Vänersborgs kommun

Missiv

Revisorerna
2024-11-07

Till:
Kommunstyrelsen

För kännedom till:
Kommunfullmäktige

Granskning av IT-säkerhet i praktiken

På uppdrag av de förtroendevalda revisorerna i Vänersborgs kommun har EY genomfört en granskning av IT-säkerhet i praktiken. Syftet har varit att bedöma ändamålsenligheten i det praktiska arbetet med IT- och informationssäkerhet samt att bedöma i vilken utsträckning en angripare riskerar att komma åt kommunens IT-miljöer genom angrepp via e-post, så kallad phishing. Ökad digitalisering leder till ökade informationssäkerhetsrisker. Cyberkriminella attackerar inte enbart den tekniska miljön utan väljer i hög utsträckning att rikta in sig på människorna i organisationen. Mänskliga svagheter utnyttjas för att komma åt känslig information eller för att sprida skadlig kod. En fullbordad phishing-attack kan innebära stora konsekvenser för en kommun, både ekonomiskt och i form av försämrat anseende. Det är därmed viktigt för organisationen att arbeta proaktivt för att hantera det ökade hotet från phishing. Granskningen har därför utförts genom att testa medarbetarnas medvetenhet och kunskap inom området, bland annat genom att simulera ett angrepp via e-post.

Den sammanfattande bedömningen utifrån det simulerade angreppet är att Vänersborgs kommun som helhet löper låg risk att utsättas för en fullbordad phishing-attack. Det finns dock ett fortsatt behov av att öka medarbetarnas medvetenhet kring hur ett falskt e-postmeddelande kan se ut. Denna bedömning grundar sig i att 98 medarbetare klickade på den länk som skickades ut, samt att 27 medarbetare uppgav sina användaruppgifter. Vi revisorer noterar att IT-avdelningen, trots överenskommelse om att inte förvarna om det simulerade angreppet, valt att på eget initiativ på förhand publicera information om e-postutskicket på intranätet. Det kan ha minskat antalet personer som klickade på länken. Vid en verklig attack kan räcka med att endast en användare uppger sina användaruppgifter för att den cyberkriminella aktören ska kunna utföra ett lyckat intrång och, i värsta fall, ta kontroll över kommunens IT-miljöer.

Det är enligt revisionen också viktigt att tydliggöra hur och till vem pågående eller potentiella säkerhetsincidenter relaterade till en phishing-attack ska rapporteras. Slutligen visar granskningen att det finns behov av att förtydliga ansvar och mandat samt förbättra samarbete mellan de delar av verksamheten som ansvarar för informationssäkerhetsfrågor.

Utifrån granskningens resultat lämnas följande rekommendationer till kommunstyrelsen:

- Upprätta styrdokument gällande incidenthantering.
- Säkerställa att det fortsatt sker övningsinsatser inom informationssäkerhet.
- Tillse en ändamålsenlig ansvarsfördelning och samverkansstruktur mellan IT-kontoret och Juridik & säkerhetskontoret vad gäller informationssäkerhetsfrågor.

Bilaga: *Granskning av IT-säkerhet i praktiken*

Granskningsrapporten översänds med önskemål om att **senast den 7 februari 2025** erhålla ett svar på vilka åtgärder som kommunstyrelsen ämnar vidta med anledning av de rekommendationer som lämnas i rapporten.

Missivet är digitalt undertecknet och saknar därför namnunderskrifter.

Gunnar Lidell, ordförande

Magnus Cassel, vice ordförande

Bilaga: *Förstudie av krisberedskapsarbetet*

Vänersborgs kommun

Detta dokument är elektroniskt signerat och juridiskt bindande.

Signed by: Leif Gunnar Lidell
Date: 2024-11-20 08:24:39
BankID refno: 991d3ff0-717a-4a25-adeb-dc66d6e66a28

Revisor : Gunnar Lidell

Signed by: MAGNUS CASSEL
Date: 2024-11-19 22:45:23
BankID refno: 0e0f6355-dd4d-409b-972e-e6b4a0ced699

Revisor: Magnus Cassel