Vänersborgs kommun

Rapport: Informationssäkerhet i praktiken
november 2024

Sammanfattning

På uppdrag av de förtroendevalda revisorerna i Vänersborgs kommun har EY genomfört en granskning som syftar till att bedöma om det finns brister i det praktiska arbetet med IT- och informationssäkerhet inom området phishing. Detta har genomförts genom att testa medarbetarnas medvetenhet och kunskap inom området, bland annat genom att simulera ett angrepp via e-post. För att effektivt genomföra ett test av personalens agerande har en del av kommunens tekniska skydd mot phishing-attacker kopplats bort – syftet har inte varit att testa tekniken.

Granskningen genomfördes från augusti till november 2024. EY utformade och genomförde granskningen tillsammans med representanter från kommunen i syfte att uppnå en så stor nytta som möjligt för verksamheten. Metoden som använts bygger på EY:s beprövade metodik för att genomföra en simulerad phishing-attack, det vill säga ett utskick av ett falskt e-postmeddelande som uppmanar till att uppge användaruppgifter. Tre huvudområden analyserades: 1) Mottagare som klickat på länken i e-postmeddelandet, 2) Mottagare som uppgav användaruppgifter på landningssidan samt 3) Mottagarnas medvetenhet kring informationssäkerhet och phishing. Dessa områden jämfördes sedan mot på förhand definierade acceptansnivåer och med vad EY anser är en godtagbar standard inom offentlig sektor.

Resultatet av genomförd simulerad phishing-attack visar att Vänersborgs kommun som helhet löper en låg risk att utsättas för en fullbordad phishing-attack. Trots att kommunen återkommande genomför övningsinsatser inom informationssäkerhet, bedömer EY att det finns ett fortsatt behov av att öka medarbetarnas medvetenhet kring hur ett falskt e-postmeddelande kan se ut. EY bedömer även att det är viktigt att tydliggöra hur, och till vem, pågående eller potentiella säkerhetsincidenter relaterade till en phishing-attack ska rapporteras. Denna bedömning grundar sig i att 98 medarbetare (2,1 %) klickade på länken samt att 27 medarbetare uppgav sina användaruppgifter. Kommunen valde att på eget initiativ på förhand publicera information om e-postutskicket på intranätet vilket kan ha påverkat övningens resultat. EY vill betona att det 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.

Enkätresultatet indikerar på att 27 procent av deltagarna inte vet hur, eller känner sig osäkra på, hur phishing ska rapporteras. Det kan härledas till en avsaknad av skriftliga policyer och rutiner för rapportering. Därtill visar genomförda intervjuer att det finns förbättringsåtgärder vad gäller samverkan inom informationssäkerhetsfrågor mellan IT-kontoret och Juridik & säkerhetskontoret. Vilket är en konsekvens av uppdelade ansvarsområden.

Kommunstyrelsen rekommenderas därför att vidta åtgärder för att förbättra sin motståndskraft mot phishing och således minska risken för fullbordade phishing-attacker. Baserat på granskningen lämnar EY tre övergripande rekommendationer:

- 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.

Innehållsförteckning

1. Bakgrund

Vänersborgs kommun med dess nämnder och förvaltningar 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 informationssäkerhet krävs att styrning och arbete bedrivs på ett sådant sätt att informationen är tillgänglig, riktigt, har tillräckligt starkt skydd samt är spårbar.

Kommunens revisorer har identifierat risker relaterat till kommunens övergripande arbete med IT- och informationssäkerhet. De förtroendevalda revisorerna har därför valt att genomföra en granskning för att testa hur väl riktlinjer och rutiner med IT– och informationssäkerhet har kommunicerats till medarbetarna i praktiken.

Granskningen har genomförts genom att EY har simulerat en attack där falsk e-post skickats ut till medarbetarna, en så kallad phishing-attack eller nätfiske. Genom ett fullgott informationssäkerhetsarbete från kommunens sida, bör medarbetarna kunna identifiera ett sådant angrepp och veta hur de ska agera för att hantera och rapportera den simulerade attacken med bibehållen säkerhet. Genom att analysera hur många som agerade korrekt kan revisorerna få en bild av hur väl utbildning och medvetenhet fungerar i praktiken.

1.1 Phishing och nätfiske

Ökad digitalisering leder till ökade informationssäkerhetsrisker. Cyberkriminella attackerar inte enbart en organisations tekniska miljö utan väljer i hög utsträckning att rikta in sig på människorna i organisationen. Cyberkriminella ägnar sig åt social manipulation genom att utnyttja mänskliga svagheter såsom rädsla och förtroende för att komma åt känslig information eller för att sprida skadlig kod, något som riskerar att allvarligt skada organisationer, deras intressenter och samhället i stort. Denna typ av manipulation kan ske på olika sätt, exempelvis genom att övertyga medarbetaren att besöka skadliga hemsidor och ladda ner skadlig programvara. Manipulation kan även ske genom att den cyberkriminella får medarbetaren att uppge viktig information genom telefon, så kallad *phishing*, eller att ansluta ett USB-minne till organisationens nätverk. Det finns även andra mänskliga faktorer vilka medför risker, som användning av svaga lösenord, eller att samma lösenord används på flera, viktiga platser.

Idag ser vi och hör alltmer om hur phishing och nätfiske sker mer frekvent i samhället, mot enskilda individer men även mot företag och organisationer som verkar inom såväl privat som offentlig sektor. Till följd av den ökade mängden angrepp har Europeiska unionen (EU) beslutat om att införa ett nytt EU direktiv rörande cybersäkerhet, Network and Information Security Directive 2, NIS2. NIS2-direktivet är ett viktigt lagstiftningsinstrument inom regleringslandskapet för cybersäkerhet. Eftersom cyberattacker ökar behöver företag, kommuner och andra organisationer säkerställa motståndskraft för att minska risken att bli utsatt. NIS2 kräver att organisationer ska vidta adekvata cybersäkerhetsåtgärder genom att delegera och verkställa ansvar för att snabbt svara på störningar. Direktivet gäller företag och organisation inom flertalet olika sektorer, däribland offentlig sektor. Direktivet är obligatoriskt att följa för de olika medlemsländerna inom EU.

En fullbordad phishing-attack kan innebära stora konsekvenser för en organisation, både ekonomiskt och i form av försämrat anseende och rykte. Det är därmed viktigt för organisationen att arbeta proaktivt för att hantera det ökade hotet från phishing. En viktig åtgärd som organisationer kan vidta för att öka sin robusthet vid angrepp från cyberkriminella aktörer, är att skapa och bibehålla en medvetenhet om hotet från phishing bland sina medarbetare. Detta genom att förbättra deras förmåga att kunna identifiera falska e-postmeddelanden. Medarbetare bör även ha en tydlig rapporteringsväg att följa för att rapportera misstänka e-postmeddelanden. Ett annat sätt att minska riskerna för den här typen av cyberattacker är att kontinuerligt genomföra medvetenhetsträning inom informationssäkerhet. Detta för att medarbetare ska kunna upptäcka och reagera på försök till nätfiske.

1.2 Syfte och revisionsfrågor

Granskningens syfte är att bedöma om det finns brister i det praktiska arbetet med IT- och informationssäkerhet i Vänersborgs kommun genom att testa utbildning och medvetenhet hos personalen inom kommunen. Vidare är syftet att bedöma i vilken utsträckning en angripare riskerar att komma åt kommunens IT-miljöer genom angrepp via e-post. Följande revisionsfrågor har legat till grund för granskningen:

- Hanterar Vänersborgs kommuns medarbetare hotet från attacker genom falska email, så kallad phishing (nätfiske) på ett ändamålsenligt sätt?
- Har Vänersborgs kommun en incidenthanteringsprocess som aktiveras på ett ändamålsenligt sätt av de testade medarbetarna under den simulerande attacken?
- Är riktlinjer för hantering och rapportering av falska e-post och andra incidenter kända hos medarbetarna?

1.3 Avgränsningar

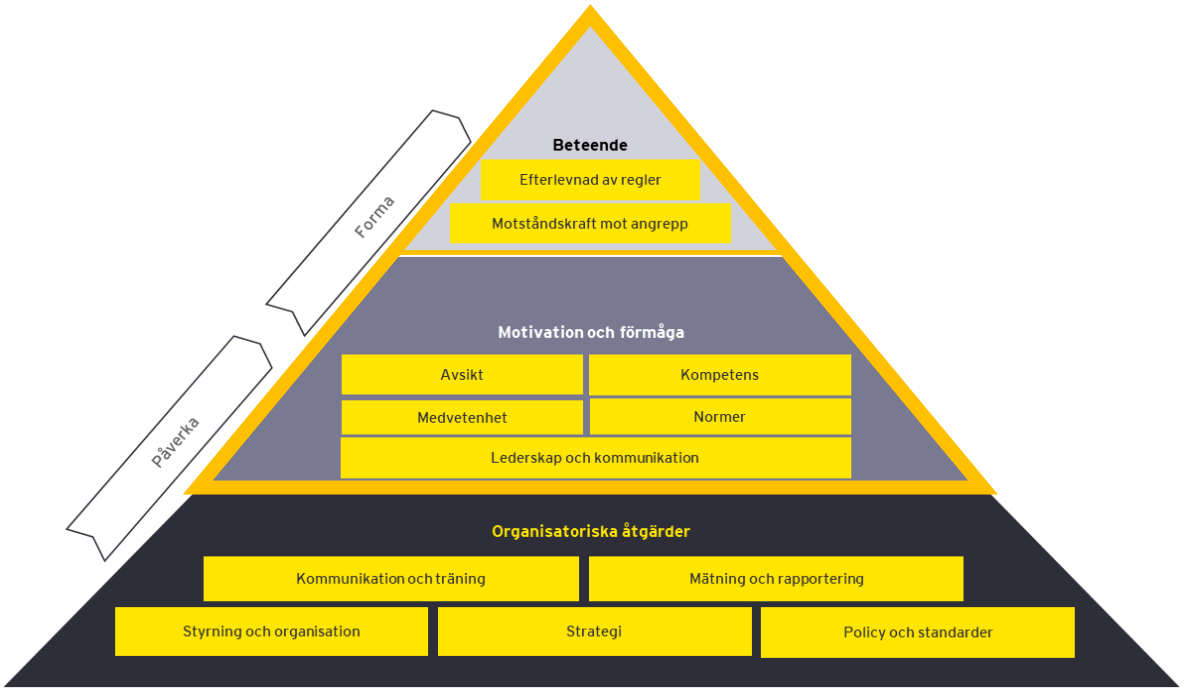
Granskningen är avgränsad till att ge en bild av hur sårbar kommunen är för attacker riktade mot personalen via e-post. Det ges alltså inte någon helhetsbild av det totala arbetet inom IT- och informationssäkerhet utan syftet är att ge en mer detaljerad bild av ett begränsat område. Då syftet är att testa personalens agerande har ingen teknisk testning utförts för att granska effektiviteten i kommunens skalskydd, det vill säga hur väl tekniska hjälpmedel fungerar för att identifiera och stoppa falska e-postmeddelanden. Det finns ingen teknisk lösning som kan ge ett helt säkert skydd mot phishing, utan det är slutligen personalens agerande som är avgörande.

1.4 Metod och genomförande

Granskningen bygger på EY:s etablerade ramverk för hur en organisation arbetar med informationssäkerhet. *Figur 1* nedan visar hur organisatoriska åtgärder som exempelvis kommunikation och utbildning, styrning samt riktlinjer ligger till grund för nivån av informationssäkerheten i en organisation. De organisatoriska åtgärderna påverkar sedan i sin tur motivationen och förmågan hos anställda att agera i enlighet med de riktlinjer organisationen fastställt. Motivationen och förmågan hos anställda baseras på flera olika faktorer som ledarskap och kommunikation, avsikt samt medvetenhet och kompetens kring

informationssäkerhet. Motivationen och förmågan hos medarbetarna i Vänersborgs kommun har i denna granskning utvärderats genom en enkät som distribuerades efter genomförd övning. Enkätens syfte var även att mottagarna själva skulle reflektera över deras medvetenhet, kunskap och beteende kring informationssäkerhet.

Motivationen och förmågan hos medarbetarna i en organisation formar i sin tur deras beteende relaterat till informationssäkerhet, närmare bestämt hur väl man efterlever regler och hur stark motståndskraften är mot ett potentiellt angrepp inom organisationen. Beteendet hos medarbetare i Vänersborgs kommun har i denna granskning utvärderats genom att utföra en simulerad phishing-attack. Notera att granskningen i sin helhet huvudsakligen fokuserar på de två översta delarna av ramverket: Beteende samt Motivation och förmåga.



Figur 1: EY:s ramverk för bedömning av en organisations informationssäkerhet.

Nedan följer en mer detaljerad beskrivning av EY:s metodisk för att utföra en phishing-övning och en detaljerade beskrivning av hur övningen genomfördes.

1.4.1 Metod

EY använder en beprövad metodik för att genomföra och analysera en simulerad phishing-attack. Övningen sätts upp med hjälp av ett verktyg som används för att skicka ut ett e-postmeddelande till den definierade målgruppen och för att samla in data kring hur mottagarna hanterat meddelandet. Därefter skickades en enkät ut till kommunens anställda med frågor som syftade till att undersöka medarbetarnas kunskap inom området informationssäkerhet. För en mer detaljerad redogörelse för EYs metodik, målgrupp och genomförande, se bilagor 1-6. Insamlad information jämförs sedan mot på förhand definierade acceptansnivåer och vad EY anser är en godtagbar standard i offentlig sektor. Den information som ligger till grund för granskningen har samlats in av EY i möten med lämpliga och kunniga personer från IT-avdelningen i Vänersborgs kommun.

För att besvara revisionsfrågorna har EY analyserat tre huvudområden enligt nedan:

- **Mottagare som klickade på länken i e-postmeddelandet** – EY har granskat hur många mottagare av det förfalskade e-postmeddelandet som klickade på den inbäddade länken till landningssidan (internetsida). Detta för att få en förståelse för personalens motståndskraft mot hotet av phishing samt hur god kunskapsnivån hos kommunens medarbetare är för att kunna identifiera ett e-postmeddelande från en falsk avsändare. EY bedömer att detta är ett viktigt område att granska då riskerna för att cyberkriminella kan utvinna känslig information, implementera skadlig kod, eller attackera en organisations IT-infrastruktur ökar avsevärt om en mottagare klickar på en skadlig länk.

- **Mottagare som uppgav användaruppgifter på landningssidan** – EY har granskat hur många mottagare av det förfalskade e-postmeddelandet som initialt klickade på länken inbäddad i e-postmeddelandet för att sedan uppge användaruppgifter på den förfalskade landningssidan. Detta för att skapa en förståelse för hur stark kommunens motståndskraft är mot angrepp av phishing samt för att mäta kunskapsnivån hos kommunens medarbetare att kunna identifiera en förfalskad landningssida från en okänd domän. EY bedömer att detta är ett viktigt område att granska då riskerna för att cyberkriminella utvinner känslig information och tar sig in i en organisations IT-infrastruktur ökar avsevärt om en medarbetare delar med sig av sina användaruppgifter.

- **Mottagares medvetenhet om informationssäkerhet och phishing** - EY har med hjälp av kommunen distribuerat en enkät med syftet att skapa sig en uppfattning om motivationen och kunskapen relaterat till denna typ av cyberhot hos mottagarna av e-postmeddelandet. Enkäten omfattar frågor kring e-postmeddelandet som användes i simuleringen och säkerhetskulturen på kommunen i form av utbildning och medvetenhet, styrande dokument och rapportering av säkerhetsincidenter. En tidig rapportering av ett misstänksamt e-postmeddelande tillåter en organisation att omedelbart upptäcka en cyberattack av detta slag, utreda dess omfattning, samt sätta in lämpliga skyddsåtgärder. EY har därför även undersökt hur många mottagare av det förfalskade e-postmeddelandet som valde att rapportera meddelandet. EY bedömer detta som ett viktigt område att granska, då det visar på hur medvetna medarbetarna inom kommunen är om hotet av phishing, samt deras kunskap om hur de ska agera i enlighet med kommunens riktlinjer när ett falskt e-postmeddelande upptäcks.

2. Analys

I följande kapitel analyseras resultatet av den simulerade attack som EY utformat tillsammans med Vänersborgs kommun. Analysen presenteras i tre delar baserat på tre huvudområden: 2.1 Mottagare som klickat på länken i e-postmeddelandet, 2.2 Mottagare som uppgav användaruppgifter på landningssidan och 2.3 Mottagares medvetenhet kring informationssäkerhet och phishing.

2.1 Mottagare som klickade på länken i e-postmeddelandet

I detta avsnitt presenteras andelen mottagare som klickade på länken i e-postmeddelandet. Vänersborgs kommun har i samråd med EY på förhand bestämt acceptansnivåer baserat på omfattningen av kommunens informationshantering och riskaptit. *Tabell 3* nedan beskriver de beslutade acceptansnivåerna för andelen mottagare som klickar på länken.

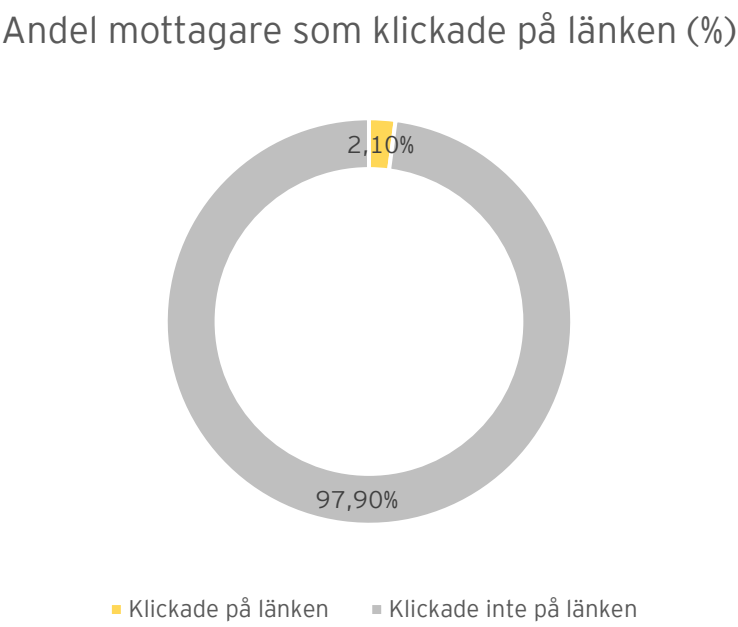
Resultatet av den simulerade attacken visar att 98 medarbetare (2,1 procent) klickade på länken i e-postmeddelandet och att Vänersborgs kommun som helhet löper en låg risk att utsättas för en fullbordad phishing-attack enligt de definierade acceptansnivåerna.

Tabell 3: Acceptansnivåer för andelen mottagare som klickar på länken i e-postmeddelandet

Riskanalys	Acceptansnivå (%)
Mycket hög risk	>15%
Hög risk	10-15%
Medelhög risk	5-10%
Låg risk	<5%

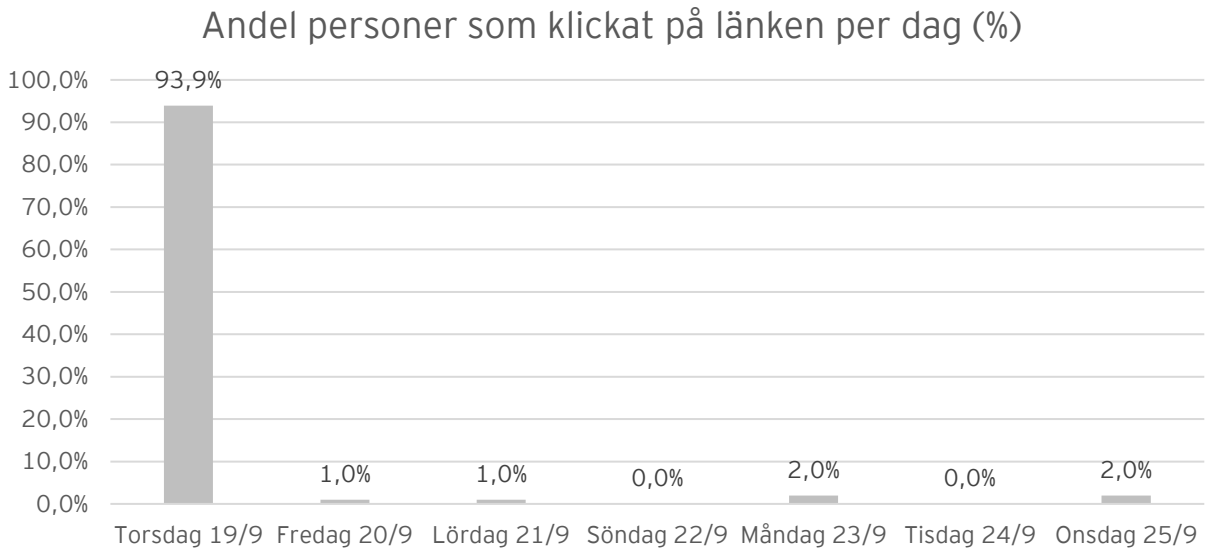
2.1.1. Resultat av simulering

Det insamlade resultatet analyserades utifrån hur många mottagare som klickat på länken i det förfalskade meddelandet. Av 4613 mottagare klickade 98 medarbetare och förtroendevalda på länken i e-postmeddelandet, vilket motsvarar 2,1 procent av mottagarna, se *figur 2* nedan. Det här resultatet innebär enligt acceptansnivåerna att Vänersborgs kommun som helhet löper en låg risk att utsättas för en fullbordad phishing-attack.



Figur 2: Fördelningen av andel mottagare som klickade på länken i e-postmeddelandet. Resultatet beskriver kommunen som helhet.

Från *figur 3* framgår det att majoriteten av mottagarna (94%) som klickade på länken gjorde detta under simuleringens första dag. Efter simuleringens första dag noterar EY att trenden är kraftigt nedgående. En nedåtgående trend är enligt EY förväntad i simulerade phishing-attacker likt den som genomförts i Vänersborgs kommun, som påkallar omedelbara handlingar från mottagaren utifrån hur e-postmeddelandet är formulerat. Kommunen valde att på eget initiativ på förhand publicera information om e-postutskicket på intranätet, vilket kan ha minskat antalet personer som klickade på länken, och i större utsträckning påverkat antalet medarbetare som rapporterat ärendet.



Figur 3: Andelen klick på den inbäddade länken per dag, under simuleringens aktiva period.

2.2 Mottagare som uppgav användaruppgifter på landningssida

I det här avsnittet presenteras andelen mottagare som efter att de klickat på länken i e-postmeddelandet även uppgav användaruppgifter i form av e-postadress och lösenord på första landningssidan. Vänersborgs kommun hade i samråd med EY på förhand bestämt acceptansnivåer baserat på verksamhetens omfattning. *Tabell 4* beskriver beslutade acceptansnivåer för andelen mottagare som uppger användaruppgifter.

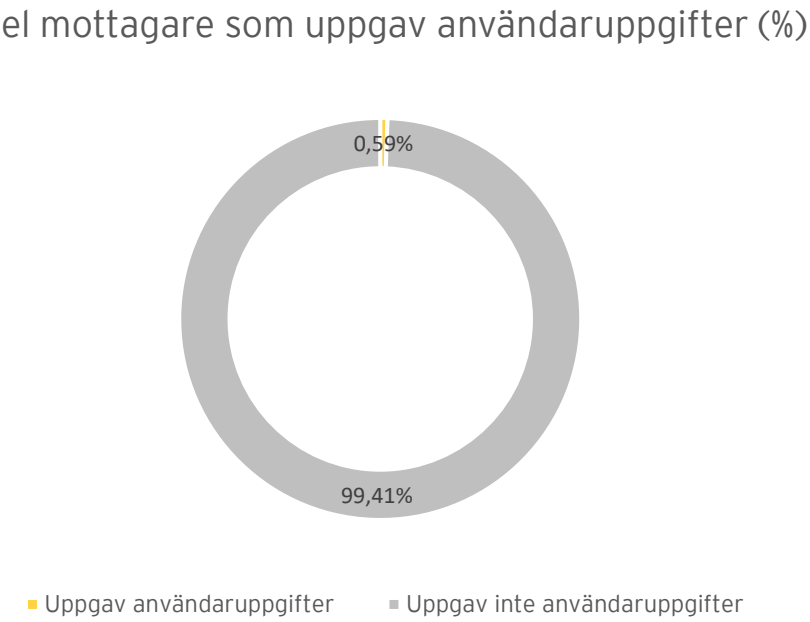
Resultatet av den simulerade attacken för kommunen som helhet visar att 27 medarbetare och förtroendevalda (0,6% av alla mottagare) uppgav sina användaruppgifter på den förfalskade landningssidan. I relation till de på förhand definierade acceptansnivåerna indikerar resultatet att Vänersborgs kommun löper en låg risk att utsättas för en fullbordad phishing-attack. Notera att acceptansnivåerna för andelen mottagare som anger användaruppgifter på landningssidan generellt sett är lägre än för andelen mottagare som klickar på länken i e-postmeddelandet. Detta då EY anser att risken för en fullbordad phishing-attack är högre om en cyberkriminell får tillgång till användardata och därmed potentiellt till kommunens IT-miljöer.

Tabell 4: Acceptansnivåer för mottagare som uppger användaruppgifter på landningssidan

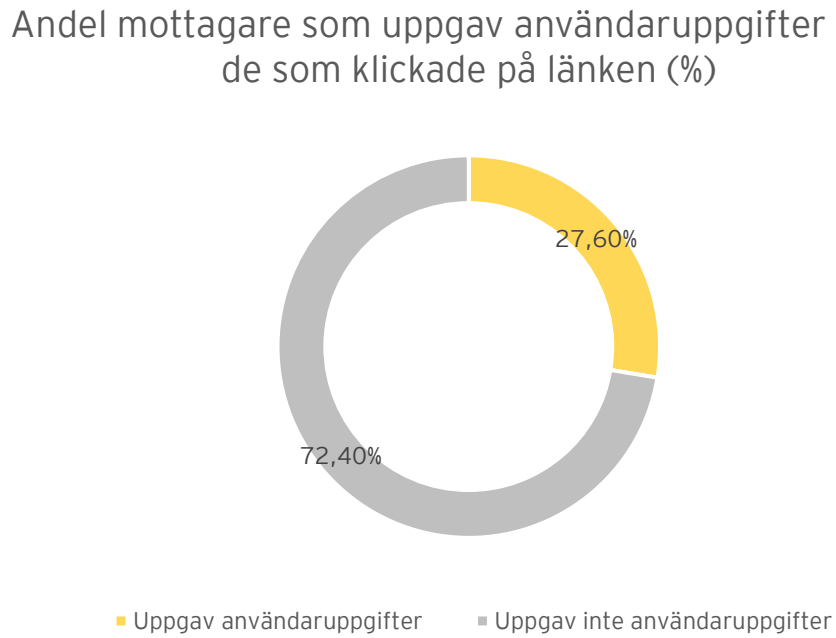
Riskanalys	Acceptansnivå (%)
Mycket hög risk	>6%
Hög risk	4-6%
Medelhög risk	2-4%
Låg risk	<2%

2.2.1 Resultat av simulering

Av det totala antalet mottagare (4613) klickade 27 medarbetare och förtroendevalda på länken samt uppgav sina användaruppgifter i form av användarnamn och lösenord på landningssidan. Det motsvarar 0,59 procent av alla mottagare, se *figur 4*. I jämförelse med acceptansnivåerna i *tabell 4*, löper därmed Vänersborgs kommun som helhet en låg risk att utsättas för en fullbordad phishing-attack.

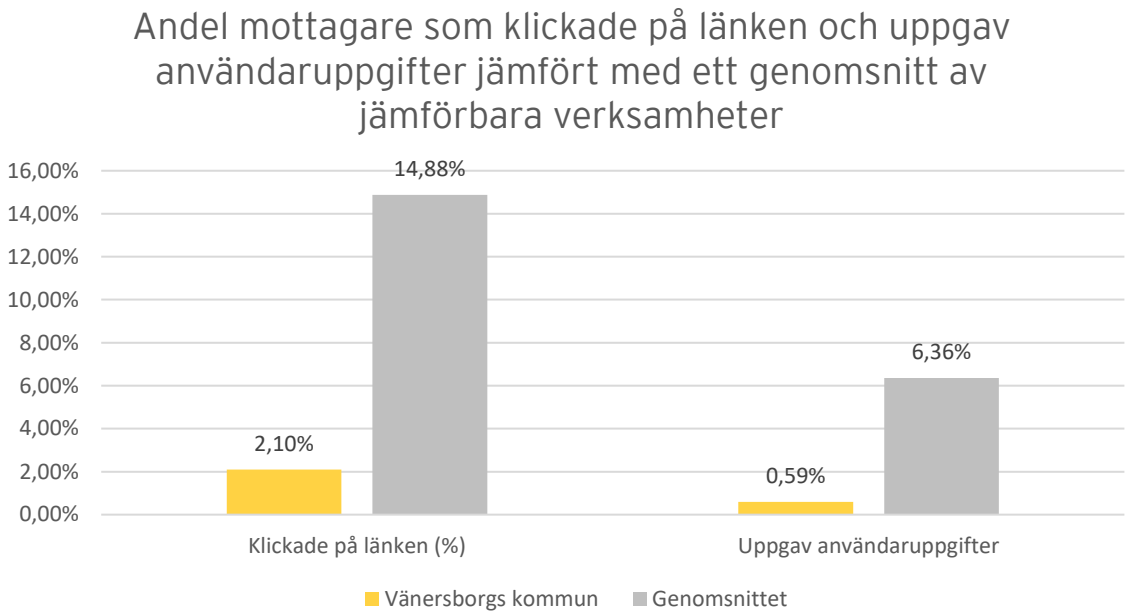


Figur 4: Fördelningen av andel mottagare som uppgav användaruppgifter på landningssidan.



Figur 5: Fördelningen av andel mottagare som uppgav användaruppgifter på landningssidan i relation till de mottagare som enbart klickade på länken.

I figur 6 visas andelen mottagare som klickade på den inbäddade länken samt andelen som uppgav användaruppgifter för Vänersborgs kommun i jämförelse med ett genomsnitt framtaget för svenska kommuner. Från denna figur ligger Vänersborgs kommun 12,78 procentenheter under genomsnittet med avseende på andelen mottagare som klickade på länken, samt 5,77 procentenheter under genomsnittet för andelen som uppgav användaruppgifter.



Figur 6: Andel mottagare som klickade på den inbäddade länken samt andel mottagare som uppgav användaruppgifter på landningssidan. I figuren jämförs Vänersborgs kommun med ett genomsnitt som baseras på testade svenska kommuner.

2.3 Mottagares medvetenhet kring informationssäkerhet och phishing

I detta avsnitt presenteras resultatet av andelen mottagare som identifierade och misstänkte det förfalskade e-postmeddelandet och som valde att rapportera till kommunen. Avsnittet presenterar även resultatet av den enkät som distribuerades efter avslutad simulering. Syftet med enkäten var att skapa en övergripande förståelse för hur medvetna de anställda i Vänersborgs kommun är kring informationssäkerhet och phishing. Enkäten inkluderade frågor inom följande två områden: 1) E-postmeddelandet som användes i övningen och vanliga indikatorer på phishing, 2) Säkerhetskulturen på kommunen i form av utbildning och medvetenhet, policy och rutiner samt rapportering av säkerhetsincidenter. Kommunen tillgängliggjorde enkäten för samtliga medarbetare och förtroendevalda som deltog i simuleringen genom att publicera denna på kommunens intranät. Samtliga chefer uppmanades att meddela sina medarbetare om enkäten. Av samtliga medarbete deltog 315 personer (6,8%) i enkätundersökningen.

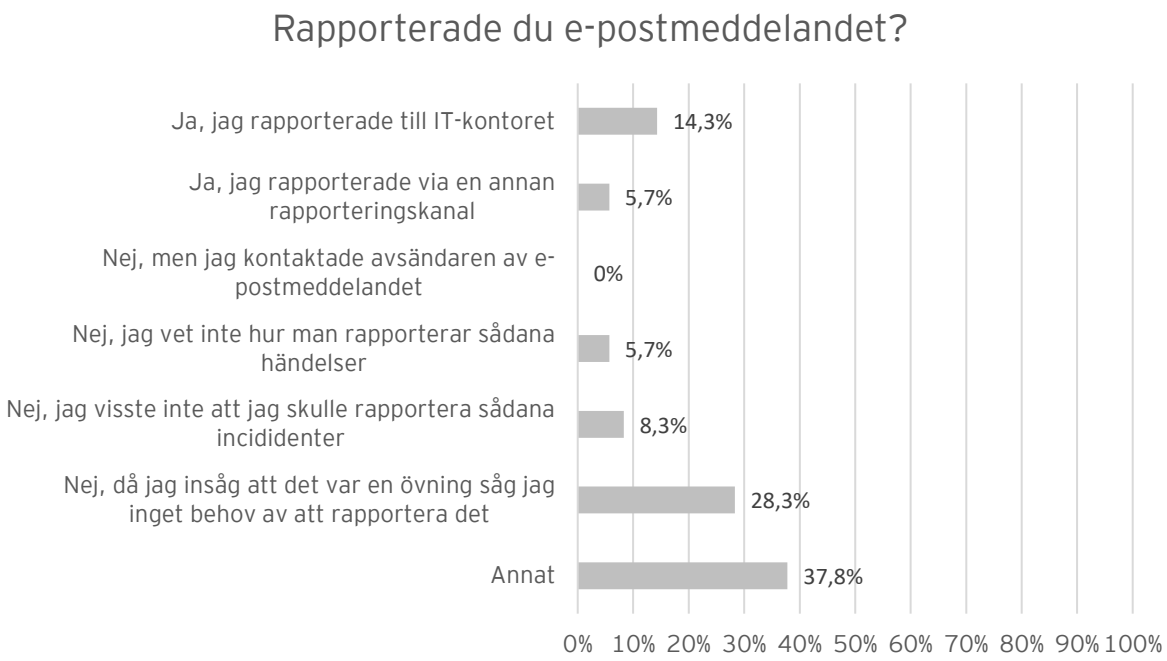
2.3.1 Rapportering

Statistik av inkomna rapporteringar som har förts av Vänersborgs kommun har beräknats på de 4613 medarbetare och förtroendevalda som totalt deltog i simuleringen. Vänersborgs kommun ombads inför simuleringen föra egen statistik över medarbetarnas tillvägagångsätt avseende rapporteringsvägar. Kommunen valde att frångå den överenskomna metoden, och kunde genom en estimering uppskatta att cirka 90 ärenden har rapporterats via telefon och e-post. Ingen ytterligare rapporteringsstatistik har förts.

2.3.2 Resultat av enkät

Figur 7 visar huruvida mottagarna valde att rapportera meddelandet eller inte, samt hur och varför. Bland de medarbetare som uppgav att de inte rapporterande e-postmeddelandet, uppgav 28,3 procent att orsaken var att de insåg att det var en övning och därmed bedömde att det inte behövde rapporteras. Vidare svarade 8,3 procent att de inte visste om att de behövde rapportera den här typen av incidenter, samtidigt som 5,7 procent svarade att de inte visste hur de skall gå till väga för att rapportera misstänkta eller falska e-postmeddelanden.

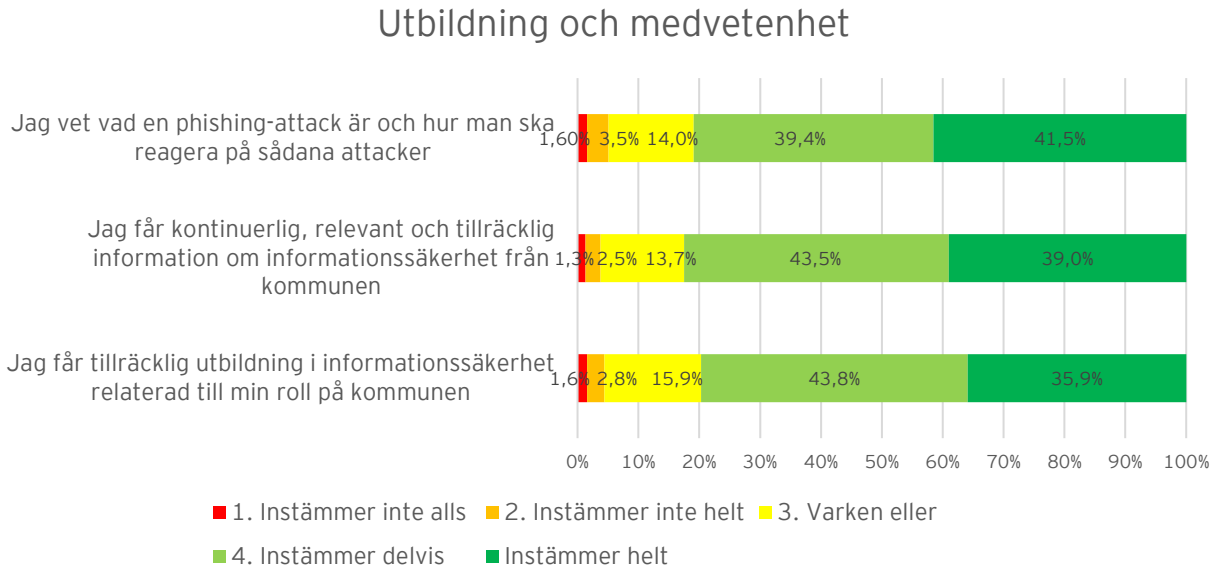
Av de som rapporterade e-postmeddelandet rapporterade 14,3 procent av medarbetarna incidenten till IT-kontoret. 5,7 procent av medarbetarna valde att rapportera incidenten via en annan rapporteringsväg.



Figur 7: Resultat av enkätfråga om mottagarnas rapportering av e-postmeddelandet och anledning bakom beslutsfattandet.

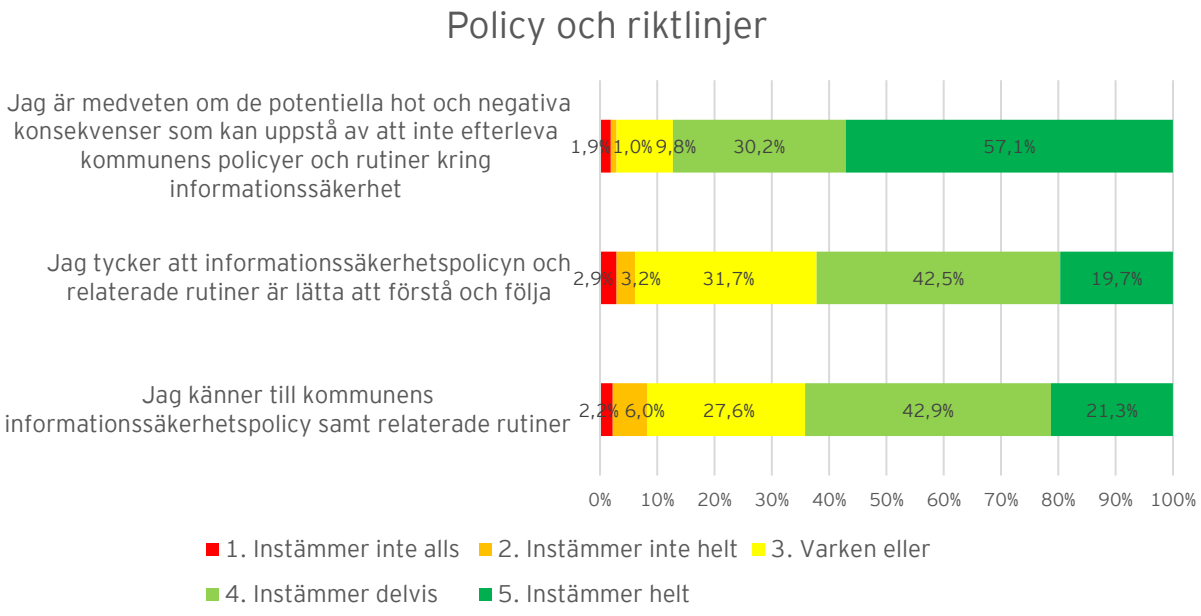
I *figur 8* visas resultatet från enkäten relaterat till medarbetarnas kunskap om vad en phishing-attack är samt hur personalen ska reagera på sådana attacker. En betydande andel (19,1%) uppger att de inte alls, inte helt instämmer eller är osäkra på vad en phishing-attack är eller hur de ska agera vid en phishing-attack.

En stor andel av medarbetarna anser även att kommunen behöver förbättras gällande att kontinuerligt tillhandahålla relevant information och tillräckligt med utbildning inom informationssäkerhet. I detta avseende är det 17,5 procent respektive 20,3 procent som anser att kommunen behöver förbättras.



Figur 8: Resultat från påstående om medarbetarnas kunskap relaterat till phishing-attacker och vikten av att rapportera dessa.

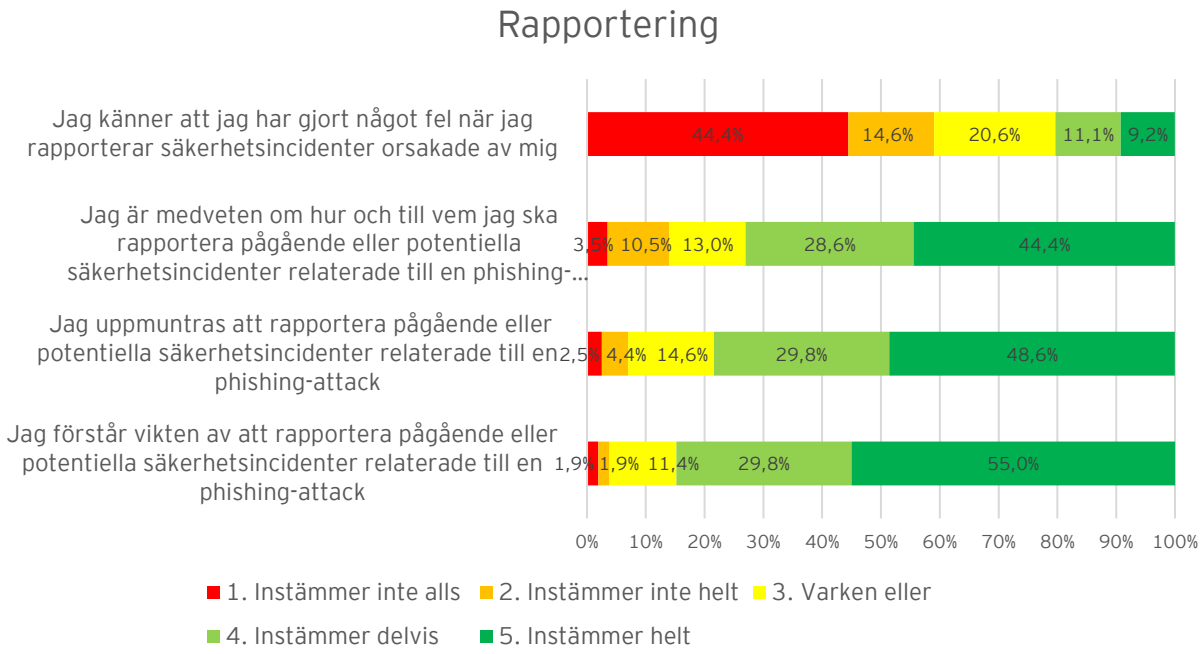
Figur 9 presenterar mottagarnas svar på frågor relaterade till kommunens styrande dokument och rutiner inom informationssäkerhet. 35,8 procent uppger att de inte instämmer eller att det finns en osäkerhet kring huruvida de känner till kommunens informationssäkerhetspolicy. 37,8 procent uppger att de inte instämmer alternativt känner sig osäkra kring huruvida gällande nämnda policy och relaterade rutiner är lätta att förstå. Enkätresultatet visar också att 12,7 procent inte alls, inte helt, alternativt varken eller instämmer i påståendet att de är medvetna om hot och konsekvenser kopplade till efterlevnad av kommunens rutiner och riktlinjer kring informationssäkerhet.



Figur 9: Resultat från påstående om styrande dokument, utbildning och rutiner inom informationssäkerhet på kommunen.

Figur 10 presenterar mottagarnas svar på frågor relaterade till rapportering. Enkätsvaren visar att 84,8 procent helt eller delvis förstår vikten av att rapportera säkerhetsincidenter. 27 procent svarar att de inte vet eller är osäkra på hur rapportering av säkerhetsincidenter ska ske.

Vidare svarar 78,4 procent att de helt eller delvis instämmer i att de uppmuntras att rapportera säkerhetsincidenter. Avslutningsvis svarar 41 procent att de varken eller, helt eller delvis instämmer i påståendet att de känner att de gjort något fel när de rapporterar självorsakade säkerhetsincidenter.



Figur 10: Resultatet från påståenden om rapportering av phishing-attacker.

2.4 Resultat från intervjuer

Baserat på information från sammanställda intervjuer framkommer att det finns förbättringsmöjligheter vad gäller samverkan mellan IT- och Juridik & Säkerhetskontoret, vilket i sin tur påverkar hanteringen av säkerhetsrelaterade frågor. En ökad interaktion och förbättrad kommunikation mellan dessa avdelningar är viktig för att stärka kommunens förmåga att effektivt hantera informationssäkerhetsfrågor.

Ansvaret för säkerhetsfrågor är uppdelat mellan IT-kontoret, som bedriver och hanterar ärenden kopplat till IT-och cybersäkerhet och Juridik & säkerhetskontoret, som arbetar med strategisk planering, utbildning och tillsyn. Av intervjuer med nyckelpersoner med insyn i kommunens säkerhetsarbete framgår att denna uppdelning upplevs ha skapat en känsla av separation mellan avdelningarna. Detta har resulterat i bristande samarbete och organisatoriska utmaningar, så som en gemensam och enhetlig syn på informationssäkerhet. Den kommunikation som sker beskrivs som oregelbunden, vilket har resulterat i en bristande och osammanhängande säkerhetsstrategi kopplat till IT-relaterade säkerhetsfrågor.

3. Övergripande rekommendationer

Baserat på den genomförda analysen har EY identifierat två övergripande rekommendationer till kommunstyrelsen. Rekommendationerna som presenteras nedan syftar till att öka kommunens motståndskraft mot framtida cyberangrepp relaterat till phishing.

3.1 Upprätta styrdokument gällande incidenthantering

Enligt EY:s ramverk för hur en organisation arbetar med informationssäkerhet styrs en organisations motståndskraft av dess medarbetares motivation och förmågor. Motivation och förmågor formas i sin tur av olika organisatoriska åtgärder såsom styrning, organisation, kommunikation, utbildning och styrdokument. För att erhålla en god motståndskraft mot cyberattacker krävs således ett övergripande, strukturerat och planlagt arbete med informationssäkerhet.

Utifrån enkätresultatet av den simulerade phishing-attacken som besvarades av 315 medarbetare inom Vänersborgs kommun, angav en relativt stor andel (73%) att de är medvetna om hur en pågående eller potentiell säkerhetsincident ska rapporteras. Trots denna grad av medvetenhet, bedömer vi att kommunstyrelsens arbete med informationssäkerhet inte är fullt ut ändamålsenligt. Detta eftersom det fortsatt är en betydande andel av kommunens medarbetare (27%) som uttrycker en osäkerhet kring hur de ska agera för att rapportera incident. Denna osäkerhet kan härledas till en avsaknad av skriftiga policyer och rutiner för rapportering. Utan dokumenterade riktlinjer är risken stor att medarbetare inte agerar korrekt vid en incident, vilket kan leda till att cyberkriminella tar sig in i kommunens IT-system och kommer åt känslig information. För att minska denna risk rekommenderar EY kommunstyrelsen att säkerställa att tydliga styrdokument tas fram och tillgängliggörs. Styrdokumenten bör omfatta incidenthantering såsom phishing, som beskriver hur IT-relaterade incidenter ska hanteras. Genom att ha dokumenterade processer kan medarbetarna känna sig trygga och mer förberedda i stressiga situationer, och kommunen kan därmed förbättra sin kapacitet att effektivt hantera och förebygga säkerhetsincidenter relaterade till phishing.

3.2 Säkerställa att det fortsatt sker övningsinsatser inom informationssäkerhet

I takt med att mängden cyberattacker mot organisationer har ökat under de senaste åren har EY noterat en markant ökning specifikt i antalet phishing-attacker. Denna trend kan delvis förklaras av förändringar i arbetsmetoder som lett till mer omfattande användning av digitala plattformar. Det är således viktigt att medarbetare som hanterar samhällsviktig information är välinformerade och har kunskap om cyberrelaterade hot för att effektivt kunna bidra till att skydda verksamheten. Sådan kunskap innefattar en förståelse för vad phishing-attacker kan innebära, metoder för att identifiera misstänkta e-postmeddelanden och vilka konsekvenser som kan uppstå till följd av en genomförd phishing-attack.

Enkätresultatet från simuleringen visar att flera medarbetare upplever osäkerhet gällande styrdokument för informationssäkerhet, hot och konsekvenser kopplade till efterlevnad av informationssäkerhet, samt vad en phishing-attack är och hur de bör agera vid en attack.

Flera medarbetare anser också att kommunen bör förbättras gällande att kontinuerligt tillhandahålla information och tillräcklig utbildning inom informationssäkerhet. Avseende rapportering svarade en övervägande majoritet av medarbetarna att de är medvetna om vikten av att rapportera och att kommunen uppmuntrar till rapportering. Trots detta var den faktiska rapporteringen under simuleringen mycket låg i förhållande till antalet mottagare av det falska e-postmeddelandet.

EY rekommenderar att kommunstyrelsen säkerställer att anställda fortsatt förses med övningsinsatser inom informationssäkerhet och kontinuerligt utvärderar om de utbildningsinsatser som tillhandahålls för medarbetarna är adekvata för att hantera aktuella säkerhetshot, såsom phishing. Detta för att ytterligare stärka beredskapen mot cyberhot och bygga en starkare säkerhetskultur.

3.3 Tillse en ändamålsenlig ansvarsfördelning och samverkanstruktur mellan IT-kontoret och Juridik & säkerhetskontoret vad gäller informationssäkerhetsfrågor

För att hantera de samverkansutmaningar som beskrivs i granskningen rekommenderar EY att kommunstyrelsen vidtar åtgärder som syftar till att förbättra den interna kommunikationen mellan IT-kontoret och Juridik & säkerhetskontoret. I detta avseende bedömer EY att en ändamålsenlig ansvarsfördelning och samverkansstruktur mellan IT-kontoret och Juridik & säkerhetskontoret behöver tydliggöras för att för att undvika missförstånd och oklarheter avseende styrning av informationssäkerhetsfrågor.

Vidare rekommenderar EY att kommunen stärker sitt samarbete för att effektivare hantera frågor inom informationssäkerhet. Kommunen behöver utveckla gemensamma mål och strategier för att skapa en enhetlig syn på informationssäkerhet inom kommunen.

4. Revisionsfrågor

Granskningen har utgått från tre revisionsfrågor. Hur väl Vänersborgs kommun svarar upp mot dessa revisionsfrågor beskrivs nedan.

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

► Hanterar Vänersborgs kommuns medarbetare hotet från attacker genom falska email, så kallad phishing (nätfiske) på ett ändamålsenligt sätt?	Vänersborgs kommuns medarbetare bedöms hantera hotet från attacker genom falska e-postmeddelanden på ett ändamålsenligt sätt. Bedömningen baseras på att Vänersborgs kommun enligt simulerad attack och förbestämda acceptansnivåer löper en låg risk att utsättas för en fullbordad phishing-attack. Simuleringen resulterade i att 98 av medarbetarna (2,1%) klickade på länken och 27 av medarbetarna (0,6%) även uppgav sina användaruppgifter. EY vill betona att det 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.	
► Har Vänersborgs kommun en incidenthanteringsprocess som aktiveras på ett ändamålsenligt sätt av de testade medarbetarna under den simulerande attacken?	EY bedömer att Vänersborgs kommun inte har en incidenthanteringsprocess som aktiveras ändamålsenligt. Trots att Vänersborgs kommun har en etablerad rutin som innebär att IT-kontoret tar kontakt med säkerhetskontoret efter att en incident upptäckts, finns det inget styrdokument som tydligt definierar hur incidenter ska hanteras av kommunens medarbetare. Baserat på den genomförda granskningen bedömer EY att Vänersborgs kommun bör arbeta för att förbättra sin motståndskraft mot phishing genom att skapa tydliga och lättillgängliga instruktioner som definierar hur medarbetarna hantera incidenter relaterade till phishing.	

▸ Är riktlinjer för hantering och rapportering av falska email och andra incidenter kända hos medarbetarna?	EY bedömer att kommunens riktlinjer för hantering av och rapportering av falska e-postmeddelanden delvis är kända hos medarbetarna. Bedömningen baseras på att Vänersborgs kommun inte har skriftliga rutiner som uppmanar eller anger hur medarbetarna ska rapportera en pågående misstänkt phishing-attack. Samtidigt som resultatet från EY:s enkätundersökning indikerar på att en relativt stor andel (27%) inte vet hur eller känner en osäkerhet hur incidenter relaterade till phishing ska rapporteras. Baserat på den genomförda granskningen bedömer EY däremot att kommunen kontinuerligt tillhandahåller övningstillfällen för att öka medarbetarnas kunskap och förståelse för phishing-attacker, vilket bidragit till ett delvis tillfredställande resultat.	

5. Slutsatser

På uppdrag av de förtroendevalda revisorerna i Vänersborgs kommun har EY genomfört en granskning av IT-säkerhet i praktiken. Granskningen har syftat till att bedöma om det finns brister i det praktiska arbetet med IT- och informationssäkerhet inom området phishing. Detta har genomförts genom att testa medarbetarnas medvetenhet och kunskap inom området, bland annat genom att simulera ett angrepp via e-post. För att effektivt genomföra ett test av personalens agerande har en del av kommunens tekniska skydd mot phishing-attacker kopplats bort – syftet har inte varit att testa tekniken.

Resultatet av genomförd simulerad phishing-attack visar att Vänersborgs kommun som helhet löper en låg risk att utsättas för en fullbordad phishing-attack. Trots att kommunen återkommande genomför övningsinsatser inom informationssäkerhet, bedömer EY att det finns ett fortsatt behov av att öka medarbetarnas medvetenhet kring hur ett falskt e-postmeddelande kan se ut. EY bedömer även att det är viktigt att tydliggöra hur, och till vem, pågående eller potentiella säkerhetsincidenter relaterade till en phishing-attack ska rapporteras. Denna bedömning grundar sig i att 98 medarbetare (2,1 %) klickade på länken samt att 27 medarbetare uppgav sina användaruppgifter. Kommunen valde att på eget initiativ på förhand publicera information om e-postutskicket på intranätet vilket kan ha påverkat övningens resultat. EY vill betona att det 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.

Enkätresultatet indikerar på att 27 procent av deltagarna inte vet hur, eller känner sig osäkra på, hur phishing ska rapporteras. Det kan härledas till en avsaknad av skriftliga policyer och rutiner för rapportering. Därtill visar genomförda intervjuer att det finns förbättringsåtgärder vad gäller samverkan inom informationssäkerhetsfrågor mellan IT-kontoret och Juridik & säkerhetskontoret. Vilket är en konsekvens av uppdelade ansvarsområden.

Kommunstyrelsen rekommenderas därför att vidta åtgärder för att förbättra motståndskraften mot phishing och således minska risken för fullbordade phishing-attacker. Baserat på granskningen lämnar EY tre övergripande 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.

Stockholm, 2024-11-07

Helena Törnqvist
Kvalitetssäkrare IT

Bilaga 1: Genomförandebeskrivning

1.1 Genomförande

Övningen har utformats och genomförts av specialister inom IT- och informationssäkerhet från EY tillsammans med utvalda representanter från Vänersborgs kommun. De utvalda representanterna från kommunen har givits möjlighet att faktagranska rapporten i syfte att säkerställa att slutsatser grundar sig i korrekta fakta. Nedan följer en ingående beskrivning av respektive huvudmoment för att förbereda, utföra och analysera den simulerade attacken.

1.2 E-postmeddelande och landningssida

En simulerad phishing-attack bygger på att ett e-postmeddelande skickas ut till en utvald målgrupp. E-postmeddelandet kan vara utformat på olika sätt beroende på övningens syfte. Det kan exempelvis innehålla en länk som leder vidare till en landningssida eller inkludera en länk som initierar en nerladdning av en fil. E-postmeddelanden som inkluderar en länk till en landningssida testar vanligtvis hur villiga medarbetarna är att dela med sig av användaruppgifter, som exempelvis inloggningsuppgifter eller att ladda ner okända filer.

För att bestämma hur e-postmeddelandet skulle utformas hölls inledningsvis möten tillsammans med representanter från kommunen, där det beslutades att inkludera en länk i e-postmeddelandet som hänvisade till en landningssida. Det aktuella meddelandet uppgavs vara skickat från Vänersborgs kommuns Servicedesk och skickades från en e-postadress med domänen "vanerborg.se", vilket är en domän som inte tillhör Vänersborgs kommun. I e-postmeddelandet fick mottagaren information om att kvotgränsen för inkorgen överskridits, och att e-post inte kunde skickas eller tas emot innan utrymmet i inkorgen ökats. Mottagaren blev därefter uppmanad till att trycka på en inbäddad länk för att lägga till mer utrymme till sitt konto. Genom att följa länken i e-postmeddelandet landade besökaren på den förfalskade landningssidan där de ombads att logga in med ett Microsoft 365-konto (e-postadress och lösenord). Om en mottagare valde att fylla i sina användaruppgifter på landningssidan, skickades de vidare till ytterligare en landningssida som informerade mottagaren att de deltagit i en simulerad phishing-attack. Syftet med den informerande landningssidan är att skapa medvetenhet om informationssäkerhet i organisationen och informera om hotet av phishing. För e-postmeddelandet som skickades ut och de båda landningssidorna, *se bilaga 2 och landningssida 1 och 2*.

1.3 Målgrupp och utskick

Målgruppen för en simulerad phishing-attack kan variera beroende på övningens syfte. E-postmeddelandet kan exempelvis vara riktat mot utvalda avdelningar inom kommunen baserat på deras risk att bli utsatt för en fullbordad phishing-attack (risknivåer): Se avsnitt *1.4.2.5 Risknivåer och acceptansnivåer* för vidare förklaring av hur risknivåer kan definieras vid en phishing-attack. E-postmeddelandet kan också skickas ut till samtliga anställda för att på så sätt skaffa sig en övergripande bild av kommunens motståndskraft och medarbetarnas medvetenhet. I samråd med Vänersborgs kommuns representanter beslutades det att samtliga av kommunens medarbetare och förtroendevalda skulle delta i

simuleringen. Detta resulterade i att 4613 medarbetare och förtroendevalda deltog i övningen.

Innan det faktiska e-postmeddelandet skickades ut hölls testmöten där den simulerade attacken testades för att säkerställa att e-postmeddelandet gick igenom skalskyddet och skulle nå fram till mottagarna. Den tekniska genomgången inkluderade behov av vitlistning, spamfilter och potentiell rate limiting[1]. Detta innebär att kommunens tekniska skydd mot phishing kopplas bort, i syfte att på ett kostnadseffektivt sätt testa personalen och inte tekniken. Det bör noteras att inget tekniskt skydd fullständigt kan förhindra ett angrepp via phishing. EY genomförde simuleringen under vecka 38, 2024. Kommunens IT-kontor beslutade att följa interna riktlinjer och publicerade på eget initiativ information om simuleringen under dess första dag, vilket kan ha minskat antalet personer som klickade på länken och således påverkat övningens resultat.

1.4 Rapportering

Att skydda sig mot hotet från en phishing-attack kan vara svårt och kräver en fungerande samverkan mellan flera olika faktorer. En viktig komponent är att effektiva rapporteringsvägar existerar och att medarbetarna är medvetna om hur dessa ska användas. Det är också av stor vikt att personer som misstänker att de blivit utsatta för angrepp vidtar nödvändiga åtgärder för att ändra inloggningsuppgifter som en angripare kan ha fått tillgång till. Åtgärder mot phishing-attacken bör vidtas skyndsamt då hotet är som störst under den initiala tiden efter att e-postmeddelandet mottagits.

Vänersborgs kommun har tagit fram riktlinjer avseende informationssäkerhet. Detta dokument ger en övergripande beskrivning av kommunens arbete för att hantera och skydda information, vilket inkluderar att försäkra att adekvat kunskap upprätthålls genom övning och utbildning bland kommunens medarbetare. Det saknas dock konkreta anvisningar för hur medarbetarna i Vänersborgs kommun ska identifiera, hantera och rapportera cyberrelaterade säkerhetshot, så som falska eller misstänkta e-postmeddelanden. Däremot uppger intervjuande nyckelpersoner att kommunen publicerar nyheter på det interna intranätet med uppmaningar om att medarbetare ska vara vaksamma på misstänkta e-postmeddelanden samt rapportera dessa.

1.5 Enkät

Efter avslutad simulering distribuerades en enkät via kommunen till mottagarna av det förfalskade e-postmeddelandet. Enkäten utformades av EY och syftet var att skapa en förståelse för motivationen och förmågan hos kommunens anställda att identifiera ett falskt e-postmeddelande. Därutöver var syftet att undersöka om medarbetarna känner till befintliga riktlinjer, utbildningsmöjligheter och rapporteringsvägar. Kommunen tillgängliggjorde enkäten för samtliga av kommunens medarbetare som deltog i simuleringen. Samtliga chefer uppmanades även att meddela sina medarbetare om enkäten. Se *bilaga 4* för enkäten som användes i samband med övningen.

[1] För förklaring av begreppen, se definitioner i *bilaga 6*.

1.6 Risknivåer och acceptansnivåer

För att tolka resultaten av en simulerad phishing-attack krävs en förståelse för potentiella risker av en fullbordad attack (risknivåer) och mottagarens relativa benägenhet att acceptera riskerna (acceptansnivåer). Risken för en fullbordad attack kan exempelvis vara mer omfattande för en större kommun som besitter mer känslig information och större finansiell kraft. Det kan också vara skillnader inom en kommun där riskerna för vissa sektorer kan vara mindre än för andra beroende på typen av verksamhet. Se *bilaga 3* för definitioner av risknivåer som EY har använt under genomförd granskning.

Tabell 1: Risknivåer för phishing-övning

Mycket hög risk	En mycket hög risk för, och i samband med, en phishing-attack existerar. Kommunen rekommenderas att omgående vidta nödvändiga åtgärder för att minimera svagheter i motståndskraften mot phishing-attacker. Detta för att undvika finansiella förluster, negativt rykte eller andra betydande konsekvenser.
Hög risk	En hög risk för, och i samband med, en phishing-attack existerar. Kommunen rekommenderas att vidta åtgärder för att utvärdera och åtgärda svagheter i motståndskraften mot phishing-attacker. Detta för att undvika finansiella förluster, negativt rykte eller andra betydande konsekvenser.
Medelhög risk	En medelhög risk för, och i samband med, en phishing-attack existerar. Kommunen rekommenderas att utvärdera och förbättra motståndskraften mot phishing-attacker. Detta för att undvika finansiella förluster, negativt rykte eller andra betydande konsekvenser.
Låg risk	En låg risk för, och i samband med, en phishing-attack existerar. Kommunen rekommenderas att arbeta vidare med att kontinuerligt säkerställa en hög motståndskraft mot phishing-attacker. Detta för att undvika finansiella förluster, negativt rykte eller andra betydande konsekvenser.

Innan en simulerad phishing-attack påbörjas är det viktigt att översätta de olika risknivåerna till specifika mätetal anpassade för den aktuella organisationen, vilket kallas för acceptansnivåer. För den simulerade övningen definierades acceptansnivåer i samråd mellan EY och Vänersborgs kommuns representant genom att omvandla risknivåerna till specifika procentandelar, se *bilaga 3*.

1.7 Tidsplan

Granskningen gemofördes från augusti 2024 till november 2024, se *tabell 2* nedan för granskningens tidplan.

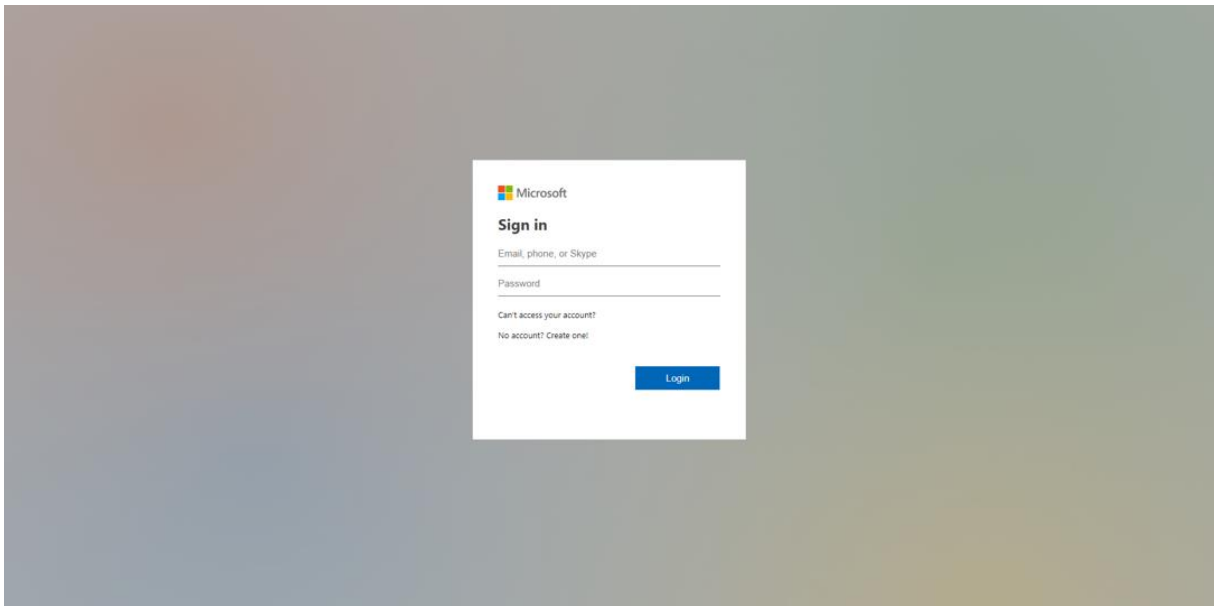
Tabell 2: Tidsplan

Förberedelser och planering	Augusti 2024
Test och utskick	September 2024
Rapportskrivning och intern kvalitetssäkring	Oktober 2024
Justering och färdigställande av rapport	Oktober 2024
Avrapportering och slutpresentation	November 2024

Bilaga 2: E-postmeddelande

Bilaga 3: Landningssida

Landningssida 1



Landningssida 2

Vänersborgs kommun

OBS! Detta e-postmeddelande var ett phishing-mail.

Det här är en simulering för att stärka motståndskraften inom Vänersborgs kommun för att kunna stå emot cyberattacker genom phishing (svenska: nätfiske).

Denna övning är beställd av kommunens förtroendevalda revisorer och genomfördes i samarbete med EY som en del av Vänersborgs kommuns fortsatta arbete med informationssäkerhet. Vi hoppas med den här övningen fortsätta utveckla medvetenheten av potentiella cyberattacker hos oss på Vänersborgs kommun.

Bedrägerier i form av social manipulation som phishing är ett växande problem, och ett förfalskat e-postmeddelande kan vara svårt att upptäcka. Vänligen se tipsen nedan som hjälp för att i framtiden lyckas känna igen denna typ av e-postmeddelanden på arbetsplatsen och även i privata sammanhang.

Den användarinformation du har angett är anonymiserad och kommer att raderas. Det är endast aggregerad statistik som kommer samlas in.

Vi vill bedöma anställdas grad av försiktighet och medvetenhet gällande phishing och uppskattar därför om du inte diskuterar detta e-postmeddelande med kollegor eller informerar dem om övningen.

Stanna upp, se efter och tänk till!

Finns det något i e-postmeddelandet som var ovanligt? Bedragare utnyttjar ofta stressiga situationer för att få oss att agera hastigt. Var särskilt kritisk till e-postmeddelanden som uppmanar dig att kringgå vanliga procedurer och/eller agera snabbt. Är det troligt att du skulle få den här typen av e-postmeddelande utan någon tidigare information från din arbetsgivare?

Om du misstänker att du har utsatts för phishing, kontakta genast IT-kontoret på Vänersborgs kommun.

1. Kontrollera avsändare

Om du misstänker att ett e-postmeddelande inte är äkta, tänk på att vara kritisk till innehållet och leta efter saker som inte stämmer. Domänen @vanerborg.se vilket e-postmeddelandet skickades från, är inte en domän som Vänersborgs kommun använder utan en så kallad bluffdomän. Dessa är gjorda så att man vid första anblick inte ska misstänka att någonting är fel.

2. Kontrollera språket

Håll utkik efter stavfel. Seriösa e-postmeddelanden innehåller oftast inte stavfel och brukar inte vara skrivna på dålig svenska. Men, det är viktigt att förstå att cyberkriminella även kan använda sig av mer sofistikerade metoder. Notera att dessa typer av e-postmeddelanden kan vara välformulerade.

3. Kontrollera länkar

Klicka aldrig på länkar inbäddade i e-postmeddelanden om du misstänker att någonting inte stämmer, eller om du inte förväntar dig att få liknande e-postmeddelanden.

Bilaga 4: Acceptansnivåer

	Mycket hög risk	Hög risk	Medelhög risk	Låg risk
Andel mottagare som klickar på länken i e-postmeddelandet	>15%	10-15%	5-10%	<5%
Andel mottagare som uppger användaruppgifter på landningssidan	>6%	4-6%	2-4%	<2%

Bilaga 5: Enkätfrågor

1. Vad var anledningen till att du klickade på länken?

- ☐ Jag tyckte att e-postmeddelande såg trovärdigt ut
- ☐ Jag visste inte att det var fel att trycka på en länk i ett e-postmeddelande
- ☐ Jag kände mig stressad att agera
- ☐ Jag klickade inte på länken
- ☐ Annat

_____

2. När insåg du att det här e-postmeddelandet var "phishing"?

- ☐ När jag såg e-postmeddelandet
- ☐ När jag klickat på länken
- ☐ När jag hade lämnat mina uppgifter och såg informationen om övningen
- ☐ När jag blev varnad om att e-postmeddelandet var falskt, exempelvis från en kollega eller någon annan.
- ☐ Annat

_____

3. Rapporterade du e-postmeddelandet?

- ☐ Ja, jag rapporterade till IT-kontoret
- ☐ Ja, jag rapporterade via en annan rapporteringskanal
- ☐ Nej, men jag kontaktade avsändaren av e-postmeddelandet
- ☐ Nej, jag vet inte hur man rapporterar sådana händelser
- ☐ Nej, jag visste inte att jag skulle rapportera sådana incidenter
- ☐ Nej, då jag insåg att det var en övning såg jag inget behov av att rapportera det
- ☐ Annat
- ☐ (Infoga fritext)

_____

Frågor om säkerhetskulturen
Frågorna om säkerhetskultur delas upp i tre underområden: 1) Utbildning och medvetenhet, 2) Policy och rutiner, och 3) Rapportering. Följande frågor besvaras på en skala enligt nedan:

1. Instämmer inte alls
2.
3.
4.
5. Instämmer helt

Utbildning och medvetenhet

4. Jag får tillräcklig utbildning i informationssäkerhet relaterad till min roll på kommunen

☐ 1. Instämmer inte alls

☐ 2.

☐ 3.

☐ 4.

☐ 5. Instämmer helt

5. Jag får kontinuerlig, relevant och tillräcklig information om informationssäkerhet från kommunen

☐ 1. Instämmer inte alls

☐ 2.

☐ 3.

☐ 4.

☐ 5. Instämmer helt

6. Jag vet vad en phishing-attack är och hur jag ska reagera på sådana attacker

☐ 1. Instämmer inte alls

☐ 2.

☐ 3.

☐ 4.

☐ 5. Instämmer helt

Policy och riktlinjer

7. Jag känner till kommunens informationssäkerhetspolicy samt relaterade instruktioner på Intranätet

- ☐ 1. Instämmer inte alls
- ☐ 2.
- ☐ 3.
- ☐ 4.
- ☐ 5. Instämmer helt

8. Jag tycker att informationssäkerhetspolicyn och relaterade instruktioner på Intranätet är lätta att förstå och följa

- ☐ 1. Instämmer inte alls
- ☐ 2.
- ☐ 3.
- ☐ 4.
- ☐ 5. Instämmer helt

9. Jag är medveten om de potentiella hot och negativa konsekvenser som kan uppstå av att inte efterleva kommunens policys och instruktioner kring informationssäkerhet.

- ☐ 1. Instämmer inte alls
- ☐ 2.
- ☐ 3.
- ☐ 4.
- ☐ 5. Instämmer helt

Rapportering

10. Jag förstår vikten av att rapportera pågående eller potentiella säkerhetsincidenter relaterade till en phishing-attack

- [ ] 1. Instämmer inte alls
- [ ] 2.
- [ ] 3.
- [ ] 4.
- [ ] 5. Instämmer helt

11. Jag uppmuntras att rapportera pågående eller potentiella säkerhetsincidenter relaterade till en phishing-attack

- [ ] 1. Instämmer inte alls
- [ ] 2.
- [ ] 3.
- [ ] 4.
- [ ] 5. Instämmer helt

12. Jag är medveten om hur och till vem jag ska rapportera pågående eller potentiella säkerhetsincidenter relaterade till en phishing-attack

- [ ] 1. Instämmer inte alls
- [ ] 2.
- [ ] 3.
- [ ] 4.
- [ ] 5. Instämmer helt

13. Jag känner att jag har gjort något fel när jag rapporterar säkerhetsincidenter orsakade av mig.

- [ ] 1. Instämmer inte alls
- [ ] 2.
- [ ] 3.

☐ 4.

☐ 5. Instämmer helt

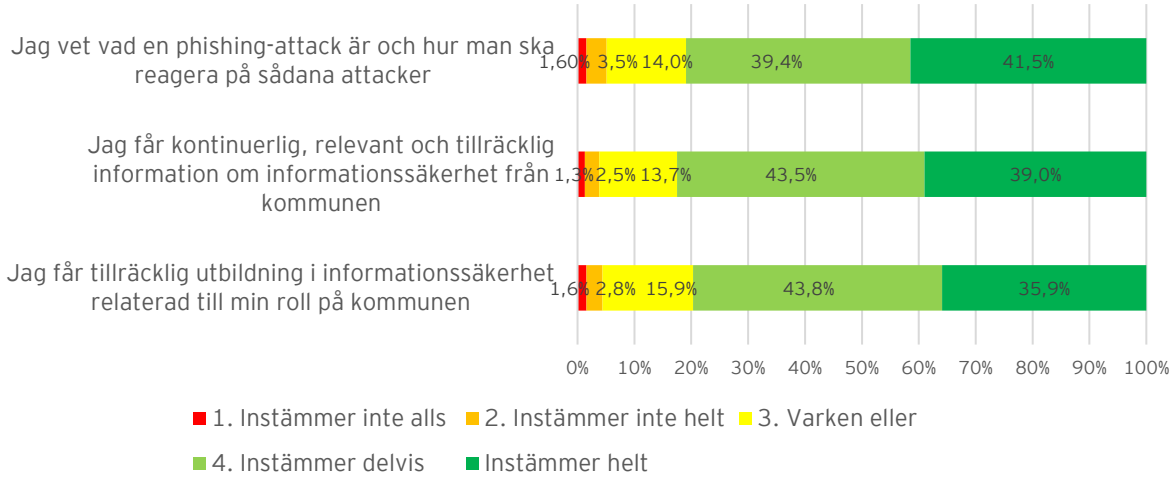
14. Övrigt

Vill du lägga till övrig information kan du göra det nedan.

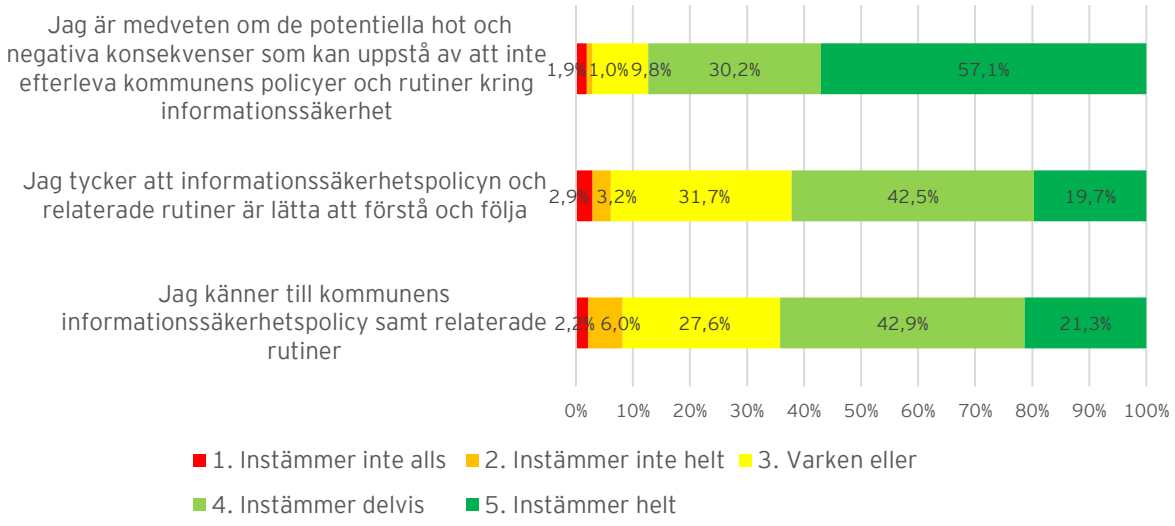
- (Infoga fritextruta)

Bilaga 6: Enkätresultat

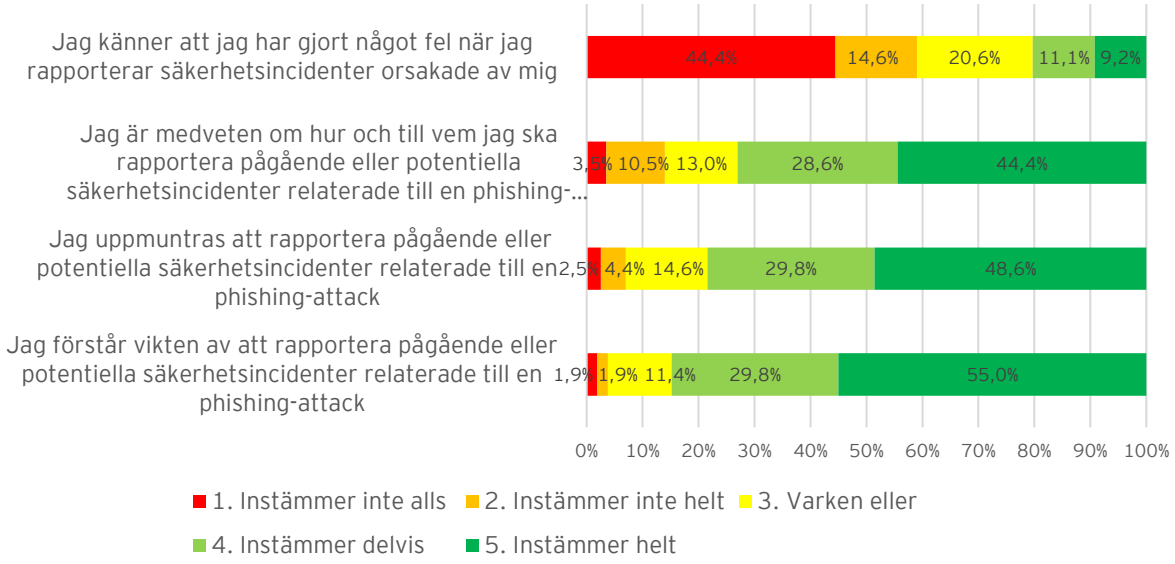
Utbildning och medvetenhet



Policy och riktlinjer



Rapportering



Bilaga 7: Definitioner

Acceptansnivåer: Acceptansnivåer är ett sätt att översätta generella och övergripande risknivåer till aktuella mätetal som går att följa upp och agera på. Acceptansnivåer bör utgå från organisationens eller företagets kontext, dvs. risknivåer och riskaptit.

Cyberattack: En cyberattack är ett samlingsnamn för olika typer av brott som utförs på IT-system. Attackerna kan utföras för att få tillgång till hemlig information, begränsa tillgången till IT-systemen, samt förstöra data eller IT-system.

Domän: Domän, även kallat domännamn, är en beskrivning av ett namn eller en adress på internet. Vanliga exempel på domännamn är det man skriver in i en webbläsare för att komma till en internetsida eller det som kommer efter "@" i en mailadress, exempelvis "google.com" eller "svt.se".

Falsk avsändare: En falsk avsändare är en avsändare som utger sig för att vara någon den inte är, exempelvis genom att imitera kända e-postadresser eller andra avsändare.

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 phishing-attacker då det ökar mottagarnas benägenhet att trycka på länken.

Intranät: Till skillnad från internet som är tillgängligt för alla är ett intranät ofta privat och bara tillgängligt för den organisation eller företag som äger det. Ett intranät är vanligtvis skyddad från omvärlden av en brandvägg och kan bestå av många sammankopplade lokala nätverk.

Landningssida: En landningssida är en internetsida dit en användare hänvisas efter att exempelvis ha tryckt på en länk eller någon annan form av uppmaning.

Phishing: Phishing, på svenska kallat nätfiske, är en metod för cyberkriminella att attackera privatpersoner, företag och organisationer. Metoden går att utforma på olika sätt men går generellt sätt 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 av phishing-attacker är att utvinna konfidentiell information eller att implementera skadlig kod.

Rate limiting: Rate limiting är en engelsk term som beskriver en inbyggd kontroll som existerar i olika e-postklienter, exempelvis Outlook. Kontrollen begränsar antalet e-postmeddelanden som kan tas emot samtidigt för att förhindra en eventuell överbelastning.

Spamfilter: Spamfilter, även kallat skräppostfilter, är en inbyggd kontroll som existerar i olika e-postklienter, exempelvis Outlook. Kontrollen sorterar alla e-postmeddelanden som en mottagare tar emot och filtrerar ut de e-postmeddelanden som troligtvis är skräppost.

Vitlistning: Vitlistning är en metod företag och organisationer använder för att kontrollera e-posttrafiken. Detta genom att på förhand definiera vilka e-postadresser som är godkända (vitlistade) och på så sätt tillåta kommunikationen.