SVALÖVS KOMMUN

Revisorerna

Kommunfullmäktige
Kommunstyrelsen

Övergripande säkerhetsgranskning av kommunens säkerhet angående externa och interna dataintrång

Svalövs kommuns revisorer har utifrån en risk- och väsentlighetsanalys beslutat att genomföra en granskning av om den interna säkerheten är ändamålsenlig när det gäller övervakning, uppföljning och beredskap av obehörigt dataintrång.

Granskningen har på vårt uppdrag genomförts av Henrik Friang från PwC. Resultatet av granskningen framgår av bilagd revisionsrapport daterad mars 2015.

Revisorerna har beslutat att översända rapporten till kommunfullmäktige för kännedom och till kommunstyrelsen för yttrande.

Svar önskas snarast.

2015-04-15

Svalövs kommuns revisorer

gm

Arne Nordqvist, ordförande

Bilaga: Övergripande säkerhetsgranskning av kommunens säkerhet angående externa och interna dataintrång, mars 2015

pwc

Svalövs kommun
Övergripande säkerhetsgranskning av kommunens säkerhet angående externa och interna dataintrång

Henrik Friang,

Säkerhetsspecialist, PwC

Mars 2015

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

Granskningen ska besvara följande revisionsfråga:

Är den interna säkerheten ändamålsenlig när det gäller övervakning, uppföljning och beredskap av obehörigt dataintrång?

Granskningen inriktas mot följande kontrollfrågor:

- Följs kommunens policys/riktlinjer för dataintrångshantering?
- Har kommunen ett ändamålsenligt arbetssätt rörande riskhantering inom IT-området?
- Är roller och ansvar i processen för risk-/dataintrångshantering inom IT-området tydligt definierade?
- Inkluderar processen effektiv kommunikation mot samtliga intressenter?
- Adresserar kommunens riskhanteringsprocess de mest väsentliga riskerna vid dataintrång?

1.3 Metod och avgränsning

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

Intervjuer har genomförts med följande personer:

- Michael Andersson, Administrativ chef med IT-ansvar
- Tom Jensen, IT-driftsansvarig

2 Observationer och påverkan

2.1 Kommer policys/riktlinjer sättas i bruk och följas? Samt kommer avsaknade policys att tas med?

Inom kommunen finns det riktlinjer och policys för IT-säkerhet. Hösten 2014 skapades det ett generellt dokument, "Informationssäkerhetspolicy", vilket planeras antas politiskt under april 2015. Dokumentet består utav tre delar; förvaltning, användare och drift. Varje del hanterar grundligt kommunens policys och riktlinjer avseende samtliga IT-säkerhetsområden. Då policydokumentet fortfarande är i en utvecklingsfas behandlar dokumentet områden och roller som inte fastställt ännu eller har förändrats, varför dokumentet kräver ytterligare uppdatering.

Svalövs kommun har etablerat majoriteten av de formaliserade rutiner och processer, för att säkerställa åtkomsthantering, intrångshantering och drift, som krävs för att säkerställa god intern kontroll. Det finns dock behov av att ytterligare komplettera och utveckla rutinbeskrivningar för att säkerställa god intern kontroll. Vidare bör samtliga rutiner uppdateras kontinuerligt.

Systemsäkerhetsanalyser finns etablerade för samtliga system. Dessa analyser omfattar förteckningar över systemen, med satta prioriteringar, vilka beroenden som finns samt en återställningsplan.

Sedan ett år tillbaka har en även säkerhetsgrupp tagits fram som kallas "Team Risk". Gruppen består av samtliga sektorchefer plus en medarbetare från varje sektor. Möten hålls varannan månad, där IT-frågor utifrån en riskbaserad ansats hanteras.

2.2 Har kommunen ett ändamålsenligt arbetssätt rörande riskhantering inom IT-området?

En process för skapande av konto för nya användare, ändring av behörighet samt avslutande av konto är etablerad. Detta sker genom specifika formulär på intranätet som fylls i av ansvarig chef, sedan skickas vidare till ärendehanteringssystemet samt systemförvaltare. Dock har det framkommit i intervjuer att vid avslutande av konton, förekommer det att ansvarig chef ej använder avsett formulär, vilket leder till att konton som tillhör inaktiva användare inte avaktiveras.

Det finns en fastställd rutin för borttagning av inaktiva konton, där man kvartalsvis tar ut en rapport över användare som ej varit aktiva under en viss tid. Inaktiva användare som fångats upp i rapporten följs upp med ansvarig chef för att fastställa anledning till inaktivitet, så som föräldraledighet eller uppsägning, innan kontot avaktiveras.

Det genomförs, åtminstone vad de intervjuade känner till, ingen regelbunden genomgång av behörigheter för att säkerställa att en användare har rätt behörigheter för sin roll i samtliga verksamhetssystem. Det bör beaktas att ansvaret för säkerställandet ligger hos respektive systemförvaltare.

2.3 Är roller och ansvar i processen för risk-/dataintrångshantering inom IT-området tydligt definierade?

Ansvaret för IT-säkerhet och integritetsskydd finns tydligt definierat i kommunens IT-säkerhetspolicy. Säkerhetspolicyn kommer, som nämnt tidigare, att formellt antas under april 2015.

Det har vid intervjuer framkommit att ett individberoende existerar inom kommunen, avseende kunskap och ansvar för IT-säkerheten. Detta beror bland annat på att IT-avdelningen är relativt liten, vilket innebär att fåtal anställda innehar omfattande kunskap avseende IT-miljön. Kommunen arbetar dock aktivt för att främja spridandet av kunskap genom bland annat omfattande dokumentation i en intern wiki, ansvar för arbetsuppgifter i grupp (tjänsternas driftansvarig respektive systemtekniker) samt anlitande av konsulttjänster för vissa tekniskt komplicerade installationer och uppgraderingar.

2.4 Inkluderar processen effektiv kommunikation mot samtliga intressenter?

IT-personalen har tillgång till all dokumentation rörande IT och säkerhet. Användare har tillgång till väsentlig dokumentation via intranätet. Kommunen har även nyligen börjat erbjuda arbetar även kontinuerligt med utbildning för nyanställda, för att öka kunskapen avseende IT-säkerhet.

2.5 Adresserar kommunens riskhanteringsprocess de mest väsentliga riskerna vid dataintrång?

Kommunen har en organisation och struktur i sitt arbete som adresserar merparten av aktuella säkerhetsfrågor.

Avseende fysisk säkerhet har man etablerat en ändamålsenlig hantering, med lämpliga skalskydd och larm. Kommunen har etablerat en kontinuerlig patchningsprocess, för att säkerställa att IT-miljön uppdateras till en tillfredsställande säkerhetsnivå.

I IT-säkerhetpolicyn har kommunen satt upp utförliga riktlinjer avseende lösenord och åtkomst, vilket minkar risken markant för intrångsförsök.

För att minska risker vid fjärråtkomst använder man sig utav VPN. Kommunen använder sig även av programmet *Novell Filr* vilket speglar användarens hemmapp samt ger dem möjligheten att dela mappar och filer med andra. *Novell Filr* är tillgängligt både via datorer, surfplattor och smartphones oberoende av klientoperativ. Tillgång till programmet kräver användarnamn och lösenord och endast anställda (ej elever) har tillgång till programmet.

Det finns ingen formaliserad rutin kring säkerhetskrav på leverantörer vid upphandling av system. Dock är IT-ansvariga oftast med vid upphandlingar, för att adressera säkerhetsfrågor. Här bör en formell process övervägas, där IT-säkerhet tas med i avtal och följs upp kontinuerligt.

3 Revisionell bedömning och rekommendationer

Granskningens revisionsfråga: *Är Svalövs kommuns interna IT-säkerhet ändamålsenlig när det gäller övervakning, uppföljning och beredskap av obehörigt dataintrång?*

Efter granskning av kontrollfrågorna bedömer vi att kontrollen över den interna säkerheten finns etablerat för flertalet säkerhetsdomäner, dock inte fullt ut och ändamålsenlig för samtliga områden. Det finns utrymme till förbättringsinsatser för att öka transparensen samt för att säkerställa kontinuitet.

Vår granskning har visat att vissa av de informella processerna idag fungerar för kommunen, men har en hög grad av individberoende. Individoberoendet bör fortsätta utvecklas framgent, genom att ytterligare öka nivån av dokumentation.

Nedan följer våra bedömningar och rekommendationer utifrån granskningens kontrollfrågor.

Följs kommunens policys/riktlinjer för dataintrångshantering?

- *IT-avdelningen bör utveckla och etablera en formaliserad incidentprocess för dataintrång.*

Har kommunen ett ändamålsenligt arbetssätt rörande riskhantering inom IT-området?

- *IT-avdelningen tillsammans med verksamheterna (systemägare) bör vidareutveckla sin process för åtkomsthantering, för att säkerställa att rättigheter i systemet speglar de anställdas arbetsuppgifter.*

Är roller och ansvar i processen för risk-/dataintrångshantering inom IT-området tydligt definierade?

- *IT-avdelningen bör fortstätta att genomföra regelbundna sårbarhetsanalyser, för att på så sätt, säkerställa att en hög IT-säkerhetsnivå i kommunen.*
- *Sårbarhetsanalyser bör genomföras både på interna och externa IT-miljöer samt på de applikationer som hanterar känslig information, som till exempel lönesystem.*

Inkluderar processen effektiv kommunikation mot samtliga intressenter?

- *Processerna för IT och verksamheten bör ytterligare formaliseras för att säkerställa att säkerhetsfrågor adresseras i samband med upphandling av verksamhetssystem.*

Adresserar kommunens riskhanteringsprocess de mest väsentliga riskerna vid dataintrång?

- *IT-avdelningen adresserar de mest väsentliga riskerna. Dock bör IT-avdelningen ytterligare formalisera sina rutiner för att säkerställa kontinuitet i arbetet.*

2015-03-12

Henrik Friang, Projektledare

Alf Wahlgren, Uppdragsledare