Revisionsrapport

Cyber security
Intrångsgranskning

Danderyds kommun

Niklas Ljung

Ronald Binnerstedt

Augusti 2017

pwc

Sammafattande slutsatser med revisionella bedömningar

Revisorerna har i sin riskanalys för 2017 bedömt att det finns en risk att kommunstyrelsen inte har säkerställt att den tekniska IT-säkerheten är tillfredsställande gällande obehörigt intrång och har därför gett PwC ett uppdrag att granska området.

Vår metod var att genom en extern penetrationstest gick vi igenom Danderyds kommuns tekniska miljö och identifierade eventuella brister. Testerna utfördes från utsidan. Vi genomförde även en övergripande genomgång av tillgänglig dokumentation för att få en uppfattning om dokumentationen var uppdaterad och löpande revideras enligt god praxis.

Vår revisionsfråga var om kommunstyrelsen har säkerställt att Danderyds kommuns nuvarande tekniska IT-säkerhet är tillräcklig för att reducera risker för obehörigt intrång till en acceptabel nivå?

Efter genomförd granskning är vår bedömning att kommunstyrelsen säkerställt att den externa säkerheten hos Danderyds kommun var god när vi utförde testerna. De sårbarheter som upptäcktes var av generell karaktär och vi bedömer även att dessa kan åtgärdas med enkla medel.

Vi bedömer dock att kommunstyrelsen behöver säkerställa en inventering av dokumentationen, en uppdatering av samtlig dokumentation och att all dokumentation åtminstone innehåller ägare, versionsnummer och versionshistorik. Vi bedömer vidare att kommunstyrelsen behöver säkerställa att den dokumentation som i dag saknas skapas.

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 avsätt 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 tekniska IT-säkerheten är tillfredsställande gällande obehörigt intrång och har därför gett PwC ett uppdrag att granska området.

2. Syfte och revisionsfråga

Syfte och revisionsfråga

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

Kontrollfrågor

- Upptäcks en eventuell attack och hanteras den av IT-personalen på ett rimligt tillvägagångssätt?

- Har Danderyds kommun externa säkerhetsåtgärder som förhindrar eventuella angripare att ”enkelt” få åtkomst till kritisk information utifrån (via Internet)?

Dokumentgenomgång

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

- Är befintlig dokumentation uppdaterad och löpande reviderad enligt god praxis?

3. Granskningsmetod

Extern penetrationstest

Genom en extern penetrationstest gick vi igenom Danderyds kommuns tekniska miljö och identifierade eventuella brister.

Testerna utfördes från utsidan.

Scenario – Externa tester via Internet

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

Genomförande

Informationsinsamling

Ett flertal verktyg användes inledningsvis för att kartlägga resurser på Danderyds 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 identifierade under informationsinsamlingen var reella sårbarheter.

Intrångsförsöket genomfördes med minimal inblandning av driftspersonal hos Danderyds kommun.

Dokumentgranskning

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

Vi genomförde en övergripande genomgång av tillgänglig dokumentation för att få en uppfattning om dokumentationen var uppdaterad och löpande revideras enligt god praxis.

4. Resultat av penetrationstesten

Extern penetrationstest

Under granskningen identifierades 8 sårbarheter/ konfigurationsbrister.
5 var av typen *medel* och 3 av typen *information* (se bilaga 1).

Generellt kan det sägas att de mer allvarliga sårbarheter som har lokaliserats riskerar att utsätta användarna för angrepp, snarare än Danderyds kommun själva.

Exempel på detta är kommunens hemsida www.danderyd.se som är sårbar när det gäller cross-site-scripting (XSS) samt clickjacking.

Extern penetrationstest (forts.)

PwC har även lokaliserat en undersida till www.danderyd.se som producerar ett detaljerat felmeddelande där den fysiska sökvägen på servern avslöjas.

Detta kan ge en potentiell angripare information om serverns filstruktur samt uppbyggnad, vilket skulle kunna användas i ett led till att angripa servern.

PwC lyckades med framgång utnyttja den lokaliserade cross-site-scripting (XSS) sårbarheten genom att förmå www.danderyd.se att svara på ett harmlöst javascript.

Utöver detta lyckades man trots en rad lokaliserade sårbarheter inte utnyttja dessa för att penetrera något system eller tjänst.

Extern penetrationstest (forts.)

Vi bedömer att den externa säkerheten hos Danderyds kommun var god när vi utförde testerna.

De sårbarheter som upptäcktes var av generell karaktär och vi bedömer även att dessa kan åtgärdas med enkla medel.

Det är dock av stor vikt att dessa åtgärdas snarast, då de i kombination samt över tid kan utvecklas till kritiska sårbarheter.

5. Resultat av dokumentgranskningen

Resultat av dokumentgranskningen

Efter granskningen av den dokumentation som vi har fått ta del av är vår bedömning att Danderyds kommuns IT-relaterade dokument ej håller en tillräckligt hög nivå.

Det saknas, eller så har vi inte fått ta del av, en mängd viktiga styrdokument och dokument som ska användas i samband med en kris eller incident. Exempel på dokument som saknas är:

- IT-strategi
- IT-plan
- Backuppolicy/plan
- Disaster recovery-plan
- Incidenthanteringsplan
- Policy/riktlinje för nätverksövervakning

Resultat av dokumentgranskningen (forts.)

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

Vår rekommendation är att man bör revidera all sin dokumentation var tolfte månad, men åtminstone var tjugofjärde månad för dokumentation som är relativt statisk.

Mycket av Danderyds kommuns dokumentation har inte reviderats på ca tjugo månader, men stora mängder är äldre än så.

Till exempel har ”riktlinjer-for-informationssakerhet” och ”systemforvaltningsmodell” inte reviderats på fyra år.

Dokumentation är bara till nytta om den är riktig.

Revideras dokumentationen regelbundet går det oftast relativt fort, eftersom det då inte rör sig om särskilt omfattande förändringar. Dessutom får Danderyds kommun då dokumentation som är tillförlitlig.

Resultat av dokumentgranskningen (forts.)

Det är viktigt att man på ett enkelt vis kan se vem som är ägare/ansvarig för ett dokument och när det senast reviderades.

Danderyds kommuns IT-dokument saknar:

- Dokumentägare/ansvarig
- Versionsnummer
- Versionshistorik

Vi bedömer att kommunstyrelsen behöver säkerställa en inventering av dokumentationen, en uppdatering av samtlig dokumentation och att all dokumentation åtminstone innehåller ägare, versionsnummer och versionshistorik. Vi bedömer vidare att kommunstyrelsen behöver säkerställa att den dokumentation som i dag saknas skapas.

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.