www.pwc.se

Övergripande säkerhetsgranskning av kommunens säkerhet angående externa och interna dataintrång

Lomma Kommun

Henrik Friang

Säkerhetsspecialist, PwC

December 2015

pwc

Innehållsförteckning

1. Sammanfattning

1.1 Fokusområden

Nedan presenteras tre fokusområde vilka utifrån genomförd granskning bör prioriteras och vara vägledande i val av vilka projekt som kommunen framgent bör fokusera på.

- Färdigställa IT-säkerhetshandboken, avseende rutinbeskrivningar kring avbrottsplan, katastrofplan samt bemanning.
- Etablera en process för systematisk uppföljning av incidenter.
- Som en del av processen för användaradministration, bör en kontroll för periodvis genomgång användarkontons behörigheter etableras, för att säkerställa att dessa är i linje med användarens arbetsbeskrivning.

1.2 Slutomdöme

Efter genomförd granskning, bedömer vi att det finns förutsättningar för att Lomma kommun ska ha en god IT och informationssäkerhet. Vår granskning har visat att kommunen proaktivt arbetar med att minska kommunens beroende av individer på IT-avdelningen genom formaliserade dokument, rutiner samt att kommunen till stor del försöker automatisera kontroller för exempelvis åtkomsthantering. Vidare har kommunen etablerat samarbeten med externa leverantörer, avseende drift och övervakning av verksamhetskritiska system.

2. Inledning

2.1. Bakgrund

Med begreppet IT menas informationsteknik som innefattar teknik för elektronisk framställning, lagring, överföring och presentation av information. Tekniken kan bestå av hårdvara, nät, kommunikation och program-varor av olika slag. Betydelsen av IT ökar allt mer inom kommunens olika verksamhetsområden och förändringar sker kontinuerligt. Kommunen hanterar många känsliga uppgifter. Brister i säkerheten kan ge stora konsekvenser såväl för kommunen som för enskilda personer.

Vår definition med IT-säkerhet menas här alla olika åtgärder som används för att för att skydda och säkerställa åtkomsten av information samt att interna och externa regelverk följs.

Granskningen syftar till att översiktligt granska kommunens IT-säkerhet.

2.2. Revisionsfråga och kontrollfrågor

Granskningen ska besvara följande revisionsfråga:

Finns förutsättningar för en god IT/informationssäkerhet?

Granskningen inriktas mot följande kontrollfrågor:

- Finns aktuella styrande och stödjande dokument som berör IT-säkerhet och är dessa införda inom nämnderna?
- Finns tydligt ansvar för att arbeta aktivt med frågor som berör IT-säkerhet?
- Finns bra rutiner för rapportering av problem och säkerhetsrelaterade händelser?
- Är förekomst av störningar och problem rimliga?
- Finns ett tillräckligt skydd kring rum som används för datordrift för att förhindra störningar, obehörigt tillträde och stöld?
- Finns tillfredsställande rutiner för hantering av behörighet till gemensamt nätverk?

2.3. Metod och avgränsning

Inom ramen för uppdraget har PwC genomfört intervjuer med utvalda personer Lomma kommun och genomfört analys av dokumentation samt en verifikation av kontohantering och säkerhetsinställningar på server- och operativsystemnivå.

Granskningen avgränsas till nämnda översiktliga kontrollmål och kontrollfunktioner i separata system innefattas inte.
Granskningsobjektet är i första hand kommunstyrelsen (övergripande ansvar för IT inom kommunen). Dock berörs till vissa delar kommunens samtliga nämnder inom kommunen då de har ett ansvar för säkerheten inom nämndens område. Granskningen avser verksamhetsåret 2015.

Intervjuer har genomförts med Patrik Flensburg, Servicechef

3. Observationer och påverkan

3.1. Finns aktuella styrande och stödjande dokument som berör IT-säkerhet och är dessa införda inom nämnderna?

Inom Lomma kommun finns det upprättade riktlinjer och policys avseende kommunens IT och säkerhetsrelaterade frågor. Övergripande styrdokument och dokument som behandlar den övergripande strategiska inritningen för kommunens IT-verksamhet finns i form av en IT-policy med tillhörande IT-anvisning. IT-policyn är antagen av kommunfullmäktige och IT-anvisningarna har antagits av kommunstyrelsen. Gällande den dagliga IT-verksamheten inom kommunen, finns dessa riktlinjer i en IT-handbok där dokumentets syfte är att vara ett styrinstrument och ett hjälpmedel i samband med IT-frågor.

Som övergripande styrdokument avseende hur kommunen ska arbeta med IT-säkerhetsfrågor, har kommunen tagit fram, kommunfullmäktige antagit, en säkerhetspolicy. Policyn stipulerar hur kommunen på en övergripande nivå ska arbeta med informationssäkerhet, IT-incidenter samt att det är kommunens IT-chef som ska ansvara för säkerhetslösningar och åtgärder i de digitala informationssystemen.

Som övergripande styrdokument finns i Lomma kommun en, av kommunstyrelsen antagen, IT-säkerhetsanvisning, som tillsammans med kommunens säkerhetspolicy, styr den övergripande och strategiska inriktningen avseende kommunens IT-säkerhet. Vidare har kommunen tagit fram riktlinjer avseende säkerhetsrelaterade frågor som berör IT-verksamheten i form av en IT-säkerhetshandbok. I IT-säkerhetshandboken återfinns en säkerhetspolicy samt anvisningar för hur man inom kommunen bör arbeta med IT-säkerhet. Handboken behandlar områden som kommunens grundläggande säkerhetskrav, säkerhetsinstruktioner, hantering av information samt planer för säkerhet, avbrott samt katastrofer. Ansvaret för att hålla IT-säkerhetshandboken uppdaterad vilar på kommunens IT-chef.

Lomma kommun har etablerat formaliserade rutiner och processer inom områdena åtkomsthantering, intrångshantering samt hantering av driften av kommunens IT. Det finns dock behov av att IT-säkerhetshandboken ytterligare uppdateras samt färdigställs i form av rutinbeskrivningar kring avbrottsplan, katastrofplan samt bemanning.

3.2. Finns tydligt ansvar för att arbeta aktivt med frågor som berör IT-säkerhet?

I IT-säkerhetshandboken som upprättats i Lomma kommun och IT-chefen ansvarar för, definieras ansvaret för kommunens IT-säkerhet. Det tydliggörs att ansvarsfördelning för datasystemsäkerheten är en avgörande förutsättning, för att Lomma kommun ska kunna leva upp till kommunens säkerhetsplan. Ansvarsfördelningen pekar flertalet roller, däribland systemägare, verksamhetsansvariga, systemansvariga, Serviceavdelningen, systemadministratörer, användare samt IT-säkerhetssamordnare. I Lomma kommun har var och en av dessa roller, inom respektive område, ett gemensamt ansvar för IT-säkerheten.

3.3. Är förekomst av störningar och problem rimliga?

Enligt Patrik Flensburg, Servicechef i Lomma Kommun, är störningar och problem i infrastruktur och applikationer numera väldigt ovanliga, sedan man i allt större utsträckning flyttar över kommunens verksamhetssystem till en virtualiserad serverstruktur.

För att vidare säkerställa drift och minimera störningar och problem, har IT-avdelningen nyligen slutfört ett projekt, avseende övervakning av infrastruktur. Den nya lösningen innebär att kommunen numera har dygnet-runt-övervakning på de mest kritiska verksamhetssystemen. Övervakningen hanteras av Lomma kommuns leverantör, ATEA, vilka kommer ansvara för att åtgärda eventuella störningar och problem som uppstår, för att inte vara fullständigt beroende av personal vid kommunens IT-avdelning.

Lomma kommun har även enligt en prioritetsskala mellan 1-5 klassificerat samtliga verksamhetssystem. Utifrån denna klassificering följer IT-avdelningen löpande en förteckning över förekomna störningar och problem som orsakat oplanerade systemavbrott. PwC har tagit del av denna förteckning och har noterat att det totalt förekommit totalt sex oplanerade systemavbrott, varav hälften av dessa har inneburit systemavbrott i de mest kritiska verksamhetssystemen under 2015. Samtliga avbrott har kunnat avhjälpas inom 24 timmar.

3.4. Finns bra rutiner för rapportering av problem och säkerhetsrelaterade händelser?

Lomma kommun har upprättat en prioriteringslista över kritiska verksamhetssystem. Klassificeringsskalan 1-5, där 1 är lägst och 5 är mest kritiskt, ligger till grund för det serviceavtal man har upprättat med kommunens leverantör för övervakning av drift. De mest kritiska systemen, 4-5, övervakas dygnet runt av leverantören, och samtliga förekomster av incidenter och säkerhetsrelaterade händelser, ska hanteras av leverantören och rapporteras till Lomma kommuns IT-avdelning. För verksamhetssystem säkerhetsklassificerade 1-3, får kommunens IT-avdelning ett larm om problem uppstår.

För support, inrapportering av incidenter och säkerhetsrelaterade händelser från användare av kommunens IT-system, använder Lomma kommun ATEA som leverantör, en så kallad ”first-line support”. Supporten upprättar för varje incident, ett ärende i kommunens ärendehanteringssystem. För incidenter som ej kan lösas av ATEAs support, kontaktas Lomma kommuns IT-avdelning för vidare utredning och åtgärder. I kommunens support och incidenthanteringssystem, görs dock ingen uppföljning eller sammanställning för att i efterhand kunna upptäcka trender eller antal förekomster av problem och störningar.

Vidare finns ett krav att samtliga användare som får åtkomst till det gemensamma nätverket, har kunskap om, och förståelse kring organisationens säkerhetsarbete och de säkerhetsåtgärder som gäller för kommunens informationssystem. I detta ingår att samtliga medarbetare, interna som externa har ett ansvar för att rapportera inträffade säkerhetsincidenter gällandes upptäckta säkerhetsbrister till kommunens samordnare, alternativt närmaste chef. Därför beviljas medarbetare behörighet i nätverket, först efter att medarbetaren informerats om organisationens säkerhetsregler. Detta finns tydligt beskrivet i kommunens IT-handbok och säkerställs genom att medarbetaren vid anställning får skriva under att man mottagit och förstått gällande säkerhetsrutiner.

Vidare finns i kommunens IT-handbok fastställt att samtliga medarbetare, återkommande, bör få information om de förändrade hot som verksamheten utsätts för, t.ex. nya typer av virusangrepp samt vilka säkerhetsåtgärder som vidtas för att möta och hantera dessa. Ansvaret för att medarbetarna informeras och utbildas i säkerhetsfrågor ligger hos respektive verksamhetsansvarig. Ingen rutin för att säkerställa att säkerhetsuppdatering delges medarbetare löpande, finns etablerad.

3.5. Finns ett tillräckligt skydd kring rum som används för datordrift förhindra störningar, avbrott, obehörigt tillträde och stöld?

Avseende kommunens fysiska IT-säkerhet, har kommunen etablerat en ändamålsenlig hantering, med lämpliga skalskydd och larm för central och känslig information och infrastruktur. Vidare har kommunen installerat en reserv el-generator för att säkerställa kontinuitet i driften av kommunens centrala IT-system. Kommunens IT-avdelning genomför tillsammans med externa konsulter varje månad testning av denna reservelgenerator.

Kommunens serverpark är till över 95 % virtualiserad genom VMware. Detta bidrar till en skalbar och säker drift, då kommunen vid driftstörning kan sätta upp en ny server inom en timme. Avseende backup av data, har kommunen etablerat en kontinuerlig backupprocess, med dagliga fullständiga backuper samt SQL-backuper varannan timme.

3.6. Finns tillfredsställande rutiner för hantering av behörighet till gemensamt nätverk?

Lomma kommun har upprättat en formell process för hantering av behörighet till det gemensamma nätverket. Processen som till stor del är automatiserad, är uppsatt för att minska administrativa insatser och samtidigt minimera risker vid skapande och borttag av konto till kommunens personal och till elever på kommunens skolor. Avseende dokumentation av processen, finns denna dokumenterad i en funktionsspecifikation för FIM (Forefront Identity Manager). Dokumentet beskriver både övergripande hur processen fungerar, och även detaljspecifikationer över olika scenarier samt önskat resultat efter processen slutförts.

I korthet, går processen ut på att inmatning av användarens uppgifter sker i systemet, Elevsystemet för elever och Personec P för kommunens medarbetare. Därefter läses informationen över i FIM och konton för åtkomst till kommunens IT-miljö ges. Med FIM har kommunen även automatiserat borttag av rättigheter för åtkomst till kommunens IT-miljö. Då kommunens personalavdelning eller elevadministratörer sätter ett avslutsdatum i respektive system för användarhantering, läses detta över till FIM-systemet vilket säkerställer att användarkontots samtliga åtkomsträttigheter automatiskt inaktiveras på önskat datum.

I samband med att kommunen införde FIM-systemet, installerade kommunen en modul för att hantera all nätverksåtkomst till kommunens nät. Modulen bygger på 801.1x, vilket är en standard för portbaserad autentisering. Autentiseringen innebär att användaren avkrävs en autentisering mot kommunens katalogtjänst innan användarens utrustning får tillåtelse att kommunicera på nätverket. Vilket bidrar till en mycket hög nivå av säkerhet, eftersom all utrustning som vill få möjlighet att kommunicera via kommunens nät, måste vara på förhand godkänd.

Ansvaret för att säkerställa att varje användare utifrån sin roll har korrekta behörigheter i kommunens olika informationssystem, vilar på respektive systemansvarig. I Lomma kommun genomförs det inga, på periodvis basis, genomgångar av användarkontons behörigheter för att säkerställa att dessa är i linje med användarens arbetsbeskrivning.

4. Revisionell bedömning och rekommendationer

Granskningens revisionsfråga har varit: *Finns förutsättningar för en god IT/informationssäkerhet?*

Efter genomförd granskning utifrån kontrollfrågorna, bedömer vi att det finns förutsättningar för att Lomma kommun ska ha en god IT och informationssäkerhet, även om ett fåtal områden kan behöva förtydligas och uppdateras.

Vår granskning har visat att kommunen proaktivt arbetar med att minska kommunens beroende av enskilda individers kompetens på IT-avdelningen genom formaliserade dokument, rutiner samt att kommunen till stor del försöker automatisera processer och låta externa leverantörer sköta drift och övervakning av kritiska verksamhetssystem

Nedan följer våra bedömningar och rekommendationer utifrån granskningens kontrollfrågor.

Finns aktuella styrande och stödjande dokument som berör IT-säkerhet och är dessa införda inom nämnderna?

- *Kommunen har tagit fram, kommunstyrelse och kommunfullmäktige har antagit IT-policy och IT-anvisningar. Det finns dock behov av att uppdatera och färdigställa rutinbeskrivningar kring avbrottsplan, katastrofplan samt bemanning. Dessa finns i dagsläget framtagna i separata dokument.*

Finns tydligt ansvar för att arbeta aktivt med frågor som berör IT-säkerhet?

- *Kommunstyrelsen i Lomma kommun har antagit säkerhetsanvisningar, innehållandes ett avsnitt kring informationssäkerhet. I anvisningarna stipuleras det att kommunens säkerhetschef ska samordna och bistå i arbetet kring informationssäkerhet. Vidare ska IT-chefen ansvara för tekniska säkerhetslösningar samt att kanslichefen ansvarar för informationshantering internt och externt samt klassificering av information.*

Finns bra rutiner för rapportering av problem och säkerhetsrelaterade händelser?

- *Kommunstyrelsen i Lomma kommun har antagit säkerhetsanvisningar, innehållandes ett avsnitt kring systematiskt säkerhetsarbete. I anvisningarna stipuleras det tydligt att identifierade hot tillsammans med inrapporterade avvikelser eller incidenter skall ligga till grund för riskanalys och därmed efterföljande beslut om eventuella insatser av olika säkerhetshöjande åtgärder.*
- *Lomma kommun har utsett en IT-säkerhetssamordnare som har ansvaret för att vara mottagare av incidentrapportering. Detta tydliggörs i IT-säkerhetshandboken, vilken tydliggör att alla medarbetare, interna som externa har ett ansvar för att rapportera inträffade säkerhetsincidenter gällandes upptäckta säkerhetsbrister till kommunens samordnare alternativt närmaste chef.*
- *Kommunens ”first line support”, vilken levereras av ATEA, ansvarar för att kunna ta emot och registrera eventuella incidenter i kommunens nya ärendehanteringssystem, Microsoft Service Manager.*
- *Kommunens IT-avdelning arbetar för närvarande med att utveckla incidentprocessen för att förbättra den support som verksamheten erbjuds genom ATEA.*
- *Ingen systematiskt uppföljning eller sammanställning av samtliga incidenter registrerade i ärendehanteringssystemet görs dock.*

Är förekomst av störningar och problem rimliga?

- *Enligt Patrik Flensburg, Servicechef i Lomma Kommun, är störningar och problem i infrastruktur och applikationer väldigt ovanliga sedan man i allt större utsträckning flyttat över kommunens verksamhetssystem till en virtualiserad serverstruktur.*
- *PwC har tagit del av en förteckning kring oplanerade systemavbrott och har observerat att det förekommit totalt sex oplanerade systemavbrott, varav hälften av dessa har inneburit systemavbrott i de mest kritiska verksamhetssystemen under 2015. Samtliga avbrott har kunnat avhjälpas inom 24 timmar.*

Finns ett tillräckligt skydd kring rum som används för datordrift för att förhindra störningar, obehörigt tillträde och stöld?

- *Ja, rum som används för datordrift har försetts med låsbara dörrar, inbrottslarm, kylaggregat samt brandskyddssystem. Vidare har kommunen i dagsläget över 95 % av hela sin drift på virtuella servrar, vilket avsevärt minskar tiden det tar att kunna återskapa och flytta över en server till annan plats vid eventuella störningar.*

Finns tillfredsställande rutiner för hantering av behörighet till gemensamt nätverk?

- *Ja, kommunen har etablerat en i princip helautomatiserad process för att hantera behörigheter till kommunens gemensamma nätverk. Behörigheterna sköts genom en anmälan, från ansvarig chef, till personalavdelningen och uppsättning av konton sker automatiserat så snart medarbetaren förts in i personalsystemet.*
- *Avseende elever vid kommunens skolor, har motsvarande process likt åtkomsthanteringen för personal etablerats.*

2016-01-18

Henrik Friang, Projektledare | *Carl-Gustaf Folkeson, Uppdragsledare*