på plats för att effektivt upptäcka pågående cyberangrepp. Klient- och serversystem kör antivirusprogramvara som flaggar intressanta händelser. Personalen som har rollen att ta emot notifikationer arbetar inte uteslutande med säkerhet, utan snarare drift.

Flera av lösningarna som skyddar datornätverk är konfigurerade att upptäcka och larma om misstänkta säkerhetsrelaterade avvikelser. Samma grupp som ansvarar för att konfigurera dessa system, dvs. nätverkstekniker, tar emot dessa notifikationer per e-mail eller SMS.

Loggar genereras på flera system i Region Gävleborgs it-miljö. Intervjuad it-personal berättar att det är kravställt att vissa system, exempelvis journalsystem, ska generera loggar med antydan att dokumenterade krav inte finns för alla. Region Gävleborg använder inte någon lösning som centralt samlar loggarna som de många system i it-miljön producerar.

Regelbundna skanningar efter skadlig kod görs på klient- och serversystemen. Antivirusprogramvara skyddar också dessa system i realtid.

Analyser av upptäckta, fullbordade angrepp sker inte systematiskt enligt en dokumenterad rutin.

2.3.3. Bedömning

Kontrollmål 3 – Har regionen förmåga att utveckla och genomföra lämpliga aktiviteter för att identifiera förekomsten av informations- och cybersäkerhetshändelser?

Vår bedömning är att kontrollmålet i begränsad utsträckning är uppfyllt.

Region Gävleborg har flera lösningar på plats för att förhindra angrepp och flagga suspekta avvikelser på klient- och serversystem och i nätverkstrafik. Dessutom genomförs omfattande loggning. Ett genomgående tema är att det saknas dokumenterade, etablerade rutiner. Vidare är personalen som i nuläget tar emot och hanterar avvikelser inte tränad i cybersäkerhet, och därav hämmas regionens förmåga att agera tillfredsställande på avvikelser.

2.3.4. Rekommendationer

- Etablera rutiner för
- vilka avvikelser som ska flaggas

- hur avvikelser ska komma till lämplig personals kännedom
- Stärk cybersäkerhetskompetensen hos personal som ansvarar för att
- implementera detektionslösningar
- ta del av notifikationer angående avvikelser
- Skapa förmåga att effektivt analysera avvikelser, dels genom att stärka personalkompetensen och dels genom tillämpning av sofistikerad, automatiserad analysprogramvara. Överväg som en del i detta att införa en särskild enhet med detta ansvar. I internationella sammanhang kallas sådana enheter ”Security operations center” (SOC).

2.4. Kontrollmål 4 – Har regionen förmåga att utveckla och genomföra aktiviteter för att vidta lämpliga åtgärder avseende en upptäck informations- eller cybersäkerhetsincident?

2.4.1. Inledning

Detta kontrollmål berör den förmåga i NIST CSF som kallas ”hantera”. Detta innebär att organisationen ska förmågan att agera snabbt och bemöta informations- och cybersäkerhetsincidenter.

2.4.2. Iakttagelser

I dagsläget rapporteras och hanteras it-incidenter och informationssäkerhetsincidenter separat, i två olika strömmar. Informationssäkerhetsincidenter anmäls genom att medarbetare mailar till olika funktionsbrevlådor (beroende på typ av informationssäkerhetsincident) och it-incidenter anmäls genom att kontakta it-support.

Funktionen för informationssäkerhet upplever att de inte får information om samtliga informationssäkerhetsrelaterade incidenter. Det finns, enligt uppgift, inte en översikt över regionens informationssäkerhetsincidenter då de i dagsläget inte registreras i ett samlat system.

Funktionen för informationssäkerhet håller för tillfället på att ta fram ett material för att öka kunskapen kring vad en informationssäkerhetsincident är. Det finns enligt uppgift en brist på kunskap kring vad en informationssäkerhet är och det behövs därför utbildning kring vad olika typer av incidenter är (exempelvis vad en NIS-incident är och vad en personuppgiftsincident är).

It:s incidenthanteringsprocess bygger på ramverket ITIL och finns beskrivet i “Rutin för incidenthantering it-avdelningen”. Samtliga it-incidenter registreras i det gemensamma ärendehanteringssystemet. Sammanfattningsvis kan det sägas att en användare som misstänker eller upptäcker en incident ska kontakta it-support. It-support har beredskap dygnet runt. It-support bedömer sedan incidenten utifrån en dokumenterad bedömningsmatris och hanterar sedan incidenter utefter hur allvarlig den bedöms att vara. Det finns dokumenterade checklistor för samtliga steg och hur eskalering ska ske beroende på hur kritisk incidenten är. Om en incident upprepas klassas det som ett problem och det finns en särskild process för hur problem ska hanteras. Det finns även en kommunikationsplan för it som beskriver vilka som ska kontaktas vid olika typer av incidenter.

I incidenthanteringsprocessen för it-incidenter ingår uppföljning och lärande. Det skrivs alltid en incidentrapport och objektförvaltaren har som ansvar att följa upp incidenten. Det finns en dokumenterad mall för hur incidentrapporter ska skrivas. Objektförvaltaren ska även se över vilka incidenter som har skett i de system som denne förvaltar. Pågående incidenter följs upp veckovis under ett möte där respektive objektsförvaltare deltar och redovisar status för sitt objekt.

It:s incidenthanteringsprocess håller för tillfället på att revideras och det genomförs justeringar i processbeskrivningarna. Det förs även enligt uppgift en dialog mellan it och informationssäkerhet för att förbättra kommunikationen och samordningen gällande incidenthantering. Funktionen för informationssäkerhet har tagit fram ett utkast till ett nytt direktiv för incidenthantering där det ingår ett förslag till gemensam rapportering av samtliga säkerhetsincidenter i regionen.

2.4.3. Bedömning

Kontrollmål 4 – Har regionen förmåga att utveckla och genomföra aktiviteter för att vidta lämpliga åtgärder avseende en upptäck informations- eller cybersäkerhetsincident?

Vår bedömning är att kontrollmålet i begränsad utsträckning är uppfyllt.

På grund av att it- och informationssäkerhetsincidenter hanteras på två olika sätt förekommer risken att det inte finns en översikt över regionens incidenter samt att incidenter inte rapporteras till rätt ställe.

Funktionen för informationssäkerhet har tagit fram ett nytt direktiv för incidenthantering men detta har ännu inte antagits. Dokumentation kring vad olika typer av informationssäkerhetsincidenter är saknas, men detta är någonting som är prioriterat att ta fram. Vår bedömning är att dessa aktiviteter skulle förbättra regionens incidenthantering men i nuläget finns detta inte på plats.

Vår bedömning är att det inte finns tillräcklig samordning mellan it och informationssäkerhet vad det gäller incidenthantering. Funktionerna rapporterar och hanterar incidenter på olika sätt och kommunikationen däremellan är bristfällig. Det har enligt uppgift påbörjats ett arbete för att förbättra detta men i nuläget finns det brister.

2.4.4. Rekommendationer

- Öka samordning mellan it och informationssäkerhet vad gäller incidenthantering.
- Anta det nya direktivet för incidenthantering och säkerställ att det finns en gemensam rapportering för incidenter i regionen.
- Öka kunskapen kring informationssäkerhetsincidenter i organisationen bland annat genom att tydlig definiera och förmedla vad olika typer av informationssäkerhetsincidenter är. Detta bör inkluderas i den utbildningsplan som rekommenderas under kontrollmål 2.

2.5. Kontrollmål 5 – Finns ändamålsenliga planer för att återställa it-driften vid incidenter och kriser t.ex. it-haveri?

2.5.1. Inledning

Detta kontrollmål berör den förmåga i NIST CSF som kallas ”återhämta”. Detta innebär att organisationen ska ha förmågan att återgå till normal verksamhet efter en informations- och cybersäkerhetsincident.

2.5.2. Iakttagelser

Funktionen för informationssäkerhet ska tillhandahålla en övergripande kontinuitetsplan som är en slags kravställan mot övrig verksamhet. Det är verksamheten som i sin tur ska arbeta med detta och skapa mer detaljerade planer för sina områden.

It arbetar med kontinuitet inom samtliga sina områden. I rutin för incidenthantering it-avdelningen listas tre olika roller som medverkande i arbetet med återställning efter en incident. Dessa roller är: It-support, Lösningsteam och Systemspecialist.

Det finns planer för återställning av exempelvis Region Gävleborgs katalogtjänst – Active Directory – och klientsystem. Det ska enligt uppgift finnas dokumenterade processer för hur man ska agera för att återställa objekt vid en händelse. Det genomförs även övningar för att fler personer än den huvudansvarige ska ha kunskap i hur återställning går till i respektive objekt.

Det finns en 20-i-topp-lista som anger vad det är som ska prioriteras vid en omfattande incident. Denna lista anger bland annat att infrastrukturen är högst prioriterad.

Datahallarna är redundanta. Sker en incident som påverkar en datahall kan verksamheten fortgå, med begränsad styrka. Datahallarna är uppbyggda på så sätt att en datahall ska kunna försvinna helt.

Det genomförs regelbundna tester av kontinuitet och det finns en process för att tillvarata lärdomar från dels dessa tester samt från faktiska händelser. Arbetet med återställning och kontinuitet förbättras ständigt. Den kommunikationsplan som it använder vid incidenter används även vid större händelser och katastrofer.

2.5.3. Bedömning

Kontrollmål 5 – Finns ändamålsenliga planer för att återställa it-driften vid incidenter och kriser t.ex. it-haveri?

Vår bedömning är att kontrollmålet i begränsad utsträckning är uppfyllt.

Funktionen för informationssäkerhet planerar att tillhandahålla en övergripande kontinuitetsplan som verksamheten sedan ska bryta ned till anpassade planer för respektive verksamhet. I nuläget finns detta inte på plats och vår bedömning är därför att det finns en brist i kontinuitetsplanering inom informationssäkerhetsområdet.

Vår bedömning är att det till viss del finns planering, övning och arbete med kontinuitet och återställning inom it men att det fortfarande finns arbete kvar att göra. Det finns inte dokumenterade planer och processer för samtliga tillgångar.

2.5.4. Rekommendationer

- Funktionen för informationssäkerhet bör säkerställa att en övergripande kontinuitetsplan tas fram
- It bör säkerställa att det finns dokumenterade kontinuitetsplaner
- It bör säkerställa att det finns dokumenterade processer för hur återställning ska gå till i samtliga tillgångar

År-månad-dag		
Uppdragsledare		*Projektledare*