Revisionsrapport

AD kontohantering

Söderköpings kommun 2018

Niklas Ljung

Oktober 2018

pwc

Innehåll

Sammanfattning

PwC har på uppdrag av Söderköping kommuns revisorer genomfört en granskning gällande kontohantering och efterföljande av regelverk inom IT. Brister gällande uppföljning och kontroll har konstaterats.

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

Har IT-avdelningen säkerställt att alla användarkonton tvingas byta lösenord var 90:e dag (vilket är kommunens standard)?

Efter genomförd granskning är PwC:s bedömning att ovanstående ***ej är uppnått***. Det finns ca 220 användarkonton i kommunens system som är aktiva konton och som *inte* tvingas byta lösenord var 90:e dag.

Rekommendationer

- PwC rekommenderar Söderköpings kommun att genomföra en genomgång/granskning av alla inställningar i kommunens AD-system.
- PwC rekommenderar Söderköpings kommun att säkerställa att det inte finns användarkonton som är undantagna lösenordsbyte var 90:e dag.
- PwC rekommenderar Söderköpings kommun att ta bort avslutade användare för att minska mängden konton och få större kontroll på aktiva konton. Det är även ur ett GDPR-perspektiv inte lämpligt att lagra personuppgifter utan motiverad anledning.

Inledning

Bakgrund

I samband med att PwC presenterade resultatet från granskningen av behörighetshantering som genomfördes under maj 2018, framkom att det fanns en del funderingar på hur kommunens IT-avdelning följer uppsatta regler kring *Password Never Expire*.

PwC åtog sig att genomföra ett mindre arbete för att få svar på frågan om det finns konton i kommunens AD som inte behöver byta lösenord.

Syfte och kontrollfråga

Granskningen syftar till att besvara följande fråga:

Har IT-avdelningen säkerställt att alla användarkonton tvingas byta lösenord var 90:e dag (vilket är kommunens standard)?

Metod

Granskningen genomförs med hjälp av *Baseline Security Assessment*. Metoden innebär att kommunens IT-avdelning får köra ett script i en eller två servrar i kommunens AD-system.

Scriptet plockar ut alla inställningar rörande kontohantering. När scriptet är kört returnerar kommunens IT-avdelning resultatet till PwC för att PwC ska kunna analysera resultatet.

Iakttagelser och bedömningar

Har IT-avdelningen säkerställt att alla användarkonton tvingas byta lösenord var 90:e dag (vilket är kommunens standard)?

Under analysen av den uthämtade AD-informationen från Söderköpings kommuns system, framkom det att det finns en del brister och förbättringsmöjligheter när det gäller kommunens kontohantering.

Efter en analys av resultatet kan man se att reglerna för kontohantering inte efterlevs.

I kommunens system finns det 1971 konton som har *Password Never Expire*. Merparten av dessa är konton är inaktiverade, men det finns ca 220 aktiva konton som har denna inställning.

Av de ca 220 konton som har inställningen *Password Never Expire* är 11 konton *Domain admin* och 21 konton har *Administrative rights*.

Special accounts with Domain administrative rights
Evidence shows that a total of 20 accounts have Domain administrative rights, of these:

- 11 accounts have the setting Password Never Expire enabled.

Special accounts with Administrative rights
Evidence shows that a total of 39 accounts have Administrative rights, of these:

- 21 accounts have the setting Password Never Expire enabled.

Det är acceptabelt att sätta konton med *Domain administrative rights* eller *Administrative rights* till *Password Never Expire* om dessa är maskinkonton, men i detta fall är flera av kontona vanliga användarkonton med höga rättigheter vilket bedöms som allvarligt.

Bedömning

Kontrollfrågan bedöms som ***ej uppnådd.***

Övriga iakttagelser och bedömningar

Av kommunens totalt 6588 konton är 3555 aktiva konton och 3033 konton avstängda konton. De avstängda/inaktiverade kontona innehåller bland annat för- och efternamn på kontots ägare. Ur ett GDPR-perspektiv är det inte lämpligt att kommunen sparar dessa konton längre än nödvändigt och reglerna för detta ska vara dokumenterade och förankrade.

Vi kan se att det finns 775 konton som någon aldrig har loggat in på, detta tyder på att någon process inte fungerar.

Bilaga

Till rapporten levereras en bilaga, *Baseline Security Assessment*. Det är resultatet från analysen av Söderköpings kommuns AD-information. I bilagan syns bara det som bedöms som negativt utifrån ”CIS Microsoft Windows Server 2012 Benchmark, version 1.1.0 - 11-04-2014”

https://benchmarks.cisecurity.org/tools2/windows/CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v1.1.0.pdf

2018-10-30

Lena Brönnert, uppdragsledare

Niklas Ljung, projektledare