Södertörns brandförsvarsförbund
Revisionen

Revisionsskrivelse
2017-12-11

Förbundsdirektionen

Granskning av IT-verksamheten

På vårt uppdrag har PwC genomfört en granskning av förbundets IT-miljö, IT-organisation och IT-säkerhet.

Vår sammanfattande bedömning utifrån granskningen är att förbundet endast delvis har säkerställt att man har en god IT-miljö och att IT-organisationen arbetar systematiskt med IT-säkerheten och att det inom ett flertal områden behöver vidtas åtgärder i syfte att stärka förbundets IT-verksamhet. Mot bakgrund av detta lämnar vi följande rekommendationer, att:

- utöka IT-funktionen med teknisk samt strategisk kompetens.
- upprätta en IT-strategi på ledningsnivå. Tilldela systemägarskap och samordna IT över hela verksamheten.
- upprätta styrande dokumentation för informationssäkerhet. Denna bör bland annat reglera behörighetshantering, uppdatering av hårdvara samt lösenordsuppbyggnad.
- tillse att styrande dokument fastställs av IT-chef och ledning. Det bör också säkerställas att dokument finns att tillgå även då dokumenthanteringssystemet är otillgängligt.
- utbilda de anställda inom IT överlag och även inom IT- och informationssäkerhet.
- införa kontroller och övervakning av nätverket samt begränsning av vilken hårdvara som kan kopplas upp mot detta.
- utvärdera till vilken nivå telefonväxeln är redundant och vidta nödvändiga åtgärder baserat på resultatet.

Vi önskar få en skriftlig redovisning av vilka åtgärder som förbundsdirektionen kommer att vidta med anledning av vår skrivelse. Svaret på denna skrivelse planeras att följas upp och diskuteras i samband med slutrevisionen för 2017, dvs i mars 2018.

För förbundets revisorer

Bengt Verlestam

www.pwc.se

Granskning av räddningstjänstens IT-verksamhet

Södertörns Brandförsvarsförbund
December 2017

Författare:

Niklas Ljung, projektledare

Ida Ek, utredare

pwc

1. Bakgrund och syfte

Bakgrund och syfte

Revisorerna har uppmärksammat att risker och hot från det framväxande digitala landskapet, cyberrisker, får ökande uppmärksamhet från både företag och myndigheter. Detta främst orsakat av de senaste årens snabba digitala utveckling med följande exponering mot internet samt ökad användning av smartphones och andra bärbara enheter hos medarbetare, både privat och i yrkeslivet. Ökad aktivitet bland kriminella och andra antagonistiska aktörer bidrar också starkt till den växande hotbilden.

Man har från såväl näringsliv som offentlig sektor insett att den hot- och riskbild som växer fram behöver tolkas och göras begriplig så att relevanta och balanserade motåtgärder kan vidtas. I grund och botten handlar det om behovet att skydda sig mot angripare som oavbrutet arbetar för att hitta nya vägar att stjäla, förstöra eller på annat sätt manipulera informationstillgångar eller informationsinfrastruktur.

Revisorerna har i sin riskanalys för 2017 bedömt att det finns en risk att Södertörns brandförsvarsförbund inte har säkerställt att den tekniska IT- säkerheten är tillfredsställande och att IT-organisationen inte arbetar optimalt. Syftet med denna granskning har varit att utreda huruvida detta är fallet eller ej.

2. Revisionsfråga, kontrollfrågor och revisionskriterier

Revisionsfråga

- Har ledningen för Södertörns Brandförsvarsförbund säkerställt att man har en god IT-miljö och att IT-organisationen arbetar systematiskt med IT-säkerheten?

Kontrollmål

1. Finns det en väl optimerad och fungerande IT-organisation?
2. Finns de styrande IT dokument som organisationen behöver, och är dessa kontinuerligt reviderade?
3. Finns det en god behörighetshantering?
4. Bedriver IT-organisationen ett aktivt IT säkerhetsarbete för att minska risken för intrång?
5. Arbetar IT-organisationen kontinuerligt och strukturerat med att hålla all teknisk hårdvara uppdaterad?

Revisionskriterier

- Skyddslag (2010:305)
- Säkerhetsskyddslag (1996:627)
- Offentlighets- och sekretesslag (2009:400)
- IT-styrdokument

3. Avgränsning och granskningsmetod samt genomförande

Avgränsning

Granskningen omfattar IT-organisationen.

Granskningsmetod och genomförande

Inom ramen för uppdraget har fyra kvalitativa intervjuer utförts tillsammans med medarbetare hos förbundet. Dessa inkluderade utöver IT-personal och chefer med IT-ansvar en representant för brandmännen samt administrativ personal. Utöver intervjuerna har viss dokumentation erhållits vilken har granskats.

Granskningen har utöver svar på revisionsfråga och kontrollmål resulterat i ett antal rekommendationer för förbundets räkning.

4. Granskningsresultat – svar på kontrollmålen

Kontrollmål 1 - Finns det en väl optimerad och fungerande IT-organisation.

- Vi bedömer kontrollmålet som **ej** uppfyllt.

Förbundets IT-organisation består av endast en person i dagsläget (1 konsult kommer att tas in på ett längre uppdrag), medan andra liknande verksamheter har IT-organisationer bestående av åtminstone 2-3 personer. Denna resursbrist innebär att strategiska IT-frågor nedprioriteras, samt att det uppstår ett stort personberoende. Bedömningen är även att frågorna nedprioriteras från ledningsnivå då det råder en viss oförståelse gällande vikten av en väl fungerande IT-organisation.

Kontrollmål 2 - Finns de styrande IT dokument som organisationen behöver, och är dessa kontinuerligt reviderade.

- Vi bedömer kontrollmålet som **ej** uppfyllt.

Förbundet har ingen fastställd IT strategi, och inte heller någon styrande dokumentation för informations- och IT-säkerhet. Dessa dokument behövs för att kunna sätta riktningen för IT samt för att formellt reglera arbetet med informations- och IT-säkerhet inom verksamheten.

Det finns en del dokumentation på förbundets portal/sharepoint. Dessa är dock ej strukturerade dokument så som rutiner, riktlinjer och policys. Det finns ingen fastställd ägare av dokumentationen, ingen versionsnumrering och ingen versionshistorik.

Kontrollmål 3 - Finns en god behörighetshantering.

- Vi bedömer kontrollmålet som **delvis** uppfyllt.

Förbundet tilldelar en anställd dess behörigheter baserat på dennes roll, stationering och arbetsuppgift - vilket anses vara en god rutin då det tillser att personen får tillgång till endast det som denne behöver för att utföra sitt arbete.

Det finns dock ingen fastställd rutin för upprättande, ändring och borttagande av konton och rättigheter. Översyn av befintliga behörigheter sker informellt och ostrukturerat.

Kontrollmål 4 - Bedriver IT-organisationen ett aktivt IT säkerhetsarbete för att minska risken för intrång.

- Vi bedömer kontrollmålet som **delvis** uppfyllt.

Förbundet tillser att brandväggar samt programvara mot skadlig kod uppdateras, vilket är att anse som aktivt IT-säkerhetsarbete. Dock utbildas inte personalen i IT-säkerhet, och det saknas förmåga att aktivt övervaka och därigenom upptäcka och stoppa intrång i nätverket.

Konsekvensen av kunskapsbristen har gestaltat sig genom ett antal kryptovirusincidenter på kort tid.

Kontrollmål 5 - Arbetar IT-organisationen kontinuerligt och strukturerat med att hålla all teknisk hårdvara uppdaterad.

- Vi bedömer kontrollmålet som **delvis** uppfyllt.

Uppdatering av förbundets hårdvara sker kontinuerligt, men inte strukturerat och rutinen är inte dokumenterad. Förbundet har en del hårdvara med gamla operativsystem som är tänkt att uppdateras, men det finns ingen formell plan för när och hur detta skall ske. Med resursbristen i åtanke är risken att detta nedprioriteras då det inte finns någon fastställd plan att förhålla sig till.

5. Sammanfattade bedömning och svar på revisionsfråga

Vår samlade revisionella bedömning är att Södertörns Brandförsvarsförbund delvis har säkerställt att man har en god IT-miljö och att IT-organisationen arbetar systematiskt med IT-säkerheten.

Vår bedömning är att IT-organisationen gör vad man kan med befintliga medel och att IT-miljön håller en förhållandevis god standard. Bristen på strategisk IT-kompetens är tydlig och behöver åtgärdas för att IT-organisationen skall kunna arbeta systematiskt.

Det finns ett stort personberoende och verksamheten klarar inte att nyckelpersonal är frånvarande. Det finns få personer med insikt i IT-driften som i en krissituation skulle kunna fatta de riktiga besluten.

Ledningen behöver ta fram en IT-strategi som IT-avdelningen kan följa i sitt dagliga arbete, detta för att kunna planera och ta hänsyn till i val av system m.m. för framtiden.

6. Rekommendationer

Vi rekommenderar förbundet att:

- Utöka IT-funktionen med teknisk samt strategisk kompetens.
- Upprätta en IT-strategi på ledningsnivå. Tilldela systemägarskap och samordna IT över hela verksamheten.
- Upprätta styrande dokumentation för informationssäkerhet. Denna bör bland annat reglera behörighetshantering, uppdatering av hårdvara samt lösenordsuppbyggnad.
- Tillse att styrande dokument fastställs av IT-chef och ledning. Det bör också säkerställas att dokument finns att tillgå även då dokumenthanteringssystemet är otillgängligt.
- Utbilda de anställda inom IT överlag och även inom IT- och informationssäkerhet.
- Införa kontroller och övervakning av nätverket samt begränsning av vilken hårdvara som kan kopplas upp mot detta.
- Utvärdera till vilken nivå telefonväxeln är redundant och vidta nödvändiga åtgärder baserat på resultatet.

7. Bilaga 1 – förbundets styrkor och förbättringsområden

Styrkor och förbättringsområden (1/2)

Styrkor

- En bedömning gällande vilka system som är mest kritiska för verksamheten har utförts.
- Det finns ett dokumenthanteringssystem där all teknisk dokumentation/information gällande IT samlas.
- Behörigheter tilldelas baserat på den anställdes roll.
- Det finns brandväggar och antivirus, och dessa uppdateras efter behov.
- Nätverket är segmenterat.
- Det finns en informell plan att uppgradera servrar till Windows Server 2016 samt klienter till Windows 10.
- Bra att kunna använda monitorerna för att sprida information och i syfte att utbilda personal i IT och informationssäkerhet.
- Avtal med IT-total om jour mån-fre 17-07 samt hela helgerna, vilket även kan nyttjas under semestertider och vid sjukdom.
- Bra serverpark.
- Fint och strukturerat serverrum.
- Bra med backup som kopieras till annan ort, men förbundet bör se över lösningen med att den skrivs över efter 2 dagar.
- Segmenterat nätverk.

Styrkor och förbättringsområden (2/2)

Förbättringsområden

- Det finns ett stort personberoende och verksamheten är sårbar då nyckelpersonal är frånvarande.
- IT-organisationen är spretig då olika system hanteras av olika funktioner/personer (kommunikation, telefoni, larmcentral) samt att det inte finns något systemägarskap.
- Det finns ingen IT-strategi som sätter riktningen för IT inom organisationen. Det finns inte heller någon formell dokumentation som reglerar IT- och informationssäkerhet.
- Det finns inget krav som reglerar lösenordsuppbyggnad.
- Kunskapen gällande IT är generelt låg bland anställda. Detta medför att kunskapen gällande informations- och IT-säkerhet är bristfällig, vilket har gestaltat sig genom ett antal kryptovirus-incidenter.
- Behörigheter tilldelas, ändras, avvecklas och utvärderas ej enligt någon systematisk och dokumenterad rutin.
- Konsulterna från IT-Total uppdaterar brandväggar och switchar löpande (7-8 gånger år), men det finns ingen skriftlig rutin för detta vilket innebär att förbundet har en begränsad insyn i hur deras miljö hanteras.
- Det råder delade meningar gällande huruvida telefonväxeln är redundant (finns det en backup om växeln blir otillgänglig) eller ej.
- Det saknas en komplett systemkarta över nätverket.
- Förbundet prenumererar inte på något utskick som hjälper dem hålla sig uppdaterade gällande vad som händer i omvärlden (exempelvis från cert-se)

2017 – 12 – 11

Richard Vahul

Uppdragsledare

Niklas Ljung

Projektledare