Södertälje kommun

Rapport: IT-säkerhet – test av teknisk säkerhet
Januari 2024

Sammanfattning

EY har på uppdrag av de förtroendevalda revisorerna i Södertälje kommun granskat hur väl kommunens information hanteras i tekniska system. Syftet med granskningen var att bedöma om det finns brister i det praktiska arbetet med IT- och informationssäkerhet genom att testa hur väl utvalda IT-system och -miljöer står emot yttre angrepp. EY har genomfört granskningen genom att utföra två tekniska tester; en sårbarhetsanalys av externt exponerad infrastruktur och ett tekniskt penetrationstest av lärplattformen Vklass som används av Södertälje kommun.

De tekniska testerna har resulterat i observerade avvikelser som sedan legat till grund för denna gransknings rekommendationer.

Den samlade bedömningen är att kommunstyrelsen delvis har säkerställt att Södertälje kommuns IT-system och -miljöer är ändamålsenligt skyddade samt delvis säkerställt en ändamålsenlig styrning kopplat till säkerheten i de utvalda IT-system och -miljöer. Bedömningen grundar sig i att flera avvikelser har observerats men att endast ett fåtal avvikelser bedöms ha högre risk. Inga avvikelser som kräver omedelbara åtgärder har observerats. Genomförda tester utesluter inte att det finns ytterligare svagheter inom kommunens IT-infrastruktur.

Baserat på de avvikelser med högst riskbedömning har ett antal förbättringsområden identifierats och rekommendationer lämnats. EY rekommenderar kommunstyrelsen i Södertälje kommun att säkerställa att:

- Noterade avvikelser åtgärdas.
- Processer och rutiner för att säkerställa lämpliga säkerhetsinställningar införs.
- Tydliga rutiner för säkerhet hos leverantörer som förvaltar känslig information införs.

Innehållsförteckning

1. Inledning

1.1 Bakgrund

Södertälje kommun och dess nämnder hanterar stora mängder digital information. Detta ger många nya möjligheter i form av effektivare förvaltning, uppföljning och utökad service till medborgare, samtidigt som risker uppstår när informationen inte hanteras ändamålsenligt. För att uppnå god IT-säkerhet krävs att styrning och arbete bedrivs på ett sådant sätt att informationen är tillgänglig, riktigt, har tillräckligt starkt skydd samt är spårbar.

Under 2022 genomförde EY en granskning av informationssäkerhet i praktiken, där en simulerad nätfiske-attack, så kallad phishing, genomfördes. EY skickade då tillsammans med kommunen ut ett förfalskat e-postmeddelande till ett urval av kommunens medarbetare där de uppmanades till att klicka på en inbäddad länk och uppge användaruppgifter. Simuleringen resulterade i att EY tillhandahölls flertalet användaruppgifter som tillhörde kommunens medarbetare. Som en uppföljning av denna granskning har EY blivit ombedda att genomföra denna granskning, för att testa hur väl kommunens information hanteras i tekniska system. Denna granskning utforskar vad en angripare hade kunnat göra under ett intrång i kommunens system efter att ha kommit över användaruppgifter så som i granskningen genomförd 2022.

Granskningen genomförs genom att EY genomför en teknisk sårbarhetsanalys samt ett intrångsförsök under säkra och kontrollerade former. Genom att analysera säkerheten i utvalda system kan revisorerna dra slutsatser om huruvida den tekniska IT-säkerheten i kommunen ligger på en ändamålsenlig nivå. En granskning av denna typ svarar övergripande på revisionsfrågorna, men ger även såväl revisorer som verksamheten en lista med tydliga avvikelser som på olika sätt kan hota säkerheten i kommunens IT-system.

EY och de förtroendevalda revisorerna har beslutat att genomföra intrångsförsöket på lärplattformen Vklass då denna anses innehålla känslig information. Vklass används av kommunen som en administrationslösning för kommunens skolor och bland annat finns information som elevers omdöme, betyg och närvaro i systemet.

Definitioner återfinns i Bilaga 2.

1.2 Syfte och revisionsfrågor

Granskningens syfte är att bedöma om det finns brister i det praktiska arbetet med IT- och informationssäkerhet genom att testa hur väl utvalda IT-system och -miljöer står emot yttre angrepp.

Följande revisionsfrågor har besvarats genom granskningen:

- Har de utvalda IT-systemen och -miljöerna i Södertälje kommun ett ändamålsenligt skydd?
- Säkerställer kommunstyrelsen en ändamålsenlig styrning kopplat till säkerheten i de utvalda IT-systemen och -miljöerna?

1.3 Avgränsning

Granskningen avgränsas till vissa IT-system och -miljöer, i syfte att ge en djupare förståelse av dessa. Denna granskning ger alltså inte en helhetsbild av kommunens totala arbete inom IT- och informationssäkerhetsarbete utan syftar till att ge en detaljerad bild över ett begränsat område. Därtill har EY:s IP-adress som använts för sårbarhetsskanningen vitlistats i brandväggen av kommunen. EY har således inte testat brandväggens tekniska skydd.

1.4 Metod och genomförande

Granskningen bygger på EY:s ramverk för granskning av IT- och informationssäkerhet, särskilt framtagen för svensk kommunal sektor.

För att besvara revisionsfrågorna har EY genomfört följande tester under november och december 2023:

- Teknisk sårbarhetsanalys av externt exponerad infrastruktur
- Tekniskt penetrationstest av lärplattformen Vklass

För genomförandet av den tekniska sårbarhetsanalysen har EY mottagit IP-adresser som bedömts relevanta av kommunen. IP-adresser utöver dessa utvalda har inte ingått i analysen.

Tekniska penetrationstest kan genomföras med olika nivåer av ingångsinformation. Om en testare genomför ett penetrationstest med full förståelse för IT-miljön kallas detta för ett *white-box test*. Om ett penetrationstest i stället genomförs utan någon som helst kunskap eller förståelse för den specifika IT-miljön kallas detta för ett *black-box test*. Då denna granskning undersöker vad en angripare kan genomföra under ett intrångsförsök efter att ha kommit över vissa användaruppgifter från kommunens medarbetare genomfördes det tekniska penetrationstestet på lärplattformen Vklass med mottagna administratörskonton. Penetrationstestet genomfördes därmed med viss kännedom och information om systemet och är därmed en kombination av ett white-box och ett black-box test, ett så kallat *gray-box penetrationstest*.

Samtliga avvikelser som iakttogs under de två testerna har bedömts utefter låg-, medium-, eller hög risknivå.

1.5 Revisionskriterier

Granskningen genomförs enligt god revisionssed inom informationssäkerhetsområdet. Bedömningar görs mot Myndigheten för samhällsskydd och beredskaps (MSBs) ramverk för LIS (Ledningssystem för informationssäkerhet), som är ett etablerat ramverk i ett stort antal kommuner och inom offentlig förvaltning. Därutöver används MSB2032 Säkerhetsåtgärder i informationssystem som revisionskriterium. Båda ramverken bygger på den svenska och internationella standarden för informationssäkerhet, ISO/IEC 27000.

2. Granskningsresultat

2.1 Sårbarhetsanalys

Sårbarhetsanalysen av Södertälje kommuns externt exponerade IT-infrastruktur syftade i huvudsak till att identifiera säkerhetsbrister och sårbarheter som kan leda till säkerhetsincidenter.

2.1.1 lakttagelser

Totalt observerades fem avvikelser. Fyra av dessa bedöms utgöra en låg risk medan en bedöms utgöra en hög risk. De lägre rankade avvikelserna omfattar bland annat konfigurationer som inte är tillräckligt skyddade samt sårbarheter i vissa inställningar för ett antal servrar. Den högst rankade avvikelsen avser svaga kryptografiska konfigurationer och bedöms kräva måttlig utveckling eller justering. Denna observation innebär att en angripare kan få tillgång till information som exempelvis kan spridas eller användas för vidare intrång.

Nr	Avvikelse	Risk
1	Svaga kryptografiska inställningar på ett flertal servrar.	Hög
2	Informationsläckage från vissa servrar.	Låg
3	Konfigurationsgränssnitt[1] kräver inte autentisering.	Låg
4	Föråldrad och sårbar webbserver.	Låg
5	Mailserver tillåter vidarebefordring.	Låg

Tabell 1: Denna tabell visar de avvikelser som gjordes i samband med sårbarhetsanalysen och dess bedömda risknivå.

2.1.2 Bedömning

Baserat på de avvikelser som har observerats bedömer EY att kommunens externt exponerade infrastruktur har vissa brister som kan underlätta för en angripare. Avvikelse 1 medför en risk att en angripare, i värsta fall, skulle kunna dekryptera och avläsa känslig information som sedan kan användas för ytterligare attacker eller spridas vidare. Information såsom inloggningsuppgifter skulle i teorin kunna avläsas. Angrepp som dessa är generellt väldigt svåra att upptäcka.

EY noterar att kommunens brandvägg har försvårat för den tekniska sårbarhetsanalysen, vilket är ett tecken på god funktionalitet. Då granskningen inte syftade till att testa brandväggen kopplades denna bort för att möjliggöra granskning av de tjänster som ligger bakom brandväggen.

[1] Den kontrollpanel där inställningar för drift av server utförs

2.2 Tekniskt penetrationstest av lärplattformen Vklass

Det tekniska penetrationstestet av lärplattformen Vklass syftade i huvudsak till att identifiera säkerhetsbrister i Vklass webbapplikation för att avgöra om en angripare kan få obehörig åtkomst med hjälp av funktionaliteten och komma åt känslig information.

2.2.1 Iakttagelser

Totalt observerades sju avvikelser. Av de avvikelser som observerades bedöms fem medföra en låg risk, en bedöms medföra en medelhög risk och en bedöms medföra en hög risk. De lägre rankade avvikelserna omfattar bland annat informationsläckage, säkerhetsinställningar som kan förbättras och andra inställningar som skapar vissa sårbarheter. De högre rankade avvikelserna påvisar att leverantören använder föråldrade mjukvarukomponenter samt mjukvarukomponenter med kända sårbarheter, vilket kan utnyttjas av en angripare.

Nr	Avvikelse	Risk
1	Användning av föråldrade tredjepartskomponenter.	Hög
2	Användning av tredjepartskomponenter med kända sårbarheter.	Medel
3	Informationsläckage från vissa felmeddelanden.	Låg
4	Informationsläckage från vissa servrar.	Låg
5	Säkerhetsinställning för anslutning kan göras hårdare.	Låg
6	Webbläsarens tolkning av tekniskt innehåll är möjligt att manipulera.	Låg
7	Funktionen för komplettering av formulär aktiverat för lösenord.	Låg

Tabell 2: Denna tabell visar de avvikelser som observerades i samband med det tekniska penetrationstestet och dess bedömda risknivå.

2.2.2 Bedömning

Baserat på de avvikelser som har observerats bedömer EY att sårbarheter i Vklass skulle kunna utnyttjas av en angripare som vill komma åt den funktion eller data som kommunen använder. Det tekniska penetrationstestet påvisar att leverantören använder föråldrade mjukvarukomponenter samt flera olika föråldrade paket med vanligt förekommande och kända sårbarheter. Dessa sårbarheter skulle kunna utnyttjas av angripare som i värsta fall skulle kunna få obehörig åtkomst till systemet, stjäla data eller orsaka skada på IT-infrastruktur. Södertälje kommun bör gå igenom resultaten tillsammans med leverantören för att diskutera åtgärder för att minska de identifierade riskerna kopplat till identifierade avvikelser.

3. Övergripande rekommendationer

Nedan beskrivs övergripande rekommendationer till kommunstyrelsen.

3.1 Åtgärdande av observerade brister

De genomförda tekniska testerna resulterade i totalt 12 avvikelser som tyder på att det finns brister i kommunens hantering av tekniska system. Avvikelser med högre riskbedömning tyder på att det finns brister och sårbarheter en angripare skulle kunna dra nytta av för att skaffa sig obehörig åtkomst, stjäla och sprida information och data eller orsaka skada.

EY rekommenderar kommunstyrelsen att säkerställa att samtliga avvikelser åtgärdas och att de avvikelserna med högst riskbedömning prioriteras.

3.2 Säkerställande av rutiner och processer

Sårbarhetsanalysen påvisar att det finns vissa brister i kommunens hantering av externt exponerad IT-infrastruktur. Bland annat använder kommunen svaga kryptografiska inställningar och föråldrade inställningar som kan riskera att en angripare avläser känslig information och eventuellt sprider denna vidare eller använder den för att orsaka ytterligare skada.

EY rekommenderar kommunstyrelsen att säkerställa att det finns rutiner och processer kopplade till att upptäcka föråldrade inställningar samt sårbarheter i IT-infrastrukturen. Vidare rekommenderas kommunstyrelsen att säkerställa att det finns rutiner och processer för att säkerställa att säkerhetsinställningar är lämpliga och förblir lämpliga över tid.

3.3 Leverantörshantering

Det tekniska penetrationstestet påvisar att det finns vissa brister och sårbarheter i systemet Vklass som i värsta fall skulle kunna utnyttjas av en angripare för att få åtkomst till systemet, stjäla data och sprida information, eller orsaka skada. Bland annat använder leverantören föråldrade mjukvarukomponenter och mjukvarukomponenter med kända sårbarheter som kan utnyttjas av angripare.

EY rekommenderar att kommunstyrelsen säkerställer att det finns rutiner och processer för att följa upp och säkerställa att leverantörer som hanterar känslig information har en god hantering av tekniska system. Exempelvis kan kommunen fortsätta genomföra tekniska tester av leverantörens system. Vidare rekommenderas kommunstyrelsen att säkerställa att den tekniska rapporten kopplat till det tekniska penetrationstestet hos Vklass hanteras tillsammans med leverantören i syfte att säkerställa att de observerade avvikelserna och sårbarheterna blir kända för leverantören, och åtgärdade.

4. Revisionsfrågor

Granskningen har utgått från två revisionsfrågor. Hur väl Södertälje kommun svarar upp mot dessa revisionsfrågor beskrivs nedan.

Tabell 3: Förklaring av färgkod

Färgkod	Förklaring
	Revisionsfråga besvaras ej tillfredsställande
	Revisionsfråga besvaras delvis tillfredsställande
	Revisionsfråga besvaras tillfredsställande

Tabell 4: Svar på revisionsfrågor

Revisionsfråga	Svar	
Har de utvalda IT-systemen och -miljöerna i Södertälje kommun ett ändamålsenligt skydd?	EY bedömer att Södertälje kommun delvis har ett ändamålsenligt skydd. Bedömningen grundar sig i att flertalet avvikelser har identifierats men att dessa varierar i risknivå. Två avvikelser bedöms medföra högre risker och påvisar allvarliga brister i säkerhetskontroller och bör därmed åtgärdas snarast. Majoriteten av avvikelserna bedöms däremot medföra en lägre risk.	
Säkerställer kommunstyrelsen en ändamålsenlig styrning kopplat till säkerheten i de utvalda IT-systemen och -miljöerna?	EY bedömer att kommunstyrelsen delvis har en ändamålsenlig styrning kopplat till säkerheten i de utvalda IT-system och -miljöerna. Bedömningen grundar sig i att avvikelser har observerats, och ett fåtal bedöms medföra medel- eller hög risk.	

5. Slutsatser

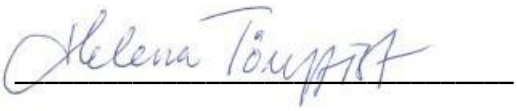
Granskningens syfte har varit att bedöma om det finns brister i det praktiska arbetet med IT- och informationssäkerhet genom att testa hur väl utvalda IT-system och -miljöer står emot yttre angrepp.

EY:s samlade bedömning är att kommunstyrelsen delvis har säkerställt att Södertälje kommuns IT-system och -miljöer är ändamålsenligt skyddade samt delvis säkerställt en ändamålsenlig styrning kopplat till säkerheten i de utvalda IT-system och -miljöer. Bedömningen grundar sig i att flera avvikelser har observerats men att endast ett fåtal avvikelser bedöms ha högre risk. Inga avvikelser som kräver omedelbara åtgärder har observerats. Genomförda tester utesluter inte att det finns andra svagheter inom kommunens IT-infrastruktur.

Med grund i ovan är EY:s främsta rekommendationer att kommunstyrelsen i Södertälje kommun säkerställer att:

- Noterade avvikelser åtgärdas.
- Processer och rutiner för att säkerställa lämpliga säkerhetsinställningar införs.
- Tydliga rutiner för säkerhet hos leverantörer som förvaltar känslig information införs.

Stockholm 2024-01-15



Helena Törnqvist
Partner, EY

Bilaga 1: Intervjuade funktioner

- Operativ IT-chef
- Fd. Operativ IT-chef
- Representant från utbildningskontoret
- Säkerhetsansvarig

Bilaga 2: Definitioner

IT-infrastruktur: IT-infrastruktur är de komponenter inom en organisation som tillsammans används för att producera, hantera, beräkna, hämta och lagra data. Exempel på detta kan vara en databas eller olika servrar.

Sårbarhetsanalys: En sårbarhetsanalys är en revision av en IT-miljö för att upptäcka sårbarheter som en angripare kan utnyttja.

Tekniskt penetrationstest: Ett tekniskt penetrationstest innebär att en aktör under kontrollerade former gör intrång i ett system. Detta kan genomföras på olika sätt och med olika nivåer av ingångslägen. Tekniska penetrationstest brukar delas upp i tre olika nivåer; White-box, Black-box och Gray-box testning.

White-box testning: En aktör genomför ett tekniskt penetrationstest med full initial förståelse för den IT-miljö som testas.

Black-box testning: En aktör genomför ett tekniskt penetrationstest utan någon initial information kring den IT-miljö som testas.

Gray-box testning: En aktör genomför ett tekniskt penetrationstest med viss information kring den IT-miljö som testas, exempelvis genom att ha tillgång till konton.

Phishing: Phishing, på svenska kallat nätfiske, är en metod för cyberkriminella att attackera privatpersoner, företag eller organisationer. Metoden går att utforma på olika sätt men går generellt ut på att lura en mottagare att ladda ner en fil, öppna ett dokument eller trycka på en länk via ett sms eller ett e-postmeddelande. Syftet är att utvinna konfidentiell information eller att implementera skadlig kod.

Inbäddad länk: En inbäddad länk är en länk man exempelvis bäddar in i en text eller i en bild, vilket innebär att man kan minska transparensen i att en länk existerar eller vart den leder. Processen är vanlig i en phishing-attack då det ökar mottagarens benägenhet att trycka på länken.