Höör och Hörby kommun

Övergripande säkerhetsgranskning av kommunens IT-säkerhet avseende externt och internt dataintrång

Henrik Friang,
IT-säkerhetsspecialist, PwC

Viktor Bergvall,
IT-säkerhetsspecialist, PwC

April 2016

pwc

Abstrakt

Efter genomförd granskning baserat på kontrollfrågorna görs bedömningen att kontrollen över intern IT- och informationssäkerhet, har utrymme för förbättringsåtgärder. Den övergripande granskningen av tekniska kontroller som övervakas av IT bedöms tillfredställande utan några tydligt påvisade brister. Fysisk säkerhet i serverhall, säkerhet i mjukvara samt i den övergripande IT-infrastrukturen bedöms som god. Tekniska kontroller kan dock bli än mer effektiva och behov av nya kontroller kan tillkomma, när en riskanalys för verksamheten utförs med utgångspunkt i externa och interna hot.

Nedan följer en sammanställning över granskningens största iakttagelser

1) Det saknas en formell process för att löpande analysera risker och hot mot kommunens verksamhet. Nuvarande riskanalyser har utgångspunkt i enskilda applikationer, men med rådande tekniska utveckling i samhället har helt nya typer av hot tillkommit, som har utgångspunkt i externa faktorer. Iakttagelsen medför att kontroller och arbetsinsatser inom området för IT- och informationssäkerhet inte har utgångspunkt i faktiska hot. Det finns en risk att fokus för riskhantering och investeringar görs i icke prioriterade områden.

2) Nuvarande organisation i form av roller, ansvarsområden, rapporteringsvägar samt nyckeltal (KPI:er) för styrning av området för IT- och informationssäkerhet, är inte tydligt definierade i styrande dokument. Iakttagelsen medför att hot och risker inom IT- och informationssäkerhet är svåra att övervaka och hantera. Arbetssättet inom område för IT- och informationssäkerhet riskerar att blir mer reaktivt än proaktivt, vilket försvårar för verksamheten att förbättra riskhanteringsprocessen på sikt.

Innehållsförteckning

1 Inledning

1.1 Bakgrund

Hanteringen av risker inom IT-området får allt större betydelse då verksamheten blir allt mer beroende av stöd från IT-system. En effektiv och framgångsrik riskhantering bygger på ett helhetstänkande. Kvaliteten, säkerheten och effektiviteten i organisationens interna processer ökar och organisationen skyddas mot till exempel obehöriga dataintrång samtidigt som beredskapsmedvetandet stärks inom organisationen.

1.2 Revisionsfråga och kontrollfrågor

Är kommunens hantering av IT-säkerhet ändamålsenligt och effektivt i förhållande till de prioriterade IT-hoten mot kommunens IT-miljö?

1.2.1 Granskningen inriktas mot följande kontrollfrågor:

- Finns prioriterade hot mot kommunens IT säkerhet dokumenterade och uppdateras dokumentationen löpande?
- Hur ser organisationen och ansvarsfördelning ut i frågor rörande IT säkerhet?
- Finns det en tydlig plan för att upprätthålla och återställa verksamhetskritiska funktioner vid tillfälle för en säkerhetsincident?
- Finns det en process för incidenthantering, hur uppdateras tekniska försvarsmekanismer och processer utifrån lärdom av inträffade säkerhetsincidenter?
- Är kommunens IT infrastruktur ändamålsenlig avseende tillgänglighet och integritet av kritisk data ut ett användarperspektiv?
- Har kommunen ett ändamålsenligt arbetssätt för att hantera risker relaterade till prioriterade hot inom område för IT säkerhet?
    - Styrande dokument
    - IT processer; behörighet, programförändring
    - Kartläggning; säkerhet i mjukvara, fysisk säkerhet – i förhållande till "good practice"
    - Samarbete med tredjepart

2 Metod och avgränsning

Inom ramen för uppdraget har PwC genomfört intervjuer med utvalda personer på Höör och Hörby kommun, analyserat dokumentation i form av styrande dokument, utfört en fördjupad teknisk analys (BSA) av säkerhetsinställningar på servrar som utgör domänkontrollanter i nätverket samt fysisk granskning av serverhall.

Intervjuer har utförts med följande personer:

- Joakim Andersson, IT-chef
- Hans Magnusson, IT-strateg
- Heinz Borchmann, IT-tekniker
- Ola Haraldsson, IT-tekniker
- Björn Thornell, Nätverkstekniker
- Cathrin Möller, IT-strateg/samordnare – social sektor, Höör kommun

Granskade dokument:

- Informationssäkerhetsinstruktion för Användare (Informationssäkerhetsinstruktion - Användare.pdf)
- Informationssäkerhetsinstruktion för Förvaltning (Informationssäkerhetsinstruktion – Förvaltning.pdf)
- Riktlinjer för informationssäkerhet (Riktlinjer för informationssäkerhet.pdf)
- Backup-policy (UNIKOM_Backupplan_v4.pdf)
- Organisationskarta Unikom (Unikom - PwC.pdf)

Baseline Security Assessment (BSA):

Som en del av granskningen utfördes en generell analys av säkerheten i IT-miljön. Via ett script analyserades domänkontrollanter i IT-miljön, och nivån av kontroll och säkerhetsinställningar jämfördes mot Center for Internet Security's (CIS) riktlinjer. En separat rapport har lämnats till Unikom för utvärdering och uppföljning.

3 Inledning

Höör och Hörby kommun, tillsammans med Östra Göinge kommun, är i nuläget i en process av att samordna sin IT-avdelning i ett kommunalägt bolag benämnt Unikom. Vid tid för granskning är denna process ej klar. Beräknat startdatum för det nya bolaget är satt till 1 juli 2016. IT-driften för Höör och Hörby kommun slogs ihop 1 januari 2011. Hässleholm kommun var även tilltänkta medägare till det nya bolaget, men valde att ej vara med. Vid tidpunkten för avhoppet hade större delen av Hässleholm kommuns IT-miljö redan migrerats, och mycket arbete kommer krävas för att separera miljöerna.

De styrande dokument som har granskats är ej uppdaterade enligt den nya strukturen, vilket ska beaktas i observationer och iakttagelser som noteras i rapporten. De styrande dokumenten kommer framåt att ersättas med uppdaterade versioner, då fokus i nuläget är på drift av IT och omstrukturering till den nya organisationen Unikom. Enligt IT-chefen kommer uppdatering av styrande dokument att påbörjas när omstruktureringen till Unikom är färdigställd.

4 Observationer och påverkan

Nedan följer en sammanställning över de revisionsfrågor som den genomförda granskningen avser besvara.

4.1 Finns prioriterade hot mot kommunens IT säkerhet dokumenterade och uppdateras dokumentationen löpande?

Den utförda granskningen påvisar att det inte finns någon dokumentation som beskriver prioriterade hot mot kommunens strategiska IT-resurser och känslig fast data. Det saknas en formell process där förvaltningarna aktivt över tid löpande analyserar interna och externa hot mot verksamhetens IT-miljö och tillsammans med Unikom identifierar kontroller för att hantera de identifierade riskerna.

4.1.1 Riskanalys av applikationer

Det har ej genomförts någon riskanalys på applikationsnivå inom respektive förvaltning. Office 365 är dock ett undantag, där en riskanalys genomfördes i samråd med Microsoft inför uppstarten. Enligt IT-policyn ska ”hotbilden för varje enskilt informationssystem som är av vikt för vår verksamhet analyseras fortlöpande...”.

4.1.2 Sammanställning över verksamhetskritiska applikationer

Unikom har en förteckning över applikationer som används i respektive kommuns olika förvaltningar. Förteckningen inkluderar även vilken eller vilka personer som är systemförvaltare inom respektive förvaltning. Någon analys och/eller sammanställning över vilka av dessa som är identifierade som verksamhetskritiska finns ej dokumenterad.

4.1.3 Påverkan

Att inte arbeta aktivt med att identifiera interna och externa hot mot en verksamhet och ej heller arbeta med riskanalys på applikationsnivå kan leda till olika typer av incidenter mot den övergripande systemmiljön med risk för stora driftstörningar och förlust av känslig fast data. Det finns även en risk att investeringar och arbetssätt fokuserar på icke prioriterade områden i förhållande till faktiska hot.

4.2 Hur ser organisationen och ansvarsfördelning ut i frågor rörande IT säkerhet?

I policydokumentet *”Riktlinjer för informationssäkerhet”* finns det en roll- och ansvarsbeskrivning över de grupper/personer som arbetar med området för IT- och informationssäkerhet. Det är policyn som ska ligga till grund för hur arbetet kring IT- och informationssäkerhet är organiserat och hur styrning av området ska säkerställa efterlevnad enligt policyn.

Dokumenterade roller och ansvar enligt policyn stämmer dock inte överens med hur organisationen är strukturerad i praktiken. Exempelvis finns det ej någon IT-säkerhetschef inom organisationen.

Inom Unikom är ansvaret uppdelat på verksamhetsområdesgrupper enligt en organisationskarta. Respektive verksamhetsområdesgrupp är ansvarig för IT-säkerheten inom det området. Processer för arbetet gällande IT-säkerhet inom verksamhetsgrupperna är informella och någon dokumentation av arbetet genomförs ej. Informella processer existerar även, där information rörande IT-säkerhet utbyts löpande mellan de olika grupperna. Det informella arbetssättet underlättas dock av faktumet att det arbetar 15 personer på hela Unikom.

IT-chefen samordnar arbetet med IT-och informationssäkerhet inom Unikom samt rapporterar till kommunstyrelsen. Det finns dock inga nedskrivna riktlinjer för vad denna rapportering skall innehålla gällande IT-säkerhet, samt när eller i vilket format rapporteringen skall ske. Enligt IT-policyn har kommunstyrelsen det övergripande ansvaret för respektive kommuns informationssäkerhet.

4.2.1 Systemägare och systemförvaltare

Respektive förvaltning är enligt policy systemägare för förvaltningens samtliga applikationer. En eller flera personer inom förvaltningen utses därefter till att bli systemförvaltare. En förteckning över applikationer per förvaltning och respektive systemförvaltare finns dokumenterad.

Systemförvaltaren har ansvar för den dagliga användningen av IT-systemet, vilket enligt policyn inkluderar administration av behörigheter i system samt att delta i arbetet om IT-säkerhetsfrågor.

4.2.2 Styrning och rapportering

I den organisation- och ansvarsfördelning som beskrivs i policyn saknas det en tydlig beskrivning över hur rapporteringsvägar är strukturerade. Vidare framgår det ej vad det är som ska rapporteras i form av tydliga mätpunkter till ansvariga personer/funktioner, med syfte att säkerställa efterlevnad av innehåll i policy, i förhållande till formulerade målsättningar. Det saknas även riktlinjer avseende vilken frekvens mätpunkter ska rapporteras till ledande personer/funktioner.

4.2.3 Påverkan

Styrande dokument som inte tydligt uttrycker roller, ansvar och rapporteringsvägar med tydliga mätpunkter medför en risk att styrning av området för IT- och informationssäkerhet inte utförs mot uppsatta målsättningar. Vidare har existerande policydokument ej uppdaterats sedan 2013. Avsaknad av styrning av området för IT- och informationssäkerhet kan leda till incidenter mot den övergripande systemmiljön med risk för stora driftstörningar och förlust av känslig fast data.

4.3 Finns det en tydlig plan för att upprätthålla och återställa verksamhetskritiska funktioner vid tillfälle för en säkerhetsincident?

4.3.1 Kontinuitetsplan

Den utförda granskningen har inte påvisat att det finns en dokumenterad kontinuitetsplan för kommunen. Enligt IT-chefen fanns det planer på att upprätta en kontinuitetsplan i samband med skapandet av övriga policydokument, men arbetet slutfördes aldrig. Kontinuitetsplan skall dock upprättas när omorganiseringen till Unikom är slutförd. Ett serviceavtal har upprättats med Microsoft, där supporttekniker beger sig till Unikom inom fyra timmar i händelse av en allvarligare incident. Även central nätverksutrustning har avtal med kort inställelsetid.

4.3.2 Backuprutiner

Det finns en formell backup-policy på plats, som bland annat beskriver på en övergripande nivå de metoder och procedurer som används för att återställa lagrad data. Det finns dock ingen detaljerad arbetsbeskrivning för hur återställning från backup sker för olika system/servrar. Unikom använder sig av generella metoder som är dokumenterade hos leverantören. Backup tas minst en gång per dygn och maximal dataförlust är angiven till 24h för samtliga system/applikationer. För vissa verksamhetssystem genomförs SQL-dumpning av databasen flera gånger per dygn. Backup tas endast till disk. Ingen data lagras längre än i 180 dagar. Backup lagras åtskilt från serverhallen genom att den skapas i Hörby och sedan skickas över till en serverhall på ett geografiskt lämpligt avstånd varje dag, där en kopia av backupen lagras.

Det finns i dagsläget inget SLA (Service Level Agreement) mot förvaltningarna som i detalj beskriver hur stor dataförlust verksamheten är villig riskera per verksamhetssystem eller katalogstruktur på nätverket. Verksamheten har dock tagit del av och accepterat backuppolicyn och dess frekvens.

Test av återläsning av backup utförs vid tillfälle, dock dokumenteras inte dessa tester.

4.3.3 Påverkan

Avsaknad av en formell kontinuitetsplan medför en risk för längre driftstörningar i affärskritiska system vid tillfälle för en incident. Acceptabel nivå av dataförlust måste verifieras med verksamheten för att säkerställa att data inte går förlorad vid en driftstörning.

4.4 Finns det en process för incidenthantering och hur uppdateras tekniska försvarsmekanismer och processer utifrån lärdom av inträffade säkerhetsincidenter?

Den utförda granskningen har påvisat att det inte finns någon formell rutin för incidenthantering där lärdom tas från inträffade säkerhetsincidenter. Det finns en formell rutin för registrering och administration av säkerhetsincidenter. Unikom använder sig idag av ett ärendehanteringssystem där användare kan göra felanmälningar gällande IT. Det saknas en tydlig definition över vilka händelser/ärenden som utgör en incident och hur olika typer av incidenter skall klassificeras och eskaleras. Beroende på hur en incident klassificeras kommer åtgärder tas med syfte att återställa påverkan från incidenten till ett normalläge.

Ärenden inkommer till first line-support som vid behov eskalerar ärendet till berörd verksamhetsområdesgrupp (t.ex. applikation, server eller nätverk). Samtliga anställda på Unikom, förutom IT-chefen, arbetar med ärenden i någon utsträckning. Det existerar informella processer för uppdatering av tekniska försvarsmekanismer baserat på inträffade incidenter. Detta arbete sker genom informella diskussioner och utbyte av information inom Unikom. Informella rutiner existerar för åtgärder vid t.ex. virusutbrott inom nätverket eller en specifik enhet.

4.4.1 Påverkan

Avsaknad av en formell rutin för uppdatering av försvarsmekanismer baserat på incidenthantering kan medföra en risk att likartade incidenter inte identifieras och hanteras i tid. Detta ökar risken för externa- och interna dataintrång i IT-miljön. En formell process för incidenthantering är även en förutsättning för att verksamheter kontinuerligt ska lära sig av tidigare erfarenheter och ständigt arbeta med att förbättra sin förmåga i att hantera hot relaterade till IT- och informationssäkerhet.

4.5 Är kommunens IT-infrastruktur ändamålsenlig avseende tillgänglighet och integritet av kritisk data ur ett användarperspektiv?

4.5.1 Tillgänglighet till kritisk data

Kommunerna i Skåne nordost har ett samarbete där man delar på internetförbindelse och övergripande IT-infrastruktur. Detta inkluderar redundans i nätet, med två separata internetförbindelser samt redundans för alla viktigare knutpunkter i IT-infrastrukturen. För fjärråtkomst till nätverket används VPN. Backup genomförs varje natt och lagras åtskilt från serverhallen. Den fysiska säkerheten i serverhallen i Hörby är enligt "good practice". Vid en allvarligare incident riskerar dock tillgängligheten att bli begränsad då det saknas en formell kontinuitetsplan.

4.5.2 Integritet av kritisk data

Inga användare i nätverket är lokal administratör på sin klient, vilket innebär att risken för säkerhetsincidenter minskar. Vidare visar resultatet från Baseline Security Assessment (BSA) på en god säkerhetsnivå för servrar. Dock har databasadministratörer full tillgång till verksamhetssystems databaser. Loggning sker endast av inloggning till databasen och loggen sparas lokalt på servern. Det genomförs heller ingen periodisk genomgång av loggarna.

Verktyget ADAudit har nyligen implementerats för att administrera loggar från servrar (ej databaser). Verktyget varnar via email vid ändringar i Active Directory och serverstrukturen, som anses kritiska.

4.5.3 Påverkan

Ur ett användarperspektiv bedömer vi IT-infrastrukturen som ändamålsenlig utifrån ovan, både avseende tillgänglighet och integritet av kritisk data. Avsaknaden av dokumentation och formella processer, i synnerhet i form av en kontinuitetsplan, ökar dock risken för att tillgängligheten påverkas vid en incident. Avsaknaden av formella processer för, och loggning av, direkta databasändringar ökar risken att integriteten av kritisk data påverkas.

4.6 Har kommunen ett ändamålsenligt arbetssätt för att hantera risker relaterade till prioriterade hot inom område för IT säkerhet?

Nedan följer en sammanställning över olika arbetssätt/kontroller som verksamheten idag använder för att hantera risker relaterade till område för IT- och informationssäkerhet. Det är viktigt att belysa att området för IT- och informationssäkerhet i verksamheter inte endast utgörs av tekniska kontroller som ägs av tekniskt ansvarig. För att hantera komplexiteten i hot krävs även ett tydligt åtagande från verksamheten. Det är primärt verksamhetens ansvar att identifiera interna och externa hot mot förvaltningar, uppsättning och övervakning av systembehörigheter samt aktiv uppföljning av systemloggar.

4.6.1 Styrande dokument

Styrande dokument, förutom backup-policy, saknas. Det finns dock tre policydokument från 2013 som berör informations- och IT-säkerhet, för användare samt systemförvaltning. Dessa dokument saknar till viss del förankring i organisationens arbetssätt. Processer och arbetsrutiner inom Unikom är ej dokumenterade, vidare saknas en kontinuitetsplan.

4.6.2 Behörighetsprocessen

IT ansvarar för uppsättning av användarkonton i kommunens nätverk, samt för de applikationer som använder sig av single sign on. Användarkonton på nätverksnivå finns för anställda som det beställts till samt elever, och medger åtkomst till grundläggande IT-funktioner så som e-post och standardprogram på arbetsstationen. Unikoms ansvar i processen är endast att göra teknisk setup av användarkonton. Active Directory (AD) används för att administrera behörigheter centralt.

Det finns i dagsläget ingen formell rutin dokumenterad för administration av behörigheter i vare sig nätverket eller verksamhetsapplikationer. Behörighetsprocessen startar med att den anställdes närmsta chef skapar ett ärende i ärendehanteringssystemet Nilex, vilket sker genom ett digitaliserat formulär. Efter kontroll att ärendet skapats av behörig person, tilldelas behörighet i AD:t. Detta sker genom Runbooks, som är en automatiserad process för att säkerställa att alla användare skapas enligt samma struktur, vilket i sin tur medger en standardisering av behörighetsprocessen. Samma process åtföljs vid förändring, borttag, eller inaktivering av behörigheter. Konton som skapats men som aldrig använts på 90 dagar inaktiveras. Konton som använts vid något tillfälle men där användaren inte loggat in på ett år inaktiveras. Ingen periodisk genomgång av aktiva behörigheter genomförs.

Den enskilda förvaltningen ansvarar för administration av behörigheter i de av verksamhetens applikationer som ej använder sig av single sign-on genom AD. Det är den anställdes närmsta chef på den enskilda förvaltningen som beslutar om vilken behörighet en specifik användare ska ha. Systemförvaltaren på den enskilda förvaltningen ansvarar för att sätta upp rollstrukturen i en applikation.

I vissa verksamhetssystem administreras behörigheter med en blankett som ska skrivas under av den anställdes närmsta chef samt att användare som ej har varit inloggade på 30 dagar inaktiveras i systemet. Denna kontroll utförs var femte vecka.

Granskningen har inte påvisat att det finns kontroller implementerade ute i förvaltningarna för att säkerställa att behörigheter i kritiska applikationer övervakas för att säkerställa att behörigheter stämmer överens med den anställdes roll i förvaltningen. Enligt IT-chefen förekommer det att användare får behålla sina tidigare behörigheter när de t.ex. byter tjänst, vilket bidrar till en ökad risk för konflikter gällande "segregation of duties".

Detta beror till stor del på att verksamheten inte meddelar Unikom vilka rättigheter som ska tas bort i samband med en behörighetsförändring.

Loggning

Det sker i dagsläget ingen regelbunden uppföljning av aktiviteter utförda av priviligierade användarkonton som används av anställda inom Unikom, för att hantera förändringar på server- och databasnivå.

På databasnivå loggas inloggningar till servern, dock sparas loggen lokalt på samma server. Samtliga administratörskonton inom IT är personliga och skall endast användas då en förhöjd behörighet krävs för att hantera en viss aktivitet. Anställda inom Unikom har i övriga fall tillgång till sitt personliga användarkonto för att hantera normala arbetsuppgifter inom rollen.

För ett urval av verksamhetssystem sker loggning av händelser i systemet och ett urval av dessa loggar analyseras fyra gånger årligen, för att identifiera otillbörliga aktiviteter. Loggrutiner finns formellt beskrivna i dokument för vissa verksamhetssystem. Granskningen har inte påvisat styrande dokument på en verksamhetsövergripande nivå för rutiner kring loggning och uppföljning av dessa.

4.6.3 Programförändringsprocessen

Infrastruktur

Det saknas i dagsläget en formell rutin som beskriver förändringshantering avseende infrastruktur inomUnikom. Ingen utveckling av programvara utförs överhuvudtaget, förutom på Sharepoint-portalerna. Integrationer mellan applikationer utvecklas av Unikom, men det handlar oftast om script som körs, ej egentliga kodförändringar. Det sker ingen formell dokumentation av dessa förändringar, som utförs efter förfrågan från systemförvaltare.

Patchning av servrar hanteras genom System Center Configuration Manager. Servrar är uppdelade i fyra olika grupper, baserat på en avvägning mellan risken att servern står utan senaste säkerhetspatchen och risken att fel uppstår vid patchning. Den första gruppen får automatiskt kritiska säkerhetspatchar direkt när de släpps från leverantören. Andra och tredje gruppen får dessa med ca en respektive två veckors fördröjning. För den fjärde gruppen innebär det att alla patchar installeras helt manuellt. Domänkontrollanterna är inkluderade i den första gruppen och har således alltid de senaste säkerhetspatcherna installerade. Patchar som ej är kategoriserade som säkerhetspatchar eller kritiska, installeras alltid manuellt.

Applikationer

På applikationsnivå sker inga programförändringar av Unikom själva. All utveckling sker av systemleverantörer och installeras sedan av IT. Installation av programförändringar brukar även köpas in som en tjänst av systemleverantören eller konsulter

4.6.4 Fysisk säkerhet

Serverhallen har granskats fysiskt utan väsentliga anmärkningar och den övergripande bedömningen är att serverhallen uppfyller standardkraven för fysisk säkerhet. För åtkomst till serverhallen krävs en tagg samt kod, och ytterligare en kod behövs sedan för att öppna varje enskilt serverrack. All passage till serverhallen loggas. När ett serverrack öppnas skickas även ett mail till IT om att så har skett. Fyra personer har tillgång till serverhallen. Det finns två brandsläckningssystem av typ gas. Ett för hela rummet och ett som är kopplat till varje enskilt rack. UPS och dieselgenerator finns i en angränsande byggnad. Det är redundans både för elförsörjning och kylsystem. Övervakning finns för både brand, inbrott och luftfuktighet, larm går både till IT och ett vaktbolag. Den enda anmärkningen vid inspektionen, är att serverhallen har placerats i källaren, vilket ökar risken för och effekten av en vattenläcka. Dock har denna risk mitigerats genom övervakningssystem.

Backup lagras på en sekundär site på ett geografiskt lämpligt avstånd, och filer återskapas därifrån vid behov. Backup genomförs varje natt för samtliga virtuella servrar.

4.6.5 Säkerhet i mjukvara

Kommunens underliggande nätverk är segmenterat, vilket innebär att de olika subnäten inte är direkt sammankopplade. För att minska risken av obehörigt intrång är utbildningsnätet separerat från övriga subnät med brandvägg. Sammanlagt är nätverket segmenterat i tre klientnät och tre servernät.

Servermiljön är helt virtualiserad genom Microsoft Hyper-V och operativsystem är uteslutande Windows Server 2008R2 – 2012R2.

Microsoft System Center Endpoint Protection (SCEP) används som antivirus både på klienter och servrar. Det säkerställer att samtliga arbetsstationer i nätverket använder rätt version och servicepack för antivirusprogrammet.

Uppdateringar av regelverket i antivirusskyddet sker per automatik, vilket innebär att när en leverantör av antivirusskydd har identifierat ett nytt hot, distribueras uppdateringar automatiskt ut till mjukvarans regelverk för att hantera det nya hotet. SCEP larmar via email om en klient har fått virus, varvid åtgärder kan vidtas. En webbtvätt håller på att implementeras, arbetat var vid granskningen ej slutfört. En mailtvätt finns i drift, som även den stoppar virus.

Lösenordspolicy

Det finns inom Höör och Hörbys kommuner en lösenordspolicy som applicerar på de verksamhetsövergripande systemen så som inloggning via Active Directory. Lösenordspolicyn är i linje med "good practice" för lösenordshantering. Det saknas dock ett styrande dokument som tydliggör vilka inställningar som ska appliceras vid installation av en ny server för att säkerställa att installationen görs för att hantera säkerhetsrisker på servernivå.

För applikationer i de olika förvaltningarna finns det ingen enhetlig kontroll för att applicera den vedertagna lösenordspolicyn inom kommunen ner på applikationsnivå. Ett undantag är de applikationer där "single sign-on" används, det vill säga användarkontot i nätverket används även direkt för att logga in i en applikation. I övriga applikationer kan avvikelser till den centrala lösenordpolicyn förekomma. Risken är att det finns verksamhetskritiska applikationer i förvaltningarna med svaga kriterier för inloggning och lösenordskrav.

Baseline Security Analysis (BSA)

PwC har utfört en BSA på två av kommunens servrar som utgör domänkontrollanter avseende användarkonton och säkerhetsinställningar. Noterade iakttagelser i samband med granskning av säkerhetinställningar bedöms inte som allvarliga. Den finala rapporten är lämnad till Unikom för vidare uppföljning.

4.6.6 Samarbete med tredje part

Samarbete med tredje part sker med både leverantörer av verksamhetssystem samt konsulter. För samtliga verksamhetssystem finns det SLA upprättade mellan verksamheten och leverantören.

Konsulter anlitas när spetskompetens behövs. IT-chef uppskattar att dessa isolerade insatser sker runt fyra gånger om året. Oftast ändrar konsulterna ej i systemet själva, utan anlitas för diskussion och design av lösningar tillsammans med IT. Lösningar implementeras sedan av IT själva eller av konsulter och IT tillsammans. Konsulter har med andra ord i regel ej egen åtkomst till nätverket och/eller applikationer. Konsulter anlitas även vid större uppdateringar av verksamhetssystem, ungefär två gånger per år.

4.6.7 Påverkan

Otillräckliga kontroller på olika nivåer i verksamheten, både tekniska och manuella, kan resultera i olika typer av incidenter mot den övergripande systemmiljön med risk för driftstörningar och förlust av känslig data.

5 Revisionell bedömning och rekommendationer

Granskningens revisionsfråga: *Är kommunens hantering av IT-säkerhet ändamålsenligt och effektivt i förhållande till de prioriterade IT-hoten mot kommunens IT-miljö?*

Efter genomförd granskning baserat på kontrollfrågorna görs bedömningen att kontrollen över intern IT- och informationssäkerhet, har utrymme för förbättringsåtgärder. Den övergripande granskningen av tekniska kontroller som övervakas av IT bedöms tillfredställande utan några tydligt påvisade brister. Fysisk säkerhet i serverhall, säkerhet i mjukvara samt i den övergripande IT-infrastrukturen bedöms som god. Tekniska kontroller kan dock bli än mer effektiva och behov av nya kontroller kan tillkomma, när en riskanalys för verksamheten utförs med utgångspunkt i externa och interna hot.

Nedan följer en sammanställning över granskningens största iakttagelser

1) Det saknas en formell process för att löpande analysera risker och hot mot kommunens övergripande verksamhet. Nuvarande riskanalyser har utgångspunkt i enskilda applikationer, men med nuvarande tekniska utveckling i samhället har helt nya typer av hot tillkommit, som har utgångspunkt i externa faktorer. Iakttagelsen medför att kontroller och arbetsinsatser inom området för IT- och informationssäkerhet inte har utgångspunkt i faktiska hot. Det finns en risk att fokus för riskhantering och investeringar görs i icke prioriterade områden.

2) Nuvarande organisationen i form av roller, ansvarsområden, rapporteringsvägar samt nyckeltal för styrning av området för IT- och informationssäkerhet, är inte tydligt definierade i styrande dokument. Iakttagelsen medför att hot och risker inom IT- och informationssäkerhet är svåra att övervaka och hantera. Arbetssättet inom område för IT- och informationssäkerhet riskerar att blir mer reaktivt än proaktivt, vilket försvårar för verksamheten att förbättra riskhanteringsprocessen på sikt.

Nedan följer våra bedömningar och rekommendationer utifrån granskningens kontrollfrågor.

5.1.1 Finns prioriterade hot mot kommunens IT säkerhet dokumenterade och uppdateras dokumentationen löpande?

Efter genomförd granskning av kontrollfrågan är bedömningen att det i dagsläget saknas en dokumenterad förståelse för prioriterade hot mot kommunens IT-säkerhet.

PwC rekommenderar Höör och Hörby kommun att utvärdera följande åtgärder:

1) Etablera en process inom respektive förvaltning där ansvariga årligen utvärderar externa och interna risker och hot mot verksamheten.

2) Genomföra en prioritering av de identifierade hoten kopplat till risk, utifrån sannolikhet och påverkan på verksamheten vid tillfälle för en incident. Varje identifierad risk ska analyseras utifrån vilken teknisk plattform nätverk/server/databas/applikation/fast data som kan komma att påverkas vid en incident. Den utförda riskanalysen ska dokumenteras inom respektive förvaltning.

3) Implementera kontroller av både teknisk och manuell karaktär med syfte att övervaka identifierade risker. Kontroller bör designas så att de utgör tydliga nyckeltal för uppföljning om en kontroll har utförts med syfte att hantera en specifikrisk.

4) Etablera en organisation med tydliga roller och ansvarsområden i övervakningen av de identifierade riskerna samt implementera en tydlig struktur för avrapportering av nyckeltal på löpande basis.

5.1.2 Hur ser organisationen och ansvarsfördelning ut i frågor rörande IT säkerhet?

Efter genomförd granskning av kontrollfrågan är bedömningen att organisationen och ansvarsfördelning i område för IT- och informationssäkerhet behöver tydliggöras ytterligare i form av roller, ansvarsfördelning och rapporteringsvägar.

PwC rekommenderar Höör och Hörby kommun att utvärdera följande åtgärder:

1) Implementera en organisation med roller som motsvarar de behov som faktiskt finns i verksamheten för att övervaka område för IT- och informationssäkerhet i form av identifierade risker. Nuvarande rollstruktur bör utvärderas på rollnivå för att utvärdera om roller fyller en funktion i förhållande till faktiska risker.

2) Rollbeskrivningar och ansvarsområden behöver tydliggöras i mer detalj. I nuvarande policydokument är ansvarsområden generellt formulerade vilket medför risk för egentolkningar av ansvar och därmed försämrad styrning av IT- och informationssäkerhetsområdet.

3) Styrning och rapportering av området för IT- och informationssäkerhet behöver formaliseras.

    a. *Implementation av kontroller:* Utifrån identifierade risker och hot mot området för IT- och informationssäkerhet bör kontroller implementeras med syfte att övervaka och hantera identifierade risker. Varje kontroll bör ha ett tydligt bevis på att den är utförd av kontrollansvarig. Ansvar för att kontroller utförs måste tydliggöras för verksamheten och kopplas till ansvarsområden.

    b. *Implementation av nyckeltal:* Implementation av tydliga mätpunkter med syfte för ansvariga att utvärdera om målsättningar för IT- och informationssäkerhet uppnås och ständigt förbättras. Nyckeltal måste vara utformade så att det är möjligt att utvärdera hur verksamheten presterar i förhållande till faktiska mål. Tydliga mätpunkter utgör grunden till ständig utveckling och förbättring i verksamhetsprocesser relaterat till IT- och informationssäkerhet.

    c. *Rapportering:* Rapporteringsvägar mellan roller måste tydliggöras, där avrapportering av utförda kontroller med tillhörande nyckeltal görs enligt en viss periodicitet med syfte att styra och övervaka området för IT- och informationssäkerhet.

5.1.3 Finns det en tydlig plan för att upprätthålla och återställa verksamhets kritiska funktioner vid tillfälle för en säkerhetsincident?

Efter genomförd granskning av kontrollfrågan är bedömningen att det i nuläget inte finns någon dokumenterad kontinuitetsplan.

PwC rekommenderar Höör och Hörby kommun att utvärdera följande åtgärder:

1) Upprätta en formell kontinuitetsplan och implementera planen så snart som möjligt. Kontinuitetsplanen bör även åtföljas av arbetsrutiner på detaljnivå för att återskapa virtuella servrar och filer utifrån backup.

2) Tillsammans med respektive förvaltning, inventera kritiska system och katalogstrukturer på nätverket, för varje system/katalogstruktur definiera verksamhetens tolerans för dataförlust. Uppdatera den formella backup-policyn med verksamhetens acceptans för dataförlust för respektive kritiskt verksamhetssystem.

5.1.4 Finns det en process för incidenthantering och hur uppdateras tekniska försvarsmekanismer och processer utifrån lärdom av inträffade säkerhetsincidenter?

Efter genomförd granskning av kontrollfrågan är bedömningen att det i nuläget inte finns någon formel process för incidenthantering, bortsett från att registrera och administreraärenden.

PwC rekommenderar Höör och Hörby kommun att utvärdera följande åtgärder:

1) Implementera en formell process för incidenthantering, samt dokumentera processen.
2) Etablera rutiner där verksamheten kontinuerligt utvecklas med lärdom av de incidenter som inträffat, varje incident ska leda till en förändringsåtgärd med syfte att minska risken för en liknande incident ska inträffa i framtiden.

3) Integrera processen som en del av styrningen av IT- och informationssäkerhetsområdet med tydliga nyckeltal för avrapportering till ansvarig.

5.1.5 Är kommunens IT infrastruktur ändamålsenlig avseende tillgänglighet och integritet av kritisk data ut ett användarperspektiv?

Efter genomförd granskning av kontrollfrågan är bedömningen att IT-infrastrukturen är ändamålsenlig avseende tillgänglighet och integritet av kritisk data. Det finns en förbättringspotential avseende loggning och övervakning av aktiviteter utförda av priviligierade användarkonton inom IT

PwC rekommenderar Höör och Hörby kommun att utvärdera följande åtgärder:

1) Formalisera och dokumentera den existerande rutinen för loggning av kritiska aktiviteter för servrar. Implementera en formaliserad rutin för periodisk uppföljning av loggar, rutinen ska inkludera dokumentation av uppföljningen.

2) Designa, dokumentera och implementera en rutin för loggning av kritiska aktiviteter på databaser samt periodisk uppföljning av loggar. Rutinen kan integreras i det existerande verktyget ADAudit som används för serverloggar.

3) Upprätta en formell kontinuitetsplan och implementera planen så snart som möjligt. Kontinuitetsplanen bör även åtföljas av arbetsrutiner på detaljnivå för att återskapa virtuella servrar och filer utifrån backup.

5.1.6 Har kommunen ett ändamålsenligt arbetssätt för att hantera risker relaterade till prioriterade hot inom område för IT säkerhet?

Efter granskning av kontrollfrågan är bedömningen att kontroller för arbetssätt inom Unikom till stora delar fungerar tillfredställande. Det finns en förbättringspotential i arbetssätt hos förvaltningar primärt relaterat till hur administration av behörigheter hanteras.

PwC rekommenderar Höör och Hörby kommun att utvärdera följande åtgärder:

1) Formalisera rutinen för administration av behörigheter så att det även är möjligt att hantera nyregistrering, uppdatering och borttag av behörigheter för verksamhetsapplikationer i det centrala verksamhetssystemet för ärendehantering. Processen ska inkludera administration av systembehörigheter ner på förvaltningsnivå vilken idag hanteras informellt ute i respektive förvaltning.

2) Formalisera rutinen för administration av behörigheter på förvaltningsnivå där systemförvaltare periodvis granskar och godkänner aktuella systembehörigheter i kritiska system. Utförandet av kontrollen kan fungera som en tydlig mätpunkt (KPI) i rollen för systemägare, med syfte att säkerställa att aktuella systembehörigheter stämmer överens med den anställdes roll i förvaltningen.

3) Inom respektive förvaltning, identifiera kritiska verksamhetssystem samt kritiska transaktioner/känslig data inom respektive system. Aktivera systemloggning för att säkerställa spårbarhet i övervakade transaktioner/förändringar i känslig data. Definiera tydliga nyckeltal i rollen för systemägare där kritiska transaktioner och förändring av känslig data övervakas och godkänns enligt ett visst intervall. Avvikelser följs upp och rapporteras som en del av styrningsmodellen för IT-säkerhet.

pwc

Henrik Friang, Projektledare

Lena Salomon, Uppdragsledare