pwc

Revisionsrapport

Innehållsförteckning

Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Solna Stad genomfört en granskning av lösenordsstandard och behörighetsinställningar i Active Directory inom staden.

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

Har kommunstyrelsen säkerställt att Solna Stads nuvarande lösenordsstandard samt kontohantering håller en tillräcklig och tillfredsställande nivå för att reducera risker för obehörig åtkomst?

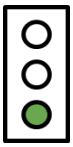
År 2018 bytte Solna Stad driftleverantör och man genomförde ett omfattande arbete kopplat till behörighets- och lösenordshantering inom Staden. I samband med bytet fick PwC, 2019 i uppdrag av de förtroendevalda revisorerna i Solna Stad att genomföra en granskning kring hantering av konton och behörigheter. Vid granskningen noterades brister gällande rutiner och efterlevnad av säkerhetsstandard. För att följa upp de rekommendationer som gavs i samband med granskningen 2019 fick PwC i uppdrag att utföra en uppföljande granskning av lösenordsstandard och behörighetshantering i Active Directory 2020.

Efter genomförd granskning är vår sammanfattande bedömning att kommunstyrelsen **har säkerställt** att Solna Stads nuvarande behörighetshantering samt lösenordsstandard håller en tillräcklig och tillfredsställande nivå för att reducera risken för obehörig åtkomst i nuläget.

Den sammanfattade bedömningen baseras på bedömningen av de fyra kontrollmålen för granskningen, vilka redovisas i rapporten.

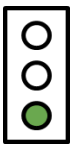
Kontrollmål 1

Kommunen har en god lösenordsstandard implementerad gällande exempelvis lösenordens längd och komplexitet.



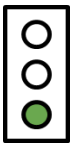
Kontrollmål 2

Inga konton med administratörsrättigheter ”*password never expired”* eller, där lösenordet ej har bytts ut på omotiverbart lång tid, har identifierats.



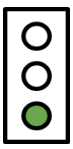
Kontrollmål 3

Kommunen har en försvarbar mängd domänadministratörskonton.



Kontrollmål 4

Behörighetssystemet är konfigurerat så att en användare som får nytt lösenord är tvingad att byta till ett personligt lösenord vid första påloggning.



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, cyberrisker, får ökad 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 även till den växande hotbilden.

Man har från såväl näringsliv som offentlig sektor insett att den hot- och riskbild som växer fram behöver bemötas. Vikten av en god behörighetshantering samt strängare lösenordskrav samt kontinuerlig revidering av användarbehörighet är en nödvändighet för att minska riskerna.

Revisorerna bedömde i sin riskanalys för 2019 att det fanns risk att kommunstyrelsen inte säkerställt att kommunen hade en god behörighetshantering och gav därför PwC i uppdrag att granska området. För att följa upp om de rekommendationer som gavs i samband med granskningen 2019 fick PwC i uppdrag att utföra en uppföljande granskning av lösenordsstandard och behörighetshantering i Active Directory 2020.

1.2. Syfte och revisionsfråga

Granskningen syftar till att besvara följande revisionsfråga:

Har kommunstyrelsen säkerställt att Solna Stads nuvarande lösenordsstandard samt kontohantering håller en tillräcklig och tillfredsställande nivå för att reducera risker för obehörig åtkomst?

1.2.1. Kontrollmål

Följande kontrollmål har använts vid granskningen för att besvara revisionsfrågan:

- Kommunen har en god lösenordsstandard implementerad gällande exempelvis lösenordens längd och komplexitet.
- Inga personliga konton med administratörsrättigheter som har *password never expired* eller där lösenordet ej har bytts ut på omotiverbart lång tid har identifierats.
- Kommunen har en försvarbar mängd domänadministratörskonton.
- Behörighetssystemet är konfigurerat så att en användare som får nytt lösenord är tvingad att byta till ett personligt lösenord vid första påloggning.

1.3. Revisionskriterier

Revisionskriterierna utgörs av nedanstående:

- Kontoinformation från Active Directory

1.4. Avgränsning

I tid avgränsas granskningen till år 2020 samt till granskningens kontrollfrågor.

1.4.1. Nominerade system

I granskningen har en Domänkontrollant Server (DC02) – Windows 2012 granskats gällande användarrättigheter och säkerhetsparametrar samt en Windows Server 2016 (PRN06) gällande säkerhetsparametrar.

1.5. Metod

Granskningen har utförts genom PwC:s tekniska koncept Baseline Security Assessment. Genomgång av systemuppsättning genom utläsning och analys av kontoinformation i Active Directory.

PwC har testat nivån på kontroll- och säkerhetsinställningar i jämförelse med CIS ramverk (Center for Internet Security) på följande servrar:

- Windows Server 2012 – DC02
- Windows Server 2016 – PRN06

2. Resultat

2.1. Kontrollmål 1

Kommunen har en god lösenordsstandard implementerad gällande exempelvis lösenordens längd och komplexitet.

2.1.1. Iakttagelser

Enligt Solna Stads lösenordspolicy används en 14 tecken lång lösenordsstandard med hög komplexitet som krav. Efter fem felaktiga inloggningsförsök ska kontot låsas i 15 minuter innan nytt försök kan påbörjas. Vid första påloggningen ska kontoägaren för samtliga kontotyper tvingas uppdatera lösenordet.

I den tekniska analysen visar säkerhetsinställningarna att användaren har 50 inloggningsförsök innan kontot blir låst. Stadens lösenordspolicy gällande kontolåsningsprincipen uppdaterades den 2020-12-03. Den tekniska analysen har baserats på säkerhetsparametrar uttagna den 2020-12-02. Övriga säkerhetsinställningar kopplade till lösenordsstandard efterlever Stadens policy.

2.1.2. Bedömning

PwC:s bedömning är att Solna Stad för närvarande har en god lösenordsstandard. Rekommendationen från CIS (Center for Internet Security) efterlevs till stor del. PwC:s samlade bedömning är att kontrollmålet är **uppfyllt**.

2.2. Kontrollmål 2

Inga personliga konton med administratörsrättigheter som har ”*password never expired*” eller där lösenordet ej har bytts ut på omotiverbart lång tid har identifierats.

2.2.1. Iakttagelser

PwC har utfört en teknisk granskning av konton med administrativa rättigheter. Beroende på behörighetstyp har dessa delats in i tre kategorier, enterprise-, domän- och administratörskonto.

Det finns inga konton med behörigheten *Enterprise Admin* som har ”password never expired” eller där lösenordet ej har bytts ut på omotiverbart lång tid.

Det finns elva konton med behörigheten *Domain Admins* som har ”password never expired”. Av dessa konton är dock samtliga systemkonton. Det finns inget konto där lösenordet ej har bytts ut på omotiverbart lång tid.

Det finns 16 konton med behörigheten *Administrative Rights* som har ”password never expired”. Av dessa konton är dock samtliga systemkonton. Det finns inget konto där lösenordet ej bytts ut på omotiverbart lång tid.

2.2.2. Bedömning

PwC:s bedömning är att det inte finns några personliga konton med ”password never expired” eller konton vars lösenord inte har bytts ut på omotiverbart lång tid. Kontrollmålet bedöms som **uppfyllt**.

2.3. Kontrollmål 3

Kommunen har en försvarbar mängd domänadministratörskonton.

2.3.1. Iakttagelser

Solna Stad har totalt 20 stycken domänadministratörskonton. Flertalet av kontona är systemkonton.

2.3.2. Bedömning

PwC:s bedömning är att Staden har en försvarbar mängd domänadministratörskonton. Kontrollmålet bedöms som **uppfyllt**.

2.4. Kontrollmål 4

Behörighetssystemet är konfigurerat så att en användare som får nytt lösenord är tvingad att byta till ett personligt lösenord vid första påloggning.

2.4.1. Iakttagelser

När en ny användare får ett konto tilldelas även ett systemgenererat lösenord. Detta lösenord måste användaren byta ut vid första påloggning.

När en redan befintlig användare behöver ett nytt lösenord kontaktar denna själv service desk. I majoriteten av fallen får personen ett nytt lösenord genom att identifiera sig i portalen via BankID. Vid fall där personen inte har BankID finns ett registrerat telefonnummer kopplat till samtliga användare som inte kan ändras av användaren själv. Ett nytt systemgenererat lösenord skickas i dessa fall via sms till personens telefonnummer.

När användaren får ett nytt lösenord tvingas personen att byta till ett personligt lösenord.

2.4.2. Bedömning

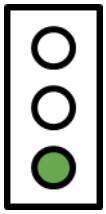
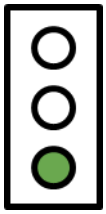
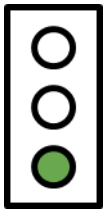
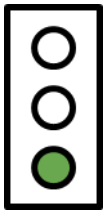
PwC:s bedömning är att behörighetssystemet är konfigurerat så att en användare tvingas byta till ett personligt lösenord vid första påloggning kopplade till AD:t. Kontrollmålet bedöms som **uppfyllt**.

3. Bedömningar

3.1. Revisionell bedömning

Efter genomförd granskning är den sammanfattade bedömningen att kommunstyrelsen har säkerställt att Solna Stads nuvarande behörighetshantering samt lösenordsstandard håller en tillräcklig och tillfredsställande nivå för att reducera risken för obehörig åtkomst.

3.2. Bedömning utifrån kontrollfrågor

Kontrollmål	Bedömning	
Kommunen har en god lösenordsstandard implementerad gällande exempel vid lösenordens längd och komplexitet.	PwC:s bedömning är att Solna Stad för närvarande har en god lösenordsstandard. Rekommendationen från CIS (Center for Inter-net Security) efterlevs till stor del. PwC:s samlade bedömning är att kontrollmålet är **uppfyllt**	
Inga personliga konton med administrativa rättigheter som har ”*password never expired*” eller där lösenordet ej har bytts ut på omotiverbart lång tid har identifierats.	PwC:s bedömning är att det inte finns några personliga konton med ”password never expired” eller konton vars lösenord inte har bytts ut på omotiverbart lång tid. Kontrollmålet bedöms som **uppfyllt**.	
Staden har en försvarbar mängd domänadministratörskonton.	PwC:s bedömning är att Staden har en för-svarbar mängd domänadministratörskonton. Kontrollmålet bedöms som **uppfyllt.**	
Behörighetssystemet är konfigurerat så att en användare som fått nytt lösenord är tvingad att byta till ett personligt lösenord vid första påloggning.	PwC:s bedömning är att behörighetssystemet är konfigurerat så att en användare tvingas byta till ett personligt lösenord vid första påloggning kopplade till AD:t. Kontrollmålet bedöms som **uppfyllt.**	

3.3. Rekommendationer

PwC har identifierat ett antal åtgärder som skulle leda till att behörighetshanteringen höjs till en högre nivå. Vi rekommenderar att Solna Stad analyserar rekommendationerna och tillämpar dem i samband med det pågående arbetet med informationssäkerheten inom Solna Stad. Utifrån genomförd granskning lämnas följande rekommendationer.

3.3.1. Rekommendation 1 – Tillåt ej användare att spara lösenord

Vid den tekniska granskningen noterades det att funktionen som ej tillåter användare att spara sitt lösenord i datorn är inaktiverat. Lösenord till konton som är sparade på datorn medför en större risk. Vid ett eventuellt angrepp kan lösenordet kapas och användas för att komma åt ytterligare servrar.

3.3.2. Rekommendation 2 – Aktivera låsning vid inaktivitet

Windows identifierar inaktivitet i en inloggningssession om mängden inaktiv tid överskrider angiven inaktivitets gräns. Denna inställning förhindrar obehörig åtkomst till enheten om den inloggade användaren skulle lämna datorn utan att avsiktligt låsa enheten. Vid den tekniska granskningen noterades det att det finns ingen gräns aktiverad då datorn ska låsas vid inaktivitet. Enligt CIS standard bör datorn låsas efter 900 sekunders inaktivitet.

2021-01-20

Anders Hägg	Niklas Ljung/Malin Lindvall
Uppdragsledare	*Projektledare*