www.pwc.se

Revisionsrapport

Granskning av intrångsskydd

Sandvikens kommun

Niklas Ljung
Mattias Gröndahl

December 2017

pwc

Innehållsförteckning

Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Sandvikens kommun genomfört en granskning av intrångsskydd hos Sandvikens kommun.

Revisionsfrågan som har varit styrande för granskningen har formulerats enligt följande:

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

Efter genomförd granskning är vår sammanfattande bedömning att kommunstyrelsen ***ej säkerställt*** att Sandvikens kommuns nuvarande tekniska IT-säkerhet är tillräcklig och tillfredsställande för att reducera risker för obehörigt intrång till en acceptabel nivå.

Den sammanfattande bedömningen baseras på bedömningarna av de fyra kontrollfrågorna för granskningen, vilka redovisas i rapporten. På samtliga fyra kontrollfrågor blir resultatet ej uppfyllt.

Vår bedömning är att Sandvikens kommuns IT-miljö är bristfällig, något som skyndsamt behöver förbättras. Merparten av alla IT-relaterade styrdokument saknas och jämfört med tester på andra organisationer med jämförbara IT-miljöer bedöms nivån vara under medel.

Utifrån genomförd granskning lämnas följande rekommendationer till kommunstyrelsen:

- Implementera stark autentisering för de applikationer som innehåller känslig information.
- Flera delar i domänpolicyn bör ses över, speciellt lösenordspolicyn som bör uppdateras för att minska användandet av svaga lösenord.
- Rutinen för konfiguration av servrar bör ses över så att man tar bort standardinloggningar och övrig standardkonfiguration som medför sårbarheter.
- Utökad segmentering av nätverk och begränsad möjlighet att kommunicera mellan nätverken skulle förhindra en angripare från att enkelt nå kommunens kritiska resurser.
- Implementera lösningar för att detektera avvikande användarbeteende.
- Inventering av dokumentationen bör genomföras, uppdatera samtlig dokumentation med ägare, datum, versionsnummer samt versionshistorik.
- Kommunstyrelsen bör ställa krav på IT-avdelningen vad det gäller dokumentation, samt införa återkommande kontroller för att säkerställa att dokumentationen är på plats och är återkommande reviderad.

En sekretessbelagd detaljerad rapport med resultat från genomförda intrångstester har lämnats över direkt till Sandvikens kommuns IT-chef.

1. Inledning

1.1. Granskningsbakgrund

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

Kommunstyrelse och facknämnder skall 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, s.k. 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. Granskningen har beslutats efter genomförd väsentlighets- och riskanalys och ingår i 2017 års revisionsplan.

1.2. Revisionsfråga

Granskningen syftar till att besvara följande revisionsfråga:

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

1.2.1. Kontrollfrågor

Följande kontrollfrågor har använts vid granskningen för att besvara revisionsfrågan:

- 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 löpande reviderad enligt god praxis?

1.3. Revisionskriterier

Revisionskriterierna utgörs av nedanstående:

- Kommunallagen
- Budget 2017
- IT-styrdokument

1.4. Revisionsmetod och avgränsning

Granskningen har genomförts genom intrångstester, dokumentstudier av för granskningen relevanta dokument samt en telefonintervju.

Intrångstesterna som genomfördes delades upp i två kategorier:

- Intern infrastruktur
- Extern infrastruktur exponerad mot Internet

Scenariot för de interna testerna har utgångspunkten att ett användarkonto utan särskilda behörigheter har tagits över av en illasinnad angripare. Målet är att undersöka den potentiella skadan då ett hot penetrerar IT-miljöns yttre barriärer.

Scenariot för de externa testerna har utförts som en så kallad blackbox-pentest där endast domänadress anges, all övrig information anskaffas under testernas gång.

Genom att begära tillgång till IT-relaterade styrdokument från Sandvikens kommun kunde PwC få en uppfattning om vilka dokument som fanns upprättade. Därefter genomförde PwC en övergripande genomgång av den tillgängliga dokumentationen för att bilda

sig en uppfattning om huruvida denna är uppdaterad och löpande revideras enligt god praxis.

Intervju har genomförts med:

- IT-chef på Sandvikens kommun

I tid avgränsas granskningen till år 2017 och till granskningens kontrollfrågor, samt till att intrångstesterna utförs såväl från utsidan som från insidan.

2. Resultat

2.1. Intrångstester

Intrångsförsök genomfördes och sårbarheter identifierades under både de interna och de externa intrångstesterna.

2.1.1. Interna intrångstester

Under de interna intrångstesterna påträffades ett antal sårbarheter där 9 av 10 sårbarheter hade riskgraderingen hög. Den resterande sårbarheten var av graden låg. Se bilaga 1 för närmare beskrivning och riskgradering.

Vid test av den interna miljön identifierades bl.a. avsaknad av önskvärda skyddsmekanismer för nätverksåtkomst, samt bristfällig segmentering av nätverken. Den bristfälliga nätverkssegmenteringen 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.

2.1.1.1. Exempel på interna sårbarheter

Standardinloggning
Flera tjänster hade en standardkonfiguration vilken godtar inloggning med standardanvändare och lösenord. Dessa tjänster kan bl.a. användas för att monitorera, hantera, konfigurera och upptäcka problem med nätverksutrustning, etc. En angripare som kommer åt dessa tjänster får ut väldigt mycket information om hur nätverket är uppsatt och kan dessutom exempelvis konfigurera om utrustning.

Domänpolicy
Policyn i kommunens Active Directory saknar flera konfigurationer som skulle kunna bidra till att göra miljön säkrare. Exempelvis är lösenordspolicyn mycket svag och tillåter lösenord utan krav på komplexitet.

Directory browsing på webbserver
Under testerna identifierades en webbserver som tillåter en oautentiserad användare att bläddra bland katalogerna samt få tillgång till webbserverns konfiguration.

Lösenord i minnet
Under testerna tillskansades ett konto med höga rättigheter på domänkontrollanten. NTDS-databasen kunde extraheras och knäckas off-line. På 4 timmar kunde cirka 15000 lösenord knäckas.

2.1.2. Externa intrångstester

Under de externa intrångstesterna påträffades ett antal sårbarheter där 5 av 6 sårbarheter hade riskgraderingen medel. Den resterande sårbarheten var av graden låg. Se bilaga 1 för närmare beskrivning och riskgradering.

Vid test av den externt exponerade delen av IT-miljön identifierades möjliga ingångar där en lösenordsattack kunde genomföras, detta i kombination med att lösenordspolicyn är

svag kan leda till att en angripare kan logga på användarnas konton och nå information som mail, intranät, etc.

2.1.2.1. Exempel på externa sårbarheter

Informationsläckage
En webbserver som visar data som potentiellt kan utnyttjas vid en attack identifierades.

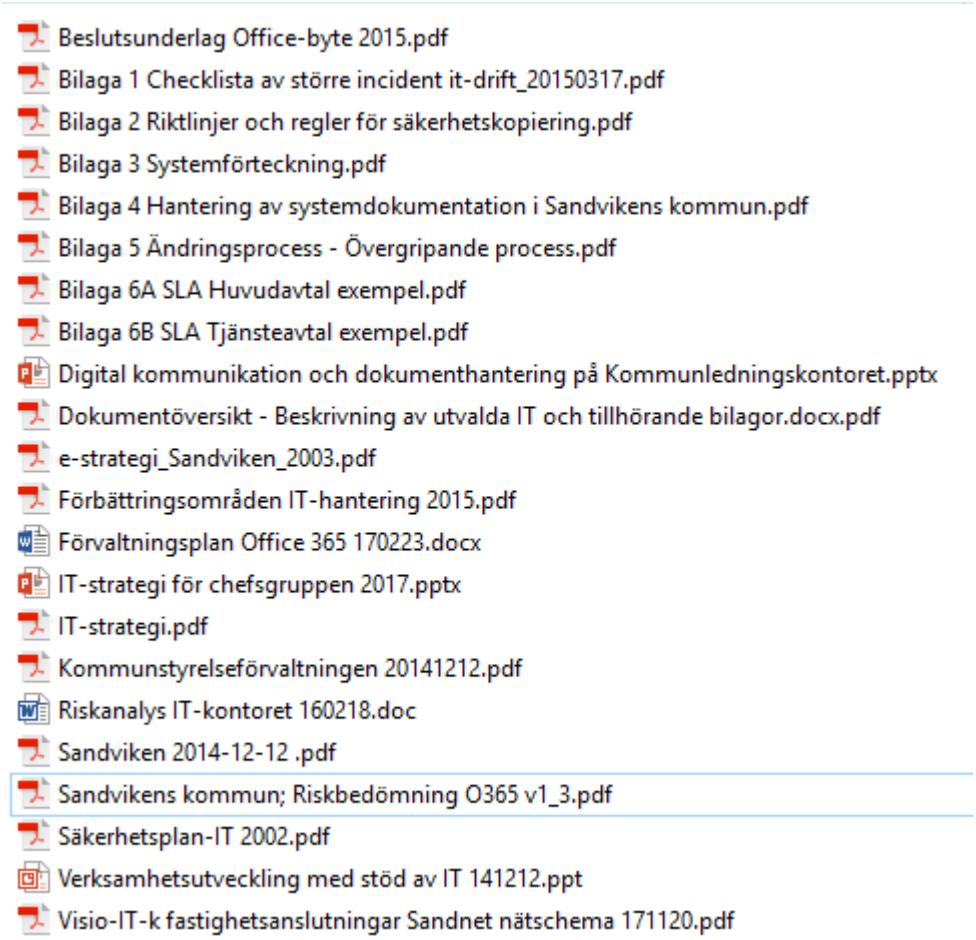
Uppräkning av användare
Portalen som används för att användarna skall kunna återställa sina lösenord går att använda för att räkna upp användare i domänen. Detta leder till att en angripare kan ta reda på om ett användarnamn är giltigt eller inte.

2.2. Dokumentgranskning

I samband med att dokumentgranskningen påbörjades hade PwC ett samtal samt genomförde en kortare telefonintervju med IT-chefen för Sandvikens kommun.

PwC informerade om att syftet med dokumentgranskningen var att se vilken dokumentation som fanns på IT-avdelningen i Sandvikens kommun samt vilket tillstånd denna var i. PwC bad att få titta på all IT-relaterad dokumentation, som exempelvis IT-policy, IT-strategi, rutiner instruktioner, kris- och katastrofplan, backupplan etc.

Under granskningens gång mottogs 22 dokument. Rubrikerna på dokumenten redovisas nedan:



Merparten av dokumentationen saknar:

- Dokumentägare/ansvarig
- Datum
- Versionsnummer
- Versionshistorik

Dokumentet med titeln *Säkerhetsplan IT för Sandvikens kommunkoncern* är daterad 2002-12-06. Desamma gäller för kommunens e-strategi. IT-utvecklingen går i dag fort framåt och system och tjänster ändras ständigt, att då ha en e-strategi från 2002 kan ses som bristfälligt.

Dokumentet *IT-strategi* daterat 2017-11-02 är det enda som kan sägas vara aktuellt och hålla en god kvalitetsnivå.

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

- IT-plan
- Disaster recovery-plan
- Backupplan
- Incidenthanteringsplan
- Policy/riktlinje för nätverksövervakning
- Drifthandbok
- Service Level Agreement (SLA)
- Rollbeskrivningar och ansvarsfördelning
- Policy och procedurer för hantering av hård- och mjukvara
- Sårbarhetsplan

PwC:s slutsats efter dokumentgranskningen är att Sandvikens IT-avdelning ej har tillgång till nödvändiga styrande dokument, regler, riktlinjer och instruktioner. Den dokumentationen som vi har tagit del av håller en bristfällig nivå. PwC rekommenderar därför att man skyndsamt skapar en handlingsplan för att komma till rätta med den bristfälliga dokumentationen.

IT-dokumentation är viktig och är en trygghet som en verksamhet behöver när det t.ex. blir personalförändringar eller driftproblem.

3. Revisionell bedömning och rekommendationer

3.1. Revisionell bedömning

Efter genomförd granskning är vår sammanfattande bedömning att kommunstyrelsen ***ej säkerställt*** att Sandvikens kommuns nuvarande tekniska IT-säkerhet är tillräcklig och tillfredsställande för att reducera risker för obehörigt intrång till en acceptabel nivå.

Vår bedömning är att Sandvikens kommuns IT-miljö är bristfällig, något som skyndsamt behöver förbättras. Merparten av alla IT-relaterade styrdokument saknas och jämfört med tester på andra organisationer med jämförbara IT-miljöer bedöms nivån vara under medel.

3.2. Bedömning utifrån kontrollfrågor

Kontrollfrågor	***Bedömning***
Upptäcks en eventuell attack och hanteras icke önskvärda incidenter på ett ändamålsenligt sätt?	**Ej uppfyllt** Trots att en stor mängd loggar bör ha genererats i övervakningsverktyg i samband med vår attack och dessa bör ha orsakat larm, dröjde det 4 dagar innan IT uppmärksammade att vårt konto hade anskaffat sig domänadministratörsrättigheter.
Hur är säkerheten avseende intrång av extern och intern aktör?	**Ej uppfyllt** PwC kunde ta över hela IT-miljön under den första dagen av de interna penetrationstesterna och undgå upptäckt under flera dagar trots att det genomfördes attacker som vanligtvis identifieras. Med de bristerna i nätverkssegmentering och låga krav på komplexa lösenord tillsammans med mycket annat bedömer vi att Sandvikens kommuns IT-miljö är bristfällig.
Finns det styrande dokument, såsom policy och riktlinjer för IT-säkerhet?	**Ej uppfyllt** Merparten av den IT-relaterade dokumentationen som bör finnas saknas.
Är befintlig dokumentation uppdaterad och löpande reviderad enligt god praxis?	**Ej uppfyllt** IT-relaterade dokument håller ej en tillräckligt hög nivå eftersom dessa ej revideras löpande, det saknas versionshistorik, datum och ansvarig/ägare.

3.3. Rekommendationer

Utifrån genomförd granskning lämnas följande rekommendationer till kommunstyrelsen.

3.3.1. Rekommendationer efter genomförda intrångstester

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

De externt publicerade delarna bör ses över och få skydd för att begränsa lösenords-gissning och utelåsning av konton. Vi rekommenderar även att man implementerar stark autentisering för de applikationer som innehåller känslig information. Detta omfattar både interna och externa tjänster.

Flera delar i domänpolicyn bör ses över, speciellt lösenordspolicyn som bör uppdateras för att minska användandet av svaga lösenord.

Rutinen för konfiguration av servrar bör ses över så att man tar bort standardinloggningar och övrig standardkonfiguration som medför sårbarheter.

Utökad segmentering av nätverk och begränsad möjlighet att kommunicera mellan nätverken, skulle förhindra en angripare från att enkelt nå kritiska resurser. Angreppskomplexiteten som skulle krävas för att utföra intrång 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 för varje serversegment.

Vidare rekommenderar PwC att man implementerar lösningar för att detektera avvikande användarbeteende. Detta för att ytterligare kunna identifiera när ett användarkonto används i ett skadligt syfte. En sådan mekanism skulle kunna varna administratörer 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.

3.3.2. Rekommendationer efter genomförd dokumentgranskning

PwC:s rekommendation är att Sandvikens kommunstyrelse ställer krav på IT-avdelningen vad det gäller dokumentation, samt att man inför återkommande kontroller för att säkerställa att dokumentationen är på plats och är återkommande reviderad.

PwC rekommenderar att en kraftansamling och inventering görs avseende dokumentationen, uppdaterar samtlig dokumentation med ägare, datum, versionsnummer samt versionshistorik.

Årlig revidering av all IT-relaterad dokumentation bör införas.

All nödvändig dokumentation som i dag saknas bör upprättas.

Vidare rekommenderar PwC att revisionen gör en återkommande kontroll över dokumentationsläget om ett år för att säkerställa att ovanstående har åtgärdats.

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

2017-12-15

Niklas Ljung

Uppdragsledare

Projektledare

4. Bilaga 1 – Riskgradering intrångs-tester

Följande graderingar används i dokumentet för att redovisa den risk en viss sårbarhet utgör.

Gradering	Beskrivning
Hög	En sårbarhet med hög risk är något man bör åtgärda omedelbart. De 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 och kan hjälpa denne i kartläggning 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.

5. Bilaga 2 - Förslag till genomgång av informationshantering och uppdatering av dokumentation