Höganäs kommun

Rapport: Informationssäkerhet i praktiken
November 2021

Sammanfattning

På uppdrag av Höganäs kommuns förtroendevalda revisorer har EY genomfört en granskning för att testa hur väl kommunens arbete med IT- och informationssäkerhet har kommunicerats till medarbetarna i praktiken, exempelvis genom utbildningar och instruktioner. Syftet med granskningen har varit att bedöma om det finns brister i det praktiska arbetet med IT- och informationssäkerhet inom Höganäs kommun. Detta genom att bedöma i vilken utsträckning en angripare riskerar att komma åt Höganäs kommuns IT-miljöer genom angrepp via e-post. De följande revisionsfrågorna har legat till grund för granskningen:

- Hur väl hanterar kommunens medarbetare hotet från attacker genom falska e-postmeddelanden, så kallad phishing?
- Hur kan Höganäs kommuns säkerhetsarbete kopplat till attacker med falska e-postmeddelanden utvecklas?

Granskningen genomfördes mellan maj 2021 till november 2021 och baserades på en simulerad attack via e-post, där medarbetare riskerar att luras lämna ut information till en falsk avsändare, en så kallad phishingattack. Granskningen utformades och utfördes av EY tillsammans med representanter från kommunen. Metoden bygger på EY:s etablerade ramverk över hur en organisation arbetar med informationssäkerhet, samt EY:s beprövade metodik för att genomföra en simulerad phishingattack. Resultaten analyserades i tre huvudområden: 1) Mottagare som klickat på länken i e-postmeddelandet, 2) Mottagare som uppgav användarinformation på landningssidan, samt 3) Mottagare som rapporterade e-postmeddelandet. Dessa områden jämfördes sedan mot på förhand definierade acceptansnivåer, samt med vad EY anser är en godtagbar standard i offentlig sektor.

Baserat på genomförd analys bedömer EY att Höganäs kommun ligger på en nivå något under det EY anser att man kan förvänta sig utav kommunen. Slutsatsen baseras på den typ av verksamhet som bedrivs samt på känslighetsgraden av den information, exempelvis personuppgifter, som kommunen behandlar i dess dagliga verksamhet. EY noterar att kommunen själva har definierat striktare acceptansnivåer, vilket gör att man enligt den egna definitionen löper en mycket hög risk att utsättas för phishingattacker. Kommunen rekommenderas att vidta åtgärder för att stärka utbildning och medvetenheten hos personalen, samt åtgärda svagheter i motståndskraften mot phishingattacker. Detta för att undvika förluster av känslig information, negativt rykte eller andra betydande konsekvenser.

Baserat på resultatet av granskningen har EY valt att presentera tre övergripande rekommendationer som Höganäs kommun bör fokusera sitt arbete på framöver:

- Utveckla ett strukturerat och regelbundet arbete med informationssäkerhetsutbildningar, särskilt fokuserat på de delar av organisationen som kan vara målgrupper för phishingattacker.
- Genomföra både teoretiska samt praktiska övningar inom phishing.
- Vidareutveckla sina befintliga rapporteringsvägar, samt kommunicerar vikten av att rapportera säkerhetsincidenter till alla medarbetare.

Innehållsförteckning

1. Bakgrund

Höganäs kommun, inklusive dess nämnder och förvaltningar, behandlar stora mängder digital information. Detta skapar 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 inom organisationen krävs det att styrning och dagligt arbete bedrivs på ett sådant sätt att informationen är tillgänglig, riktig, har tillräckligt starkt skydd samt är spårbar.

I tidigare granskningar har kommunens revisorer identifierat risker relaterat till kommunens övergripande arbete med IT- och informationssäkerhet, samt sårbarheter kopplat till verksamhetskritiska system inom kommunen. Revisorerna har därför valt att genomföra en granskning för att testa hur väl kommunens arbete med IT- och informationssäkerhet har kommunicerats till medarbetarna i praktiken.

En sådan granskning genomförs genom att EY simulerar en cyberattack där falska e-postmeddelanden skickas ut till medarbetarna, en så kallad phishingattack (svenska: nätfiske). Genom ett fullgott informationssäkerhetsarbete bör medarbetarna kunna identifiera ett sådant angrepp och veta hur de ska agera för att hantera och rapportera ett misstänksamt e-postmeddelande med bibehållen säkerhet. Genom att analysera hur många mottagare av e-postmeddelande som agerade korrekt kan revisorerna få en bild av hur väl utbildning och medvetenhet fungerar i praktiken inom kommunen.

1.1 Phishing

Digitalisering leder till en ökad risk relaterad till informationssäkerhet. Cyberkriminella aktörer väljer i en hög utsträckning att inte enbart attackera teknologin i en organisation, utan även människorna i den. Cyberkriminella utför social manipulation genom att utnyttja mänskliga svagheter som rädsla och förtroende för att utvinna känslig information som är viktig att skydda, eller för att sprida skadlig kod som kan tillfoga en organisation, dess intressenter, samt samhället stor förstörelse. Under den osäkra situationen av COVID-19 har EY sett en ökning av denna typ av cyberkriminalitet, särskilt genom phishing. Detta innebär att den mänskliga aspekten blir avgörande för att säkerställa ett adekvat skydd av en organisations tillgångar, samt för att uppfylla gällande lagkrav om informationssäkerhet och integritet.

En fullbordad attack av phishing kan innebära stora konsekvenser för en organisation, både finansiellt, men även sociala konsekvenser som ett försämrat anseende och rykte. Det är därmed viktigt att vara proaktiv och bekämpa det ökade hotet av phishing. Risken för en fullbordad attack av phishing reduceras om medarbetare inom en organisation är medvetna om hotet av phishing, har kunskapen att kunna identifiera indikationer av ett falskt e-postmeddelande med fientligt uppsåt, samt har en tydlig rapporteringsväg att följa för att rapportera eventuellt misstänkta e-postmeddelanden. Att kontinuerligt genomföra medvetenhetsträning inom informationssäkerhet för att medarbetare ska upptäcka samt reagera på hotet från phishing är ett alternativ för att mitigera riskerna från denna typ av cyberattacker.

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 utbildning och medvetenhet hos medarbetare inom kommunen. Vidare är syftet också att bedöma i vilken utsträckning en angripare riskerar att komma åt Höganäs kommuns IT-miljöer genom angrepp via e-post. De följande revisionsfrågorna har legat till grund för granskningen:

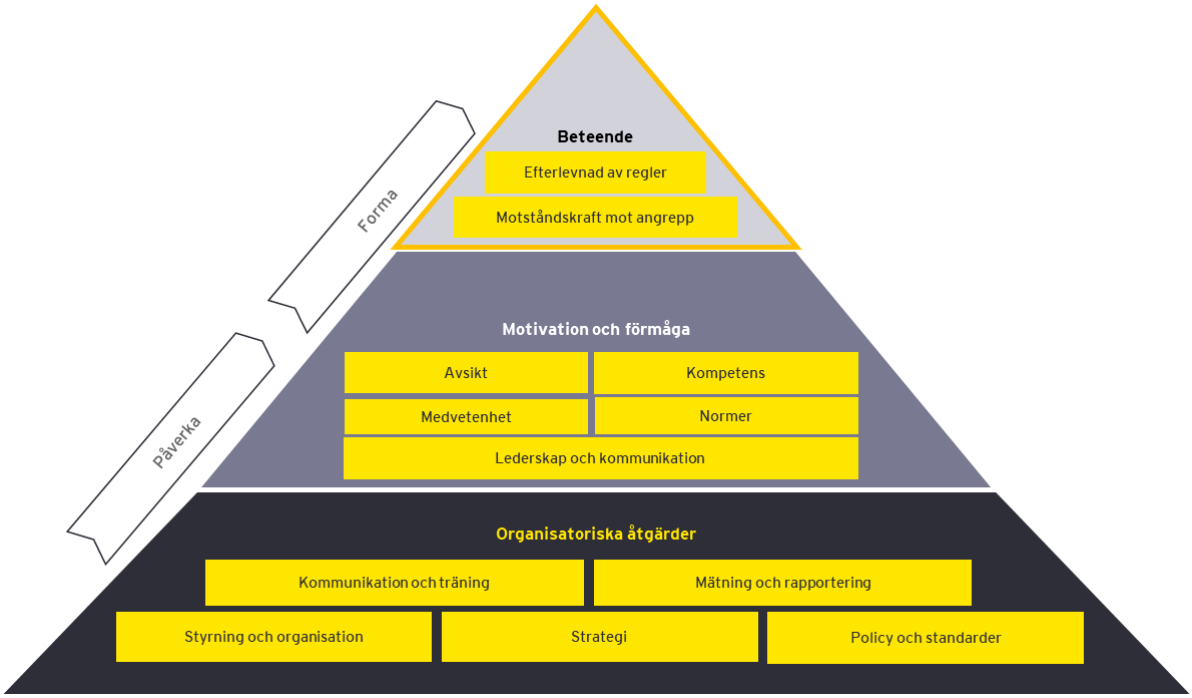
- Hur väl hanterar kommunens medarbetare hotet från attacker genom falska e-postmeddelanden, så kallad phishing?
- Hur kan Höganäs kommuns säkerhetsarbete kopplat till attacker med falska e-postmeddelanden förbättras?

1.3 Avgränsningar

Granskningen är avgränsad till att ge en bild över hur sårbar kommunen är för attacker riktade mot personalen via e-post. Det ges alltså inte någon helhetsbild av kommunens totala arbete inom IT- och informationssäkerhet utan syftet är ge en mer detaljerad bild av ett begränsat område. Ingen teknisk testning har heller utförts för att granska effektiviteten i kommunens skalskydd, dvs. hur väl existerade och inbyggda säkerhetskontroller fungerar för att identifiera och stoppas illvilliga e-postmeddelanden.

1.4 Metod och genomförande

Granskningen bygger på EY:s etablerade ramverk för hur en organisation arbetar med informationssäkerhet. *Figur 1* nedan visar hur arbetstagarens motivation och förmåga att uppfylla kraven påverkas av genomförda organisatoriska åtgärder. Detta formar i sin tur den enskilda medarbetarens efterlevnad av regler, samt motståndskraft mot angrepp.



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

Den genomförda granskningen har fokuserat på att analysera beteendet hos kommunens medarbetare genom att utföra en simulerad phishingövning. Övningen testar således främst kommunens, samt de anställdas, motståndskraft mot denna typ av angrepp. Nedan följer en mer detaljerad beskrivning av EY:s metodik för att utföra en phishingövning samt en detaljerad beskrivning av hur övningen genomfördes.

1.4.1 Metod

EY använder en beprövad metodik för att genomföra, och analysera, en simulerad phishingattack. Övningen sätts upp med hjälp av ett verktyg som används för att skicka ut ett e-postmeddelanden till den definierade målgruppen, samt för att samla in data kring det faktiska utfallet. Insamlad information jämförs sedan mot på förhand definierade acceptansnivåer, samt vad EY anser är en godtagbar standard i offentlig sektor. Den information som ligger till grund för granskningen har insamlats av EY i möten med utvalda nyckelpersoner som arbetar med informationssäkerhet inom Höganäs kommun.

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

- **Mottagare som klickade på länken i e-postmeddelandet** – EY har granskat hur många mottagare av det förfalskade e-postmeddelande som klickade på länken till landningssidan inbäddad i e-postmeddelandet. Detta för att få en förståelse för kommunens motståndskraft mot hotet av phishing, samt hur god kunskapsnivån inom 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 eller laddar ner en bilaga i ett e-postmeddelande skickat från en okänd avsändare.
- **Mottagare som uppgav användarinformation 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 användarinformation 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 kan utvinna känslig information och ta sig in i en organisations IT-infrastruktur ökar avsevärt om en medarbetare delar med sig av sin användarinformation som kan leda till en organisations tillgångar.
- **Mottagare som rapporterade e-postmeddelandet** – EY har granskat hur många mottagare av det förfalskade e-postmeddelandet som identifierade indikationerna på phishing, samt valde att rapportera meddelandet till kommunens IT-avdelning. Detta för att mäta kommunens motståndskraft mot phishing, skapa en förståelse för hur väl kommunens medarbetare identifierar ett e-postmeddelande från en falsk avsändare, samt hur väl rapporteringsvägen för att rapportera dessa fungerar, och i vilken utsträckning den används av medarbetarna i praktiken. EY bedömer detta som ett viktigt område att granska, då det dels visar på hur medvetna medarbetarna inom kommunen är kring vikten av att rapportera phishing, samt hur väl rapporteringsvägen fungerar i praktiken. Detta då 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 skyddsåtgärder.

1.4.2 Genomförande

Övningen har utformats och genomförts av specialister inom IT- och informationssäkerhet från EY, tillsammans med utvalda representanter från Höganäs 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.

1.4.2.1 E-postmeddelande och landningssida

En simulerad phishingattack bygger på att ett e-postmeddelande skickas ut till en utvald målgrupp. E-postmeddelande kan vara utformat på olika sätt baserat på övningens syfte. E-postmeddelandet kan exempelvis innehålla en länk som leder vidare till en internetsida (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 anställda är att dela med sig av användarinformation som inloggningsuppgifter eller att ladda ner okända filer.

För att bestämma hur e-postmeddelandet skulle utformas hölls inledningsvis möten tillsammans med kommunens representanter. Beslutet föll på att inkludera en länk i e-postmeddelande som hänvisade till en landningssida. På landningssidan uppmanades det att berörd person skulle uppge inloggningsuppgifter (e-postadress samt lösenord) till sitt outlook-konto. För e-postmeddelandet som skickades ut samt landningssidan, se *Bilaga 1*.

1.4.2.2 Målgrupp och utskick

Målgruppen för en simulerad phishingattack kan variera beroende på övningens syfte. E-postmeddelande kan exempelvis vara riktat mot utvalda avdelningar eller bolag baserat på deras risknivå. E-postmeddelandet kan också skickas ut till samtliga anställda för att på så sätt skaffa sig en övergripande bild av kommunens motståndskraft samt de anställdas medvetenhet.

I samråd med kommunens representanter beslutades det att skicka ut e-postmeddelandet till samtliga 2737 medarbetare inom Höganäs kommun. Innan det faktiska e-postmeddelandet skickades ut hölls ett testmöte 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 samt potentiell rate limiting. Onsdagen den 8 september 2021, dagen efter att den tekniska genomgången avslutats med lyckade resultat, skickades e-postmeddelandet ut till samtliga mottagare. Simuleringen var sedan aktiv i en veckas tid, fram till den 15 september 2021.

1.4.2.3 Rapportering

Att skydda sig mot hotet från en phishingattack är komplicerat och är en samverkan mellan många olika faktorer. En viktig komponent är att effektiva rapporteringsvägar existerar, samt att de anställda är medvetna kring dessa. Åtgärder bör vidtas skyndsamt då hotet är som störst under den initiala tiden efter att e-postmeddelandet mottagits. Det är också av stor vikt att personer som förmodar att de blivit utsatta för angrepp vidtar nödvändiga åtgärder för att ändra inloggningsuppgifter som en angripare kan ha fått tillgång till.

Inom Höganäs kommun ska rapporteringen av ett förmodat falskt e-postmeddelande rapporteras till IT-avdelningen. Rapporteringen kan ske via e-post eller ett telefonsamtal. När IT-avdelningen har

tagit emot en rapportering tar de vidare ärendet och undersöker dess natur. Ifall det bekräftas att ett illvilligt e-postmeddelande har tagits emot av någon av kommunens anställda läggs det upp en varning på kommunens intranät. Samtliga anställda som misstänker att de utsatts för falskt e-postmeddelande uppmanas att rapportera detta till IT-avdelningen för att få hjälp att byta inloggningsuppgifter. För varningen som lades upp i samband med den simulerade övningen, se *Bilaga 2*.

1.4.2.4 Risknivåer och acceptansnivåer

För att tolka resultaten av en simulerad phishingattack krävs en förståelse kring potentiella risker av en fullbordad attack (risknivåer), samt mottagarens relativa benägenhet att acceptera dessa (acceptansnivåer). Risken för en fullbordad attack kan exempelvis vara mer omfattande för en större kommun då dessa besitter mer känslig information samt större finansiell kraft. Det kan också vara skillnader inom en kommun, där vissa förvaltningar kan ha mindre risk än andra baserat på typen av verksamhet. Se *Tabell 1* för den definition av risknivåer som EY har använt under genomförd granskning:

Tabell 1: Risknivåer för phishingövning

Mycket hög risk	En mycket hög risk för, och i samband med, en phishingattack existerar. Kommunen rekommenderas att omgående vidta åtgärder för att åtgärda svagheter i motståndskraften mot phishingattacker. Detta för att undvika finansiella förluster, negativt rykte eller andra betydande konsekvenser.
Hög risk	En hög risk för, och i samband med, en phishingattack existerar. Kommunen rekommenderas att vidta åtgärder för att utvärdera och åtgärda svagheter i motståndskraften mot phishingattacker. Detta för att undvika finansiella förluster, negativt rykte eller andra betydande konsekvenser.
Medel risk	En medel risk för, och i samband med, en phishingattack existerar. Kommunen rekommenderas att utvärdera och förbättra motståndskraften mot phishingattacker. Detta för att undvika finansiella förluster, negativt rykte eller andra betydande konsekvenser.
Låg risk	En låg risk för, och i samband med, en phishingattack existerar. Kommunen rekommenderas att arbeta vidare med att kontinuerligt säkerställa en hög motståndskraft mot phishingattacker. Detta för att undvika finansiella förluster, negativt rykte eller andra betydande konsekvenser.

Innan en simulerad phishingattack påbörjas är det även viktigt att översätta de olika risknivåerna som existerar till specifika mätetal anpassade för den aktuella organisationen, vilket kallas för acceptansnivåer. För den simulerade övningen definierades acceptansnivåer av kommunens representanter genom att omvandla risknivåerna till specifika procentandelar, se *Bilaga 3*.

1.4.3 Tidsplan

Granskningen genomfördes från maj 2021, till november 2021, se *Tabell 2* nedan för granskningens tidsplan.

Tabell 2: Tidsplan

Förberedelser och planering	Maj – September 2021
Test och utskick	September 2021
Rapportskrivning samt intern kvalitetssäkring	September 2021
Justering samt färdigställande av rapport	Oktober 2021
Avrapportering och slutpresentation	November 2021

2. Analys

En phishingattack kan genomföras på många olika sätt vilket kan påverka resultatet samt eventuella konsekvenser av attacken. Beroende på vad en cyberkriminell aktör har för målsättning med en attack kan den vara mer eller mindre riktad till specifika personer eller avdelningar inom kommunen. Sättet man utformar phishingattacken på påverkar därmed resultatet och bör vägas in i analysen av detta. I följande kapitel analyseras resultatet av den simulerade attack som EY gemensamt med kommunen utformat. Analysen presenteras i tre delar som kretsar runt tre nyckeltal: 2.1 Mottagare som klickat på länken i e-postmeddelandet, 2.2 Mottagare som uppgav användarinformation på landningssidan, samt 2.3 Mottagare som rapporterade e-postmeddelandet.

2.1 Mottagare som klickade på länken i e-postmeddelandet

Resultatet av den simulerade attacken visar att 16% av alla mottagare klickade på den inbäddade länken i e-postmeddelandet. Resultatet av granskningen visar att kommunen, inklusive nämnder, förvaltningar samt helägda bolag, löper en mycket hög risk att utsättas för en phishingattack i jämförelse med kommunens på förhand definierade acceptansnivåer.

Höganäs kommun hade i samråd med EY på förhand bestämt acceptansnivåer för vilka resultat som bör accepteras baserat på verksamhetens omfattning och nuvarande arbete kring medvetenhet av informationssäkerhet. Se *Tabell 3* för de på förhand beslutade acceptansnivåerna.

Tabell 3: Acceptansnivåer för andel mottagare som klickar på länken

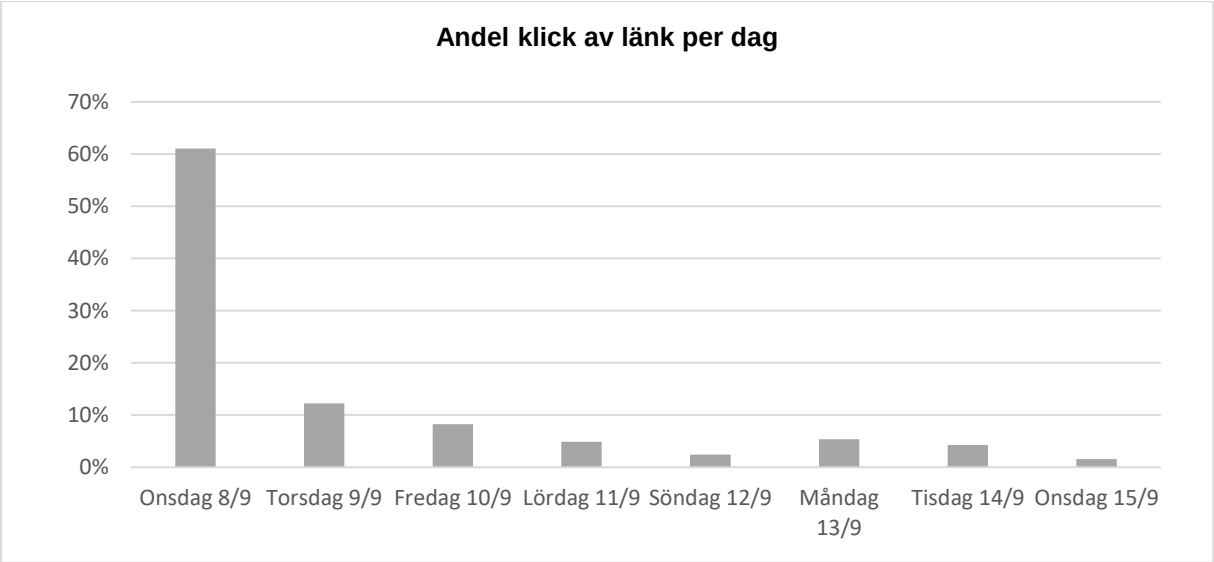
Riskanalys	**Acceptansnivå (%)**
Mycket hög risk	>5%
Hög risk	3,1–5%
Medel risk	1,5–3%
Låg risk	<1,5%

2.1.1 Resultat av simulering

Totalt skickades e-postmeddelandet till 2737 medarbetare inom Höganäs kommun, inklusive förvaltningar samt kommunala bolag. 449 av dessa mottagare öppnade e-postmeddelandet och klickade på den inbäddade länken i meddelandet, motsvarande 16% av alla mottagare, se *Figur 2* nedan. I relation till acceptansnivåerna presenterade i *Tabell 3*, löper därmed Höganäs kommun, inklusive förvaltningar samt kommunala bolag, en mycket hög risk för att utsättas för en lyckad attack av phishing.

Figur 2*:* Fördelning av andel mottagare som klickade på länken i e-postmeddelandet (%).

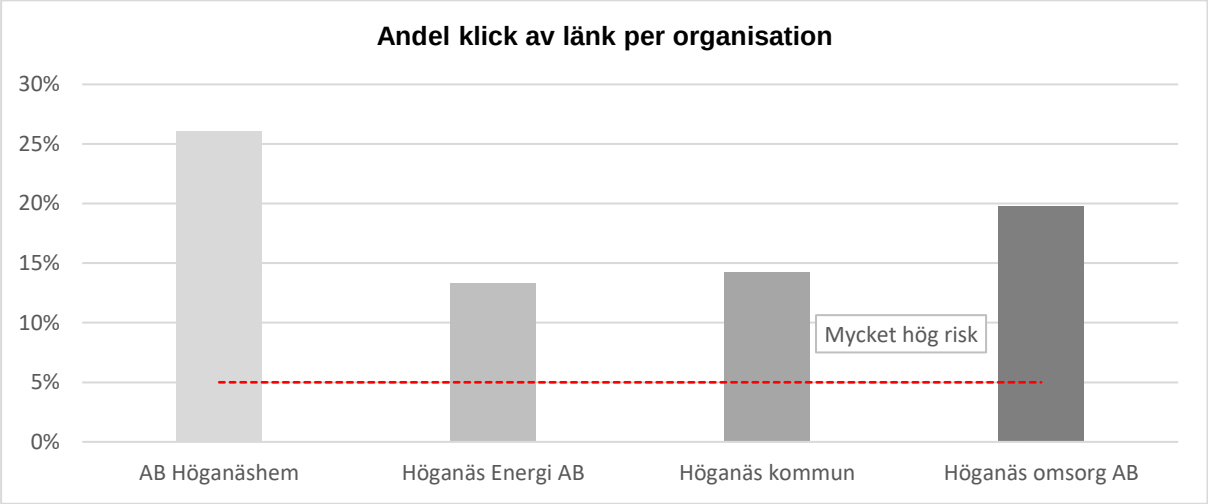
Simuleringen var aktiv under en veckas period. Majoriteten av mottagarna som klickade på länken i e-postmeddelandet gjorde detta under simuleringens första dag, motsvarande 61% av alla mottagare som tryckte på länken. *Figur 3* visar att andelen mottagare som klickade på länken i e-postmeddelandet under resterande dagar sjönk sedan markant, vilket enligt EY är förväntat i en simulerad attack som påkallar omedelbara handlingar av mottagaren.



Figur 3: Andel klick av länk i e-postmeddelande per dag (%).

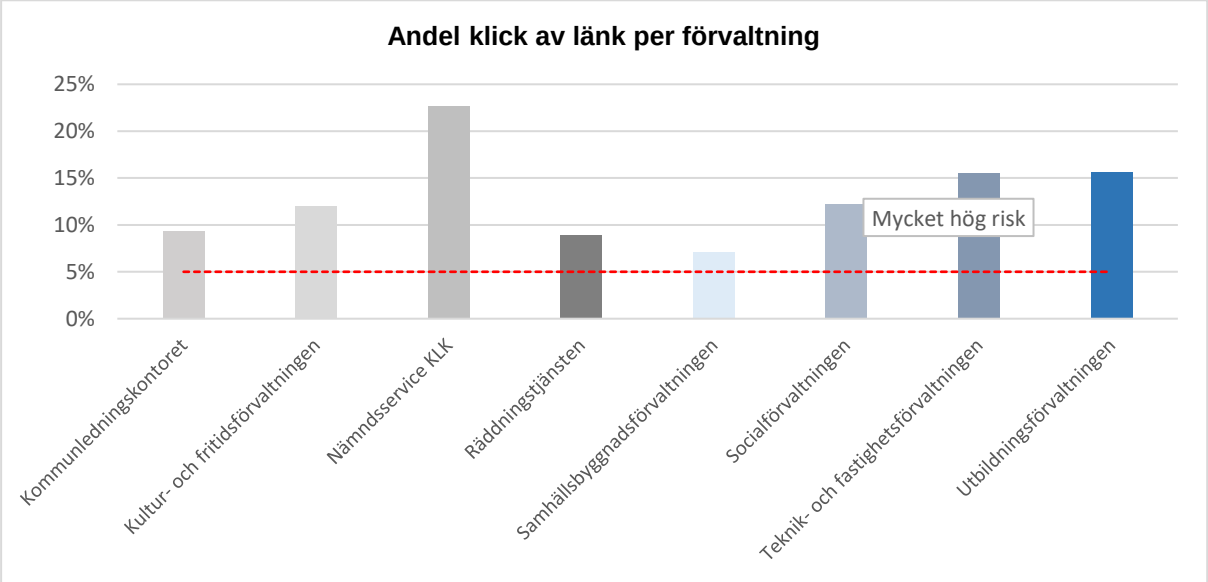
Figur 4 visar hur stor andel av e-postmeddelandets mottagare som klickade på den inbäddade länken i e-postmeddelandet, per organisation. EY noterade att AB Höganäshem var organisationen med den högsta andelen mottagare som klickat på länken (6) baserat på deras totala antal mottagare (23), motsvarande 26% av bolagets totala antal mottagare. Även inom Höganäs omsorg AB noterade EY att cirka 20% av bolagets anställda (203 mottagare av totalt 1025) klickade på den inbäddade länken i e-postmeddelandet. Det totala resultatet av antal mottagare som klickade på den inbäddade länken i e-postmeddelandet, i relation till de på förhand bestämda acceptansnivåerna visar på att samtliga

delar av Höganäs kommun inklusive förvaltningar samt bolag, löper en mycket hög risk att utsättas för en phishingattack.



Figur 4: Fördelning av mottagare som klickade på länk per organisation (%). Notera att andel mottagare som klickat på e-postmeddelandet för varje organisation är baserat på det antal e-postmeddelanden som skickades till respektive organisation.

Figur 5 visar hur stor andel av e-postmeddelandets mottagare som klickade på den inbäddade länken i e-postmeddelandet, per kommunens förvaltningar. EY noterade att Nämndsservice KLK var förvaltningen med det högsta andelen mottagare som klickat på länken (12) baserat på deras totala antal mottagare (53), motsvarande 23% av förvaltningens totala mottagare. EY noterade att alla kommunens förvaltningar löper en mycket hög risk för att utsättas för en lyckad cyberattack genom phishing, i jämförelse med de tidigare bestämda acceptansnivåerna.



Figur 5: Fördelning av mottagare som klickade på länk per förvaltning (%). Notera att andel mottagare som klickat på e-postmeddelandet för varje förvaltning är baserat på det antal e-postmeddelanden som skickades till respektive förvaltning.

2.2 Mottagare som uppgav användarinformation på landningssida

Resultatet av den simulerade attacken visar att 7% av e-postmeddelandets mottagare uppgav användarinformation på den förfalskade landningssidan. Resultatet visar att kommunen, inklusive nämnder, förvaltningar samt helägda bolag, löper en mycket hög risk att utsättas för en phishingattack i jämförelse med kommunens på förhand definierade acceptansnivåer.

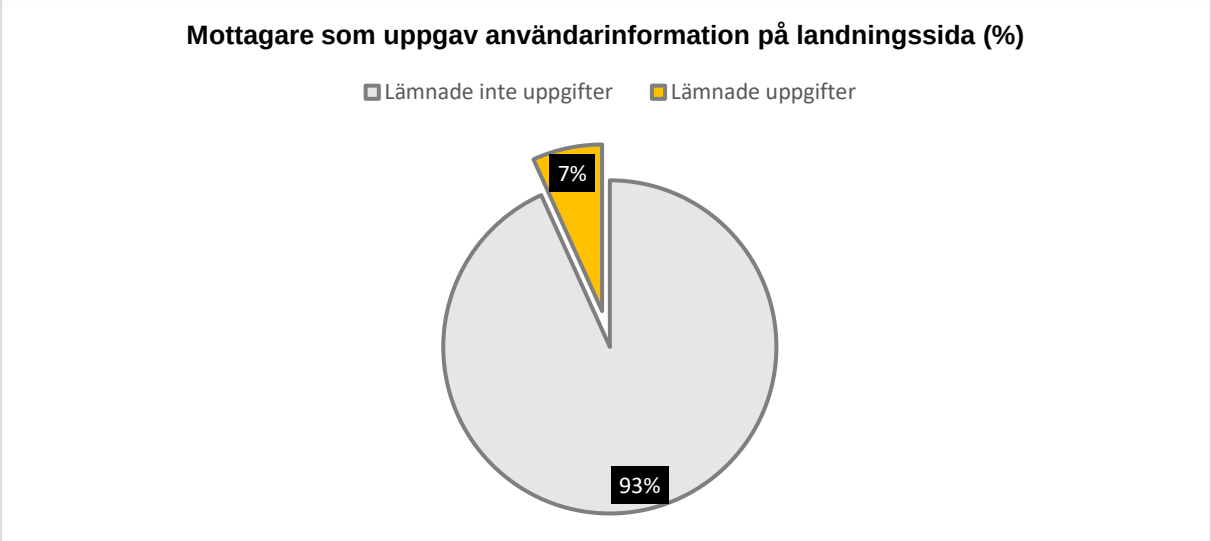
Höganäs kommun hade i samråd med EY på förhand bestämt acceptansnivåer för vilka resultat som bör accepteras baserat på verksamhetens omfattning och nuvarande arbete kring medvetenhet av informationssäkerhet. Se *Tabell 4* för de på förhand beslutade acceptansnivåerna.

Tabell 4: Acceptansnivåer för andelen mottagare som uppger användarinformation

Riskanalys	Acceptansnivå (%)
Mycket hög risk	>2%
Hög risk	1,1–2%
Medel risk	0,25–1%
Låg risk	<0,2%

2.2.1 Resultat av simulering

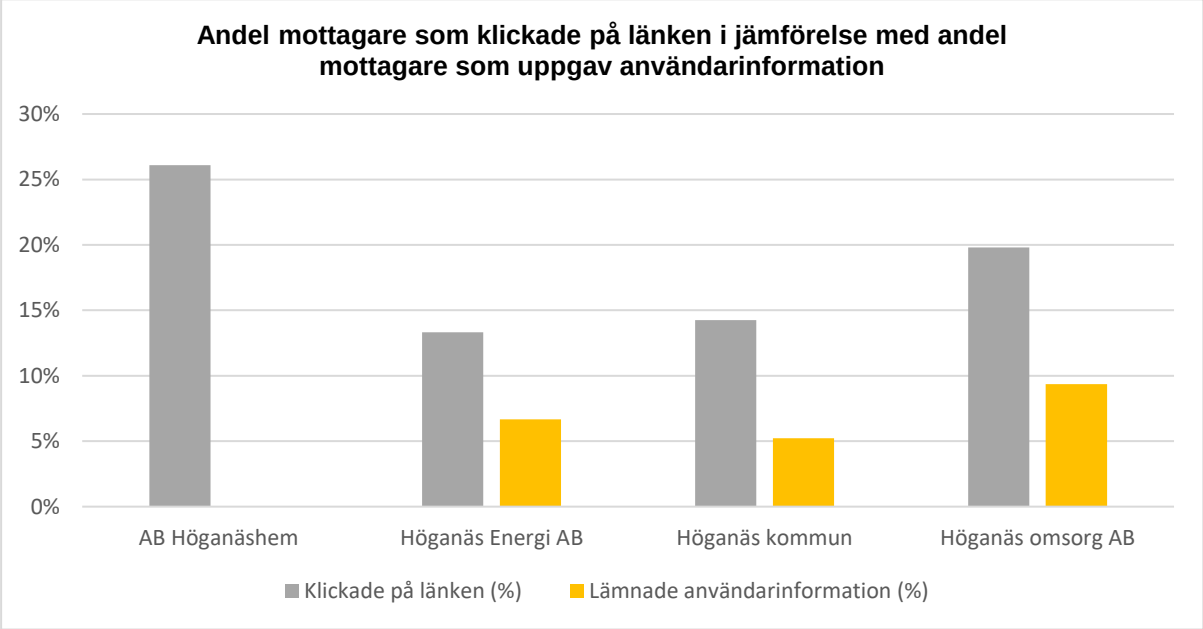
Totalt skickades e-postmeddelandet till 2737 anställda på Höganäs kommun, inklusive förvaltningar samt kommunala bolag. 185 av dessa mottagare klickade på länken i e-postmeddelandet samt uppgav användarinformation på landningssidan, motsvarande 7% av alla mottagare, se *Figur 6*. I relation till acceptansnivåerna presenterade i *Tabell 4*, löper därmed Höganäs kommun, inklusive förvaltningar samt kommunala bolag, en mycket hög risk för att utsättas för en lyckad phishingattack.



Figur 6: Fördelning av mottagare som uppgav användarinformation på landningssida (%).

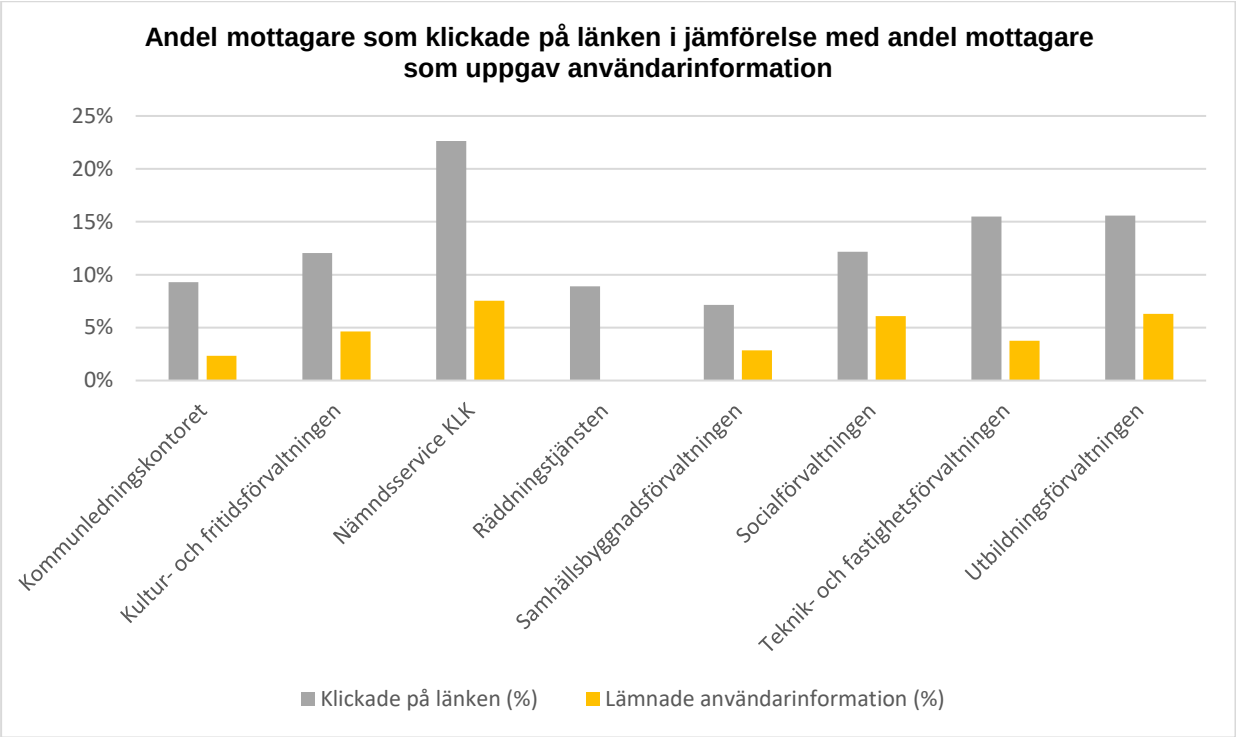
Figur 7 visar en jämförelse över andelen mottagare som klickade på länken i e-postmeddelandet i relation till andelen mottagare som uppgav användarinformation på landningssidan per organisation. EY noterade att AB Höganäshem var bolaget där flest mottagare procentuellt klickade på länken i e-

postmeddelandet, men där ingen av dessa mottagare uppgav användarinformation på landningssidan. I jämförelse med de på förhand bestämda acceptansnivåerna visar detta på att AB Höganäshem löper en låg risk för att utsättas för en lyckad phishingattack. EY noterade att Höganäs omsorg AB uppnådde den högsta andelen mottagare som uppgett användarinformation på den förfalskade landningssidan, där 96 mottagare av totalt 1026 mottagare (9% av alla mottagare) lämnat sin information. I jämförelse med acceptansnivåerna löper Höganäs kommun samt dess helägda bolag Höganäs Energi AB och Höganäs omsorg AB en mycket hög risk för att utsättas för en lyckad phishingattack.



Figur 7: Jämförelse av mottagare som klickade på länken i relation till mottagare som uppgav användarinformation på landningssida (per organisation). Notera att andelen mottagare är baserat på det antal e-postmeddelanden som skickades till respektive organisation.

Figur 8 visar en jämförelse över andelen mottagare som klickade på länken i e-postmeddelandet i relation till andelen mottagare som uppgav användarinformation på landningssidan för respektive förvaltning. Resultatet visar att alla mottagare inom alla förvaltningar utom räddningstjänsten angav användarinformation på landningssidan. EY noterade att 6% av mottagarna inom socialförvaltningen samt utbildningsförvaltningen uppgav användarinformation på landningssidan, vilket EY bedömer som en hög nivå i jämförelse med antalet mottagare som enbart klickade på länken i e-postmeddelandet. I jämförelse med de på förhand bestämda acceptansnivåerna löper alla förvaltningar inom Höganäs kommun en mycket hög risk för att utsättas för en lyckad phishingattack, förutom räddningstjänsten som löper en låg risk.



Figur 8: Jämförelse av mottagare som klickade på länken i relation till mottagare som uppgav användarinformation på landningssida (per förvaltning). Notera att andelen mottagare är baserat på det antal e-postmeddelanden som skickades till respektive förvaltning.

2.3 Mottagare som rapporterade e-postmeddelandet

Inom Höganäs kommun rapporteras misstänksamma e-postmeddelanden till kommunens IT-avdelning, via valfritt kommunikationsmedel. Totalt rapporterade 119 mottagare e-postmeddelandet till IT-avdelningen under pågående simulering, motsvarande 4% av alla mottagare. Noterbart är att det var relativt få av de mottagare som lämnade användarinformation på landningssidan som rapporterade att de hade gjort så till IT-avdelningen (12%). Detta resultat kan vara särskilt kritiskt då det ökar risken för att konfidentiell information sprids till fientliga aktörer utan kommunens vetskap. Resultatet visar även på att majoriteten av rapporteringarna inkom under morgonen av simuleringens första dag, samt att antalet mottagare som klickade på länken i e-postmeddelandet minskade i samband med att rapporteringarna började inkomma, samt när kommunen publicerade en varning om phishingattacken på intranätet.

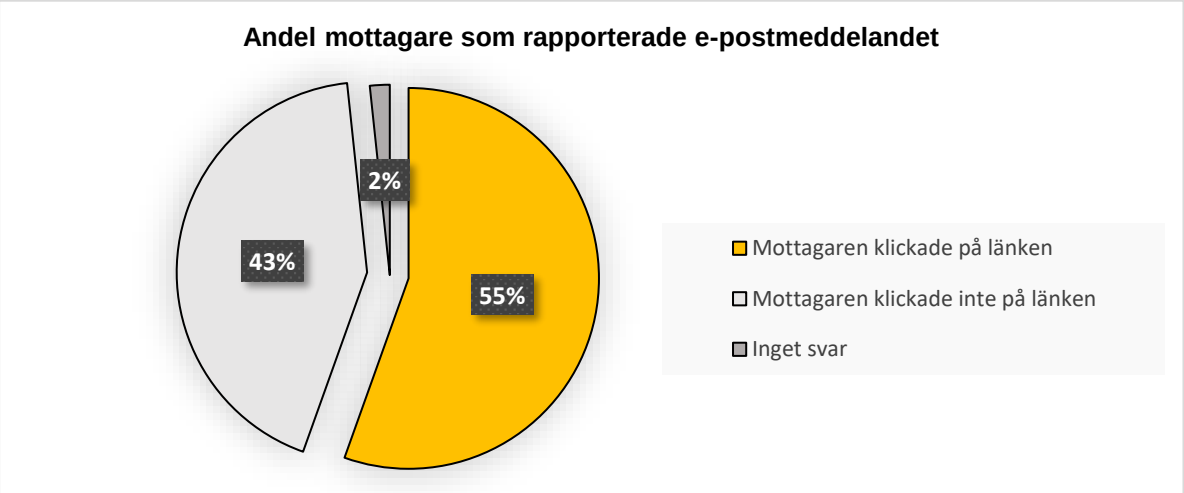
2.3.1 Resultat av simulering

Tabell 5 visar att 4% av e-postmeddelandets mottagare (motsvarande 119 medarbetare) rapporterade e-postmeddelandet till IT-avdelningen. Tabellen visar också att 15% av simuleringens mottagare som klickade på länken i e-postmeddelandet rapporterade e-postmeddelandet. EY noterade att 12% av de mottagare som lämnat sin användarinformation på landningssidan rapporterade detta till IT-avdelningen. Detta innebär att 88% av e-postmeddelandets mottagare som uppgav sin konfidentiella information på landningssidan inte rapporterade detta till kommunens IT-avdelning.

Tabell 5: Nyckeltal för rapportering

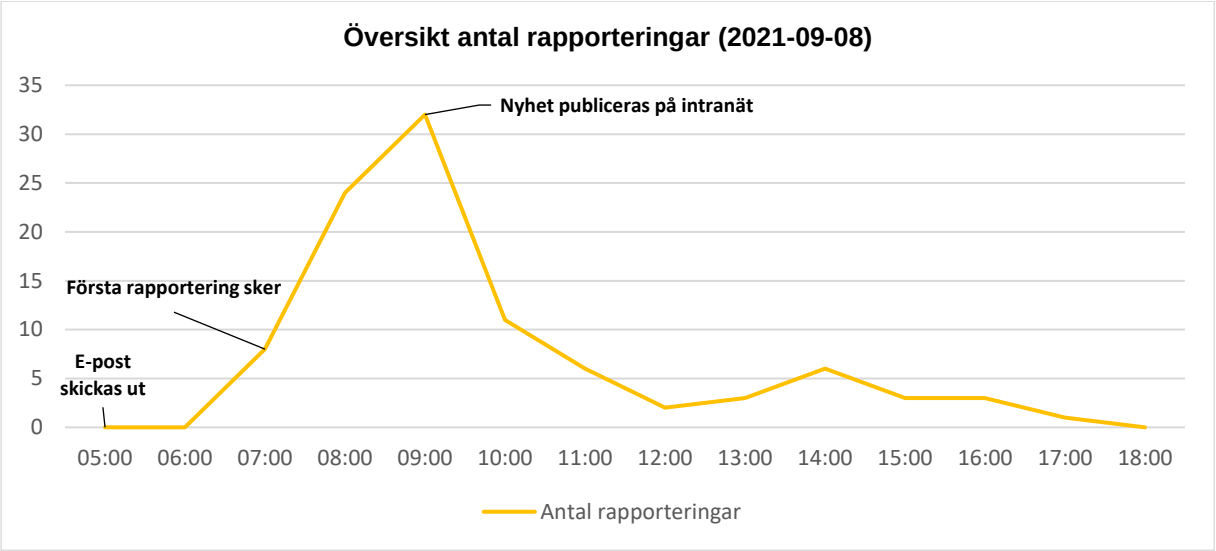
Område	Resultat
Total andel mottagare som rapporterade e-postmeddelandet	4 %
Andel av de mottagare som klickade på länken som rapporterade e-postmeddelandet	15 %
Andel av de mottagare som uppgav användarinformation på landningssidan som rapporterade e-postmeddelandet	12 %

Figur 9 visar en översikt över de mottagare som valde att rapportera e-postmeddelandet till IT-avdelningen. 55% av dessa (motsvarande 66 medarbetare) angav under rapporteringstillfället att de hade klickat på länken i e-postmeddelandet. 43% (motsvarande 51 medarbetare) angav att de inte hade klickat på länken.



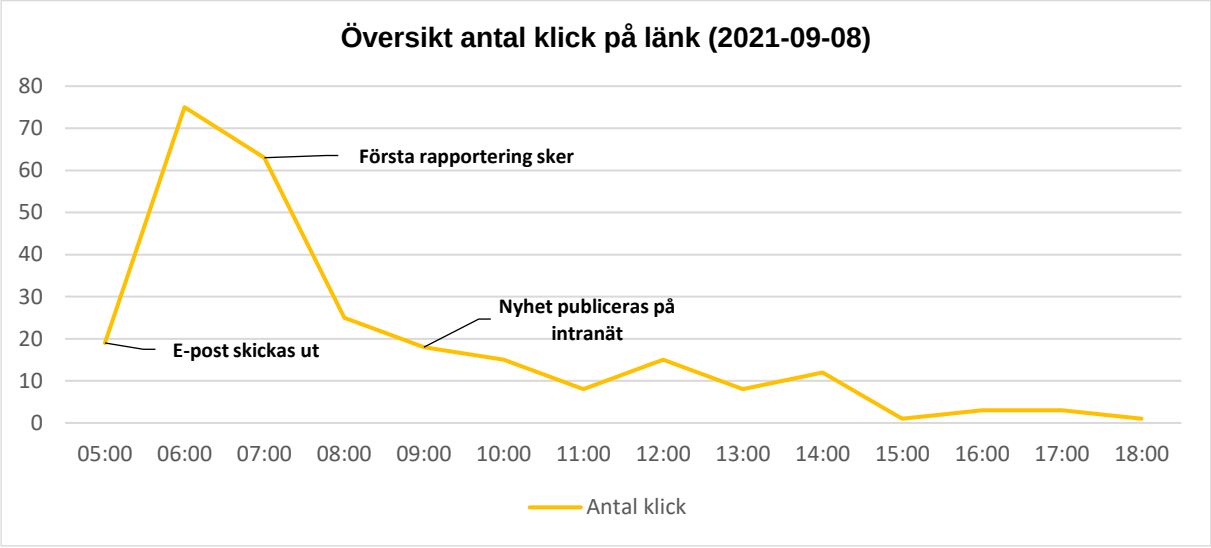
Figur 9: Andel rapporterade ärenden till IT-avdelningen där mottagaren klickat på länken i e-postmeddelandet (%).

EY noterade att majoriteten av alla rapporteringar av e-postmeddelandet (85%) inkom till IT-avdelningen under simuleringens första dag. *Figur 10* visar fördelningen per timme över antalet rapporteringar som inkom under denna dag. Detta visar att den första rapporteringen inkom till IT-avdelningen mellan klockan 06:00–07:00, samt att flest medarbetare rapporterade det misstänksamma e-postmeddelandet mellan klockan 08:00-09:00. Höganäs kommun publicerade en varning gällande den pågående attacken på intranätet under denna tidsperiod, vilket fick konsekvensen att antalet rapporterade ärenden minskade drastiskt.



Figur 10: Antal rapporteringar av e-postmeddelandet under simuleringens första dag (2021-09-08).

EY noterade att de flesta mottagare som klickade på länken (61%) gjorde detta under simuleringens första dag. *Figur 11* visar att flest mottagare klickade på länken i e-postmeddelandet mellan klockan 05:00-06:00, samt mellan klockan 06:00-07:00, det vill säga innan arbetsdagens början och innan en varning hunnit publiceras på kommunens intranät. EY noterade även att andelen mottagare som klickade på den inbäddade länken i e-postmeddelandet minskade efter att den första rapporteringen inkommit till IT-avdelningen, samt efter att kommunen publicerade varningen till sina medarbetare via intranätet.



Figur 11: Antal mottagare som klickade på länken i e-postmeddelandet under simuleringens första dag (2021-09-08).

3. Övergripande rekommendationer

Baserat på genomförd analys bedömer EY att Höganäs kommun ligger på en nivå något under det EY anser att man kan förvänta sig av kommunen. Bedömningen baseras på den typ av verksamhet som bedrivs och på känslighetsgraden av den information, exempelvis personuppgifter, som kommunen behandlar i dess dagliga verksamhet. EY noterar att kommunen själva har definierat striktare acceptansnivåer, vilket gör att man enligt den egna definitionen löper en mycket hög risk att utsättas för phishingattacker. Kommunen rekommenderas således att vidta åtgärder för att stärka utbildning och medvetenheten hos personalen, samt åtgärda svagheter i motståndskraften mot phishingattacker. Detta för att undvika förluster av känslig information, negativt rykte eller andra betydande konsekvenser. I följande avsnitt presenterar EY de mest relevanta och övergripande rekommendationerna som Höganäs kommun bör fokusera sitt arbete på framöver. EY rekommenderar att arbetet med samtliga rekommendationer påbörjas inom 12 månader.

3.1 Strukturerat och regelbundet arbete med informationssäkerhetsutbildningar

Enligt EY:s ramverk för hur en organisation arbetar med informationssäkerhet styrs en organisations motståndskraft mot angrepp av de anställdas motivation och förmågor. Motivation och förmågor formas i sin tur av olika organisatoriska åtgärder likt styrning, organisation, kommunikation, utbildning och styrdokument. För att erhålla en god motståndskraft mot cyberattacker krävs det således ett övergripande, strukturerat och planlagt arbete med informationssäkerhet. Detta arbete bör inkludera en tydlig plan för hur organisationen ska öka medvetenheten genom planlagda och regelbundna utbildningsinsatser inom informationssäkerhet.

Baserat på resultaten av den genomförda granskningen rekommenderar EY att Höganäs kommun utvecklar ett formaliserat program av informationssäkerhetsutbildningar för samtliga medarbetare inom kommunen. Detta för att kunna förbättra kommunens motståndskraft mot cyberattacker. Syftet med programmet bör också vara att öka medvetenheten kring vikten av informationssäkerhet, samt att utbilda medarbetare om de hot och risker som finns relaterade till informationssäkerhet i deras dagliga arbete. Programmet rekommenderas att inkludera specifika mål för utbildningar inom informationssäkerhet, exempelvis olika delmål för olika informationssäkerhetsområden. EY rekommenderar även att kommunen genomför en utförlig intressentanalys för att identifiera särskilda målgrupper inom kommunen som programmet kan behöva riktas mot. Dessa målgrupper skulle exempelvis kunna vara förvaltningar eller kommunala bolag som är i en särskilt hög riskgrupp baserat på karaktären av dess verksamheter. Utifrån denna analys rekommenderar EY att programmet ska konkretisera hur kommunikation, samt utbildningsaktiviteter med respektive målgrupp, ska utformas, genomföras samt följas upp.

3.2 Teoretiska samt praktiska övningar inom phishing

Mängden cyberattacker hos organisationer har ökat under de senaste åren. Bland dessa attacker har EY framförallt noterat en markant ökning i antalet phishingattacker som utförts. En faktor som ligger till grund för detta är COVID-19 och den ökade användningen av digitala verktyg detta har inneburit. De anställdas medvetenhet och kunskap kring informationssäkerhet blir således allt viktigare för att

säkerställa ett adekvat skydd av informationen hos en organisation, samt för att uppfylla gällande lagkrav om informationssäkerhet och integritet. Att klicka på en inbäddad länk i ett e-postmeddelande, eller att uppge användardata, under en pågående cyberattack genom phishing kan exempelvis leda till stora konsekvenser för en kommun, både på individ- samt organisationsnivå. Detta då cyberkriminella kan försöka utvinna konfidentiell information, eller implementera skadlig kod i mottagarens enhet.

Baserat på utförd granskning rekommenderar EY att Höganäs kommun formulerar en tydlig plan kring hur medvetenheten och kunskapen kring phishing ska ökas genom hela organisationen, och specifikt i de delar av kommunen som löper störst risk för denna typ av attacker. Utbildningsplanen bör inkludera teoretiska aspekter av området, så som vad vanliga indikationer på ett falskt e-postmeddelande kan vara, samt vilka konsekvenser en fullbordad phishingattack kan innebära. Utöver specifika utbildningstillfällen, rekommenderas kommunen att kontinuerligt sprida utbildningsmaterial till sina medarbetare, exempelvis i form av checklistor medarbetarna kan följa vid misstanke av en phishingattack. Utöver teoretisk utbildning, rekommenderar EY Höganäs kommun att även utföra praktiska övningar av motståndskraften mot phishing inom kommunen. Detta kan exempelvis innebära regelbundna och planlagda tester av säkerhetsmedvetenheten och kunskapen inom phishing hos medarbetarna. Detta för att kontrollera effekten av genomförda utbildningsinsatser, samt för att fortsätta sprida medvetenheten inom kommunen. Praktiska övningar relaterade till cyberattacker via e-postmeddelanden bör genomföras regelbundet, för att utbilda och öva medarbetarnas praktiska kompetens att kunna identifiera ett falskt e-postmeddelande, avsändare, eller domän. Det finns olika sätt en kommun kan genomföra tester, men framförallt rekommenderar EY att kommunen utforskar möjligheten att fortsätta med uppföljande simuleringar av phishingattacker för att erhålla analyserbar och enhetliga data.

3.3 Kommunicera betydelsen av rapportering

Det finns olika sätt en organisation kan minska effekterna av en pågående cyberattack genom att underlätta identifiering, förhindra spridning och stoppa attacken. En viktig faktor är att effektiva rapporteringsvägar existerar, samt att de anställda är medvetna om hur, och när, dessa ska användas. När det rör sig om phishingattacker kan rapporteringen av ett misstänksamt e-postmeddelande möjliggöra att hotet identifieras, samt att adekvata skyddsåtgärder kan vidtas inom skälig tid. Att snabbt identifiera och motverka en phishingattack kan således ha stor påverkan på hur skadliga konsekvenser blir, samt möjligheterna att sedermera stoppa den. Rapporteringsvägen bör också utvärderas regelbundet och övervakas av informationssäkerhetsansvariga inom kommunen.

Baserat på resultatet från granskningen rekommenderar EY att Höganäs kommun ser över sina befintliga rapporteringsvägar, samt medvetenheten hos kommunens medarbetare kring dessa. Rapporteringsvägarna bör vara tydliga, kommunicerade och tillgängliga för alla. Ifall någon medarbetare har frågor kring rapporteringsvägar bör det var tydligt vart, eller till vem, de ska vända sig. Utöver detta rekommenderas kommunen att arbeta vidare med att kommunicera vikten av att rapportera eventuella säkerhetsincidenter inom kommunen. Kommunikationen bör inkludera tydliga förväntningar och kravställningar på rapportering då man misstänker att man blivit utsatt för en cyberattack eller att man angett användarinformation till en extern aktör. EY bedömer att rapporteringsfrekvensen hos en organisation som utsätts för en phishingattack riskerar att minska vid ökat hemarbete, då medarbetare inte har samma regelbundna kontakt med varandra. Denna risk är således ytterligare en faktor som talar för behovet av att kommunicera vikten av att rapportera säkerhetsincidenter till samtliga medarbetare.

4. Revisionsfrågor

Granskningen har utgått från två revisionsfrågor, vilka besvaras nedan.

Färgkod	Förklaring
	Revisionsfråga uppfylls ej
	Revisionsfråga uppfylls delvis
	Revisionsfråga uppfylls

Revisionsfråga	Svar	
► Hur väl hanterar Höganäs kommuns personal hotet från attacker genom falska e-postmeddelanden, så kallad phishing?	Baserat på genomförd granskning bedömer EY att Höganäs kommun bör arbeta för att förbättra personalens förmågor att hantera det ökade hotet av phishingattacker. Slutsatsen bygger på att Höganäs kommun ligger på en nivå något under det EY anser att man kan förvänta sig utav kommunen. EY noterar att kommunen själva har definierat striktare acceptansnivåer, vilket gör att man enligt den egna definitionen löper en mycket hög risk att utsättas för phishingattacker. Detta styrker behovet av att vidta åtgärder för att stärka medvetenheten hos personalen, samt åtgärda svagheter i motståndskraften mot phishingattacker.	
► Hur kan Höganäs kommuns säkerhetsarbete kopplat till attacker med falska e-postmeddelanden utvecklas?	Resultatet ifrån genomförd granskning indikerar att det finns ett behov av att förbättra säkerhetsarbetet kopplat till phishingattacker. EY har därför valt att presentera de mest relevanta och övergripande rekommendationerna som Höganäs kommun bör fokuserar sitt arbete på framöver. Den första rekommendationen handlar om att utveckla ett strukturerat och regelbundet arbete med informationssäkerhetsutbildningar, särskilt fokuserat på de delar av organisationen som kan vara målgrupper för phishingattacker. Utöver detta rekommenderas kommunen att fortsätta genomföra både teoretiska samt praktiska övningar inom phishing. Slutligen rekommenderar EY att kommunen vidareutvecklar sina befintliga rapporteringsvägar, samt kommunicerar vikten av att rapportera säkerhetsincidenter till alla medarbetare.	

5. Slutsatser

Antalet cyberattacker har ökat stort under de senaste åren. Bland dessa attacker kan det särskilt noteras en ökning inom kategorin phishing, vilket innebär att angriparen försöker lura användare att lämna ut information genom falsk e-post. De anställdas medvetenhet och kunskap kring informationssäkerhet blir således allt viktigare för att säkerställa ett adekvat skydd av informationen hos en organisation, samt för att uppfylla gällande lagkrav om informationssäkerhet och integritet. Att klicka på en inbäddad länk i ett e-postmeddelande, eller att uppge användarinformation, under en pågående cyberattack genom phishing kan exempelvis leda till stora konsekvenser för en kommun, både på individ- samt organisationsnivå. Detta då cyberkriminella kan försöka utvinna konfidentiell och känslig information, eller implementera skadlig kod i mottagarens enhet. Det kan exempelvis räcka med att endast en användare delar med sig av sitt användarnamn och lösenord för att en cyberkriminell ska få tillgång till socialtjänstregistret eller annan sekretessbelagd information.

Granskningens syfte har varit att bedöma om det finns brister i det praktiska arbetet med IT- och informationssäkerhet inom Höganäs kommun. Syftet har uppnåtts genom att bedöma i vilken utsträckning en potentiell angripare riskerar att kunna komma åt Höganäs kommuns IT-miljöer genom angrepp via ett e-postmeddelande. De följande revisionsfrågorna har legat till grund för granskningen:

- Hur väl hanterar kommunens medarbetare hotet från attacker genom falska e-postmeddelanden, så kallad phishing?
- Hur kan Höganäs kommuns säkerhetsarbete kopplat till attacker med falska e-postmeddelanden utvecklas?

Baserat på genomförd granskning bedömer EY att Höganäs kommun ligger på en nivå något under det EY anser att man kan förvänta sig av en kommun. Slutsatsen baseras på den typ av verksamhet som bedrivs och på känslighetsgraden av den information, exempelvis personuppgifter, som kommunen behandlar i dess dagliga verksamhet. EY noterar att kommunen själva har definierat striktare acceptansnivåer, vilket gör att man enligt den egna definitionen löper en mycket hög risk att utsättas för phishingattacker. Kommunen rekommenderas att vidta åtgärder för att stärka utbildning och medvetenheten hos personalen, samt åtgärda svagheter i motståndskraften mot phishingattacker. Detta för att undvika förluster av känslig information, negativt rykte eller andra betydande konsekvenser.

Baserat på resultatet av granskningen har EY valt att presentera tre övergripande rekommendationer som Höganäs kommun bör fokusera sitt arbete på framöver:

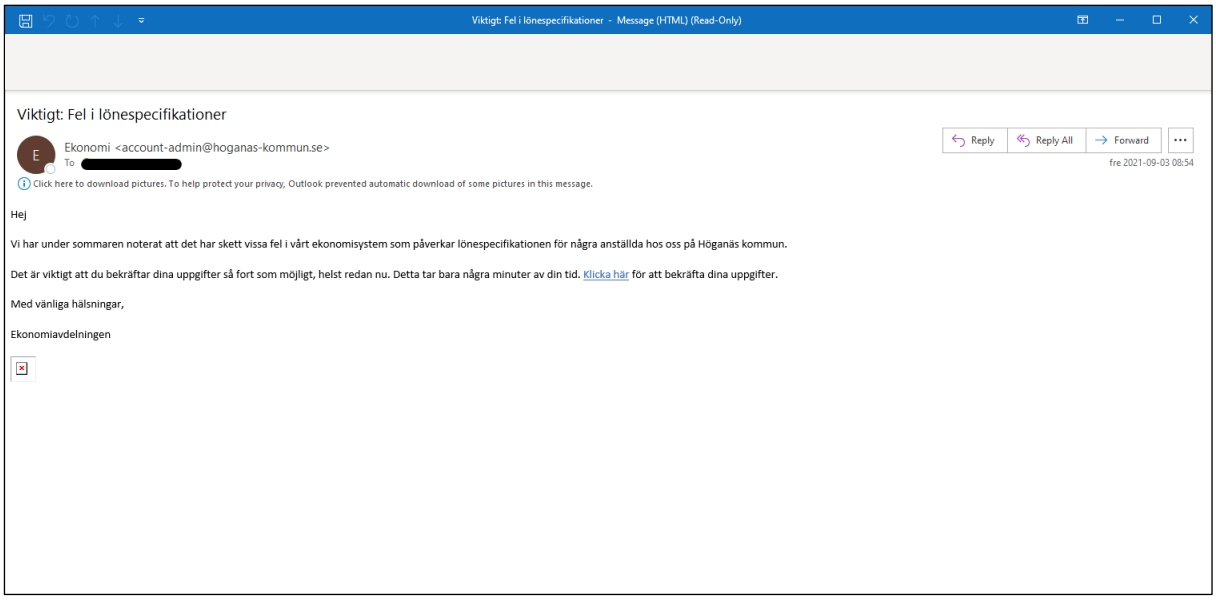
- Utveckla ett strukturerat och regelbundet arbete med informationssäkerhetsutbildningar, särskilt fokuserat på de delar av organisationen som kan vara målgrupper för phishingattacker.
- Genomföra både teoretiska samt praktiska övningar inom phishing.
- Vidareutveckla sina befintliga rapporteringsvägar, samt kommunicerar vikten av att rapportera säkerhetsincidenter till alla medarbetare.

Stockholm den 2021-10-22

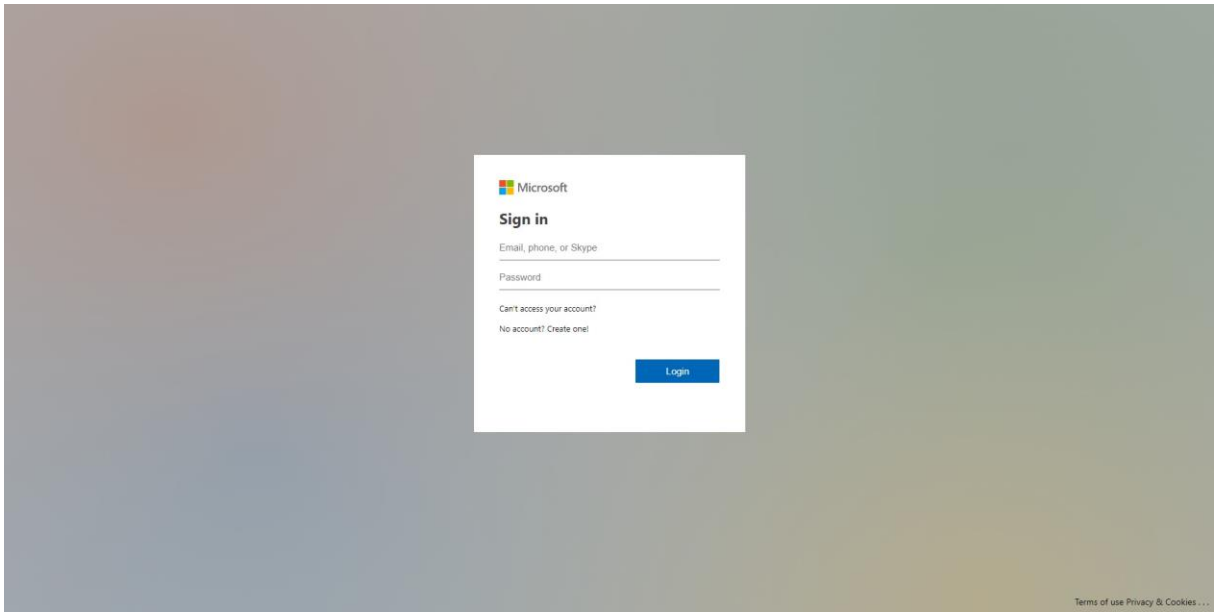
Helena Törnqvist, Partner, EY

Bilaga 1: E-postmeddelande och landningssida

E-postmeddelande



Landningssida



Bilaga 2: Publicerad varning på intranätet

2021-09-08 08:15/SANDRA
I ärendena har vi nu uppdaterat texten till användaren som skickar in ärende om att vi lagt ut nyhet på arbetsnätet med nedanstående text:

”Se nyheten om detta på arbetsnätet. Hjälp oss att sprida informationen till dina kollegor att inte klicka på länken.”

Support börjar använda den nu.

2021-09-08 08:12/SANDRA
Nyhet utlagd:
”Se upp! Bluffmejl - Klicka inte på länken!
Under morgonen har kommunens anställda mottagit ett spam med rubriken "Viktigt! Fel i lönespecifikationer". Klicka inte på länken! Fyll INTE i några uppgifter! Har du klickat - kontakta genast IT-avdelningen via ärende.
Tekniker arbetar med att blocka länken. Sprid till dina kollegor!?”

2021-09-08 08:12/SANDRA
Vi har fått in 40 mejl minst gällande nyheten.

Jag fick mitt spammejl 6:46 idag.

Bilaga 3: Acceptansnivåer

	Mycket hög risk	Hög risk	Medel risk	Låg risk
Andel som klickar på länken i e-postmeddelandet	>5%	3,1 – 5 %	1,5 – 3%	<1,5%
Andel som uppger användarinformation på landningssidan	>2%	1,1 – 2 %	0,25 – 3%	<0,25%

Bilaga 4: 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 härma 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 phishingattacker 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 samt kan bestå av många sammankopplade lokala nätverk.

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.

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 samt 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 med syftet 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 kommunikation med desamma.