Mjölby kommun

Mjölby Kommun

Granskning av intern IT-säkerhet

Juni 2017

pwc

1. Bakgrund och syfte

Bakgrund och syfte

Av kommunallagen och god revisionssed följer att revisorerna årligen ska granska styrelser, nämnder och fasta fullmäktigeberedningar.

Kommunstyrelse och facknämnder ska förvalta och genomföra verksamheten i enlighet med fullmäktiges uppdrag, lagar och föreskrifter. För att fullgöra uppdraget måste respektive organ bygga upp system och verktyg för ledning, styrning, uppföljning, kontroll och rapportering samt säkerställa att dessa verktyg tillämpas på avsett sätt. En bristfällig styrning och kontroll kan riskera att verksamheten inte bedrivs och utvecklas på avsett sätt.

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 kommunstyrelsen inte har säkerställt att den interna tekniska IT-säkerheten är tillfredsställande och har därför gett PwC ett uppdrag att granska området.

2. Syfte och revisionsfråga

Syfte och revisionsfråga

Har kommunstyrelsen säkerställt att Mjölby kommuns nuvarande tekniska IT-säkerhet är tillräcklig och tillfredsställande för att reducera risker för obehörigt intrång till en acceptabel nivå?

Kontrollfrågor

Hur upptäcks en eventuell attack och hanteras icke önskvärda incidenter på ett ändamålsenligt sätt?

Hur är säkerheten avseende intrång av extern och intern aktör?

Finns det styrande dokument, såsom policy och riktlinjer för IT-säkerhet?

Är befintlig dokumentation uppdaterad och reviderad?

3. Granskningsmetod

Intern och extern penetrationstest

En teknisk säkerhetsgranskning är ett sätt att testa IT-säkerheten genom att utföra realistiska attacker mot verkliga system.

För att uppnå hög kvalitet och effektivitet i arbetet, arbetar PwC med scenarion för olika typer av realistiska tester. Ett scenario innehåller hot, tillvägagångssätt och mål.

Scenario 1 – Intern teknisk säkerhetsgranskning

En person utan behörighet till Mjölby kommuns IT-system får fysisk tillgång till det interna nätverket. Personen kartlägger nätverket och attackerar viktiga interna system. Målet är att få tillgång till och kunna ändra information, alternativt att störa systemens tillgänglighet.

Scenario 2 – Externa tester via Internet

En extern hacker, utan djupare kunskaper om Mjölby kommun, kartlägger organisationens närvaro på Internet. Målet är att bryta sig in i intressanta system exponerade mot Internet.

Genomförande

Omfattning

Testerna genomförs utan förkunskap om hur miljön ser ut (så kallad black box testning).

Informationsinsamling

Ett flertal verktyg användes inledningsvis för att kartlägga resurser på Mjölby kommuns nätverk. Samtliga resurser som omfattades av testerna kartlades och identifierades.

Dessutom samlades information in från publika källor, så som kommunens hemsida, för att bistå vid de senare intrångsförsöken.

Intrångsförsök

Intrångsförsök gjordes för att påvisa att de potentiella säkerhetsbristerna som identifierades under informationsinsamlingen var reella sårbarheter.

Dokumentgranskning

Genom att begära tillgång till IT-relaterade styrdokument får PwC en bild av vad som finns.

PwC genomför en övergripande genomgång av tillgänglig dokumentation för att få en uppfattning om dokumentationen är uppdaterad och löpande revideras enligt god praxis.

4. Resultat av penetrationstesten

Intern och extern penetrationstest

Intrångsförsök genomfördes och sårbarheter identifierades under båda den interna och den externa penetrationstesten.

Vid test av den externt exponerade delen av IT-miljön identifierades webbapplikationer med svag autentisering. En av dessa visade sig använda *Active Directory* (AD) för inloggning. Den svaga autentiseringen i kombination med den externa exponeringen samt att det saknas utelåsningsmekanismer möjliggjorde att PwC kunde genomföra en lösenordsattack och på så sätt gissa till sig användarnamn och lösenord för flera konton.

Vid test av den interna miljön saknas det skydd för begränsning av nätverksåtkomst. Bristfällig nätverkssegmentering gjorde att PwC utan svårigheter kunde nå kommunens olika IT-resurser. Trots att en stor mängd loggar bör ha genererats i övervakningsverktyg, vilket bör ha orsakat larm om att en intern attack pågick, såg PwC inga tecken på respons från IT-avdelningen.

Intern och extern penetrationstest (forts.)

Resultatet av penetrationstesten resulterade i ett antal sårbarheter:

- Hög risk - 19 st., varav en fanns i 10 system
- Medel risk - 2 st., varav en fanns i 4 system
- Låg risk - 2 st.
- Information - 2 st.

Se bilaga 1 för närmare förklaring och riskgradering.

Intern och extern penetrationstest (forts.)

Exempel på sårbarheter:

Nätverksåtkomst. Personal från PwC kunde enkelt koppla in utrustning på nätverket utan att någon skyddsmekanism identifierades. Utrustningen fick IP-adress och kunde nå interna resurser obehindrat.

Lokal Admin. Personal från PwC kunde enkelt bli lokal administratör på en klient-PC då denna saknade hårddiskkryptering. Genom att starta upp datorn på alternativt media och ändå ha full access till hårddisken kunde man skapa en egen lokal administratör

Wannacry. Genom att angripa servern x.x.x.x kunde PwC få fjärråtkomst som localsystem med en MeterPreter-session, varpå man kunde skapa ett lokalt administratörskonto och logga på maskinen med Remote Desktop.

Antivirus. Efter att PwC fått fjärråtkomst med en MeterPreter-session kunde PwC ladda mimikatz-moduler för att läsa ut lösenord från befintligt påloggade administratörer.

Intern och extern penetrationstest (forts.)

Återanvändning av lösenord. Genom att extrahera den lokala administratörens lösenordshash kunde PwC genomföra en pass-the-hash-inloggning mot andra servrar som hade samma lokala administratörslösenord.

Lösenordsgissning. PwC kunde gissa sig till lösenordet till 60 konton på ett fåtal försök genom att göra testpåloggningar mot Exchange Web Service. Denna typ av lösenordsgissning är även exponerad till Internet, vilket möjliggör för en angripare att genomföra attacken från Internet.

Vmware. Under kartläggningen identifierades vSphere-servern, och med hjälp av de behörigheter PwC anskaffat sig i tidigare intrångsförsök kunde man ansluta till denna.

Detaljerat resultat och rekommendationer om penetrationstesten finns i den sekretessbelagda rapporten som har överlämnas direkt till IT-avdelningen.

Intern och extern penetrationstest (forts.)

Det finns ett antal åtgärder som kan genomföras för att höja den totala säkerheten till en högre nivå.

Med tanke på de påträffade sårbarheterna ser det ut att finnas ett stort behov av att identifiera och hantera kommunens resurser så att man kan få en överblick av miljön och identifiera sårbarheter. PwC rekommenderar att man ser över rutiner för patchning av servrar och klienter så att det till stor del sker automatiskt samt ger rapporter med jämna intervaller så att man kan identifiera avvikelser. Detta omfattar även att hantera 3:e parts produkter så att även dessa får säkerhetsuppdateringar. En god rutin är att man internt med jämna mellanrum genomför en sårbarhetsanalys på sina resurser.

Då PwC ej påträffade någon reaktion från IT-säkerhetsavdelningen tyder det på att det saknas förmåga att identifiera och reagera på attacker såväl internt som externt. PwC rekommenderar därför att man ser över hur man hanterar loggar. PwC rekommenderar att man samlar loggar centralt där de enkelt kan analyseras, från detta kan även automatiskt larm konfigureras när loggarna avviker från de normala.

Intern och extern penetrationstest (forts.)

Utökad segmentering av nätverk, möjligheten att kommunicera mellan dem, skulle förhindra en angripare från att enkelt nå kritiska resurser. Angreppskomplexiteten som skulle krävas för att utföra intrången i denna rapport skulle öka avsevärt samtidigt som det skulle bli svårare att undvika detektering.

Exempelvis bör inte användarnas klientdatorer kunna nå vilka servrar som helst. Endast de nödvändigaste portarna och resurserna bör vara tillgängliga till serversegment. Det finns till exempel sällan en god anledning till att ge användare möjligheten att ansluta till Domänkontrollanten (DC) med Remote Desktop (RDP) port TCP 3389, eller att direkt ansluta till databasservrar (SQL) på port TCP 1433.

PwC rekommenderar att man implementerar lösningar för att detektera avvikande användarbeteende. Detta för att kunna identifiera när ett användarkonto används i ett skadligt syfte. Exempel på tillfällen då en sådan mekanism skulle kunna varna administratörer kan vara då användare loggar in från okända IP-adresser vid avvikande tider eller när de ansluter till andra resurser än vanligt. Det finns även möjlighet att identifiera när en pass-the-hash-attack utförs vilket idag är en vanligt förekommande attack vid angrepp mot liknande miljöer.

5. Resultat av dokumentgranskningen

Resultat av dokumentgranskningen

I samband med granskningen av dokumentationen har PwC haft samtal med berörda parter i IT-organisationen och det har framkommit att:

- Mjölby kommuns IT-organisation har haft flera tunga år och har mycket att få ordning på.
- IT-organisationens nuläge är en ny CIO som tillsammans med sina 2 närmaste chefer (drift och support) agerar för att komma till ett önskat läge med en tydlighet och adekvat struktur för en optimal IT-avdelning. En personalpolitik som utvecklar medarbetare och verksamheten.
- Första steget har varit att tydliggöra roller och utmaningar samt krav. Nästa fas (nuläge) är att implementera ett ramverk för att leverera IT-tjänster (en variant av ITIL) där det blir mer naturligt och ett större behov i att skapa nödvändig dokumentation, processer, topologiska kartor osv.

Resultat av dokumentgranskningen (forts.)

Efter granskningen av den dokumentation som PwC har fått ta del av är PwC:s bedömning att Mjölby kommuns IT-relaterade dokument håller en tillräckligt hög nivå.

Dock saknas mycket dokumentation som behöver skapas för att dokumentationen ska vara den trygghet som en verksamhet behöver.

Arbetet med att ta fram saknad dokumentation samt hålla den befintliga dokumentationen uppdaterad och reviderad ska inte nedprioriteras.

Det är dock viktigt att man genomför detta arbete på ett strukturerat sätt och följer någon typ att standard t ex ITIL.

IT-utvecklingen går i dag fort framåt och system och tjänster ändras ständigt. Det är därför viktigt att dokumentationen löpande revideras.

PwC:s rekommendation är att man reviderar dokumentationen var tolfte månad.

Resultat av dokumentgranskningen (forts.)

Revideras dokumentationen regelbundet går det oftast relativt fort, eftersom det då inte rör sig om särskilt omfattande förändringar.

PwC rekommenderar också att man inför versionshistorik på dokumentationen för att kunna följa när och av vem dokumenten reviderades.

PwC:s bedömning är att IT-organisationen är på rätt väg och att man bör ge dem tid att komma till rätta på ett strukturerat sätt.

Dock är PwC:s rekommendation att man gör en återkommande kontroll över dokumentationsläget om ett år.

Se bilaga 2 för förslag till genomgång av informationshantering och uppdatering av dokumentation.

6. Bilaga 1

Riskgradering

Gradering	Beskrivning
Hög	En sårbarhet med hög risk är något man bör åtgärda omedelbart. Dessa sårbarheter är relativt lätta för en angripare att utnyttja och kan förse denne med full access till de berörda systemen.
Medel	En sårbarhet med medel risk är oftast svårare att utnyttja och ger inte samma tillgång till det drabbade systemet.
Låg	En sårbarhet med låg risk ger ofta information till en angripare som kan hjälpa denne i kartläggningen inför en attack. Dessa bör åtgärdas i mån av tid, men är inte lika kritiska som övriga brister.
Information	En teknisk eller administrativ brist som bör åtgärdas, eller ett förslag på förbättring.

7. Bilaga 2

Förslag till genomgång av informationshantering och uppdatering av dokumentation

2. Skapa övergripande standard för organisationens informationshantering

Standarden beskriver vad olika dokumenttyper ska innehålla, exempelvis:

- Versionshantering
- Dokumentansvar
- Revisonscykel

3. Processbeskrivning för hur dokumentation ska skapas, underhållas och avvecklas

Inom respektive ansvarsområde upprättas de rutiner som är nödvändiga för att leva upp till organisationens krav. Exempelvis hur kvalitetsgranskning skall utföras eller hur fastställande av dokument av olika typer utförs.

4. Säkerställ en god struktur

Struktur för dokumentation och information måste vara lättöverskådlig och lätt att hitta i även som nyanställd.

5. Inventering av befintlig information

Skapa en lista på vilken dokumentation som saknas samt vem som är ansvarig för att ta fram informationen.

Gör en prioritering!

1. Identifiera ägaransvar för samtlig information

Klargöra vem, dvs, vilken roll som är ansvarig för vilken dokumentation. Exempelvis IT-chef, tekniker och informationssäkerhetsansvarig.

6. Tidplan

Sätta en tidplan utifrån prioritering, när dokumentationen bör vara uppdaterad och reviderad.

7. Påbörja uppdatering/ revidering

Påbörja det faktiska arbetet med att uppdatera informationen

8. Klassning av dokument

Fastställ informationsklass, besluta om revisionscykelns intervall och ev. granskningsförfarande, etc.

11. Projektavslut

Avsluta projekt och överlämning till linjen.

10. Fastställande

Fastställ den information som kräver detta.

9. Granskningsförfarande

Granskning och second opinion på producerad och reviderad dokumentation.

8. Kontaktuppgifter

Kontaktuppgifter

Niklas Ljung
Projektledare
niklas.ljung@pwc.com
0701 96 03 69

Ronald Binnerstedt
Penetrationstestare
ronald.binnerstedt@pwc.com
0766 37 61 20