Kategorisering på uppfattningar om digitala hot på webbapplikationer

Med en studie som visar de ekonomiska konsekvenserna av cyberattacker

Categorization of conceptions about digital threats on web applications

With a study showing the economic consequences of cyber attacks

Elyas Alyoussef

Examensarbete inom
Datateknik och ekonomi
Grundnivå, 15 hp
Handledare på KTH: Fredrik Heiding
Examinator: Ibrahim Orhan
TRITA-CBH-GRU-2022:022

KTH
Skolan för kemi, bioteknologi och hälsa
141 52 Huddinge, Sverige

Sammanfattning

Detta examensarbete tar upp digitala hot mot webbapplikationer och kategoriserar allmänhetens uppfattning om dem. Digitala hot är oftast kopplade till ekonomiska konsekvenser varvid även dessa kommer att studeras. Målet med detta arbete är att bidra till en vetenskaplig artikel i framtiden, som kan vara värdefull för allmänheten, samt för framtida arbete och sysselsättning.

För att analysera samlade uppfattningar användes konstant jämförande metoden. Resultatet avslöjar flera spännande fynd för teori och praktik, där uppfattningar om cybervärlden presenteras för att kunna förstå mer hur andra ser på cybersäkerhet idag. Det visar även betydande variationer bland deltagarnas uppfattningar och att informationssäkerhet, även om den gradvis utvecklas, har en lång väg tills den blir en obruten del av affärsverksamheten och arbetskraftens verklighet.

Denna studie kan även fungera som en guide för de olika uppfattningarna om cyberattacker eftersom den ger en översikt över de idag mest relevanta cyberattackerna. Arbetet kompletterades med en studie som belyser ekonomiska konsekvenser av cyberattacker. Utöver detta studerades även cyberattacken mot Coop under sommaren 2021.

Nyckelord
Säkerhet, cyberattack, ekonomi, digitala hot, webbapplikationer, cybersäkerhet.

Abstract

This thesis presents a categorization of conceptions about digital threats on web applications with a study showing the economic consequences of cyber-attacks. The aim of this thesis is to contribute to a scientific article, which can be valuable to the public, as well as for future work and employment.

Constant comparison method was used to analyse aggregate perceptions. The results reveal several exciting findings for theory and practice, where perceptions of the cyber world were presented in order to understand more how others see cybersecurity today. It also shows significant variations among the participants' perceptions. This shows that information security, even if it is gradually developed, has a long way to go until it becomes an unbroken part of the business.

This study can also serve as a guide for the different perceptions of cyber-attacks as it provides an overview of the most relevant cyber-attacks today. This thesis was supplemented with a study that highlights the economic consequences of cyberattacks. In addition to this, the cyber-attack on Coop during the summer of 2021 was also studied.

Keywords
Security, cyber-attack, economic, digital threats, web applications, cyber security.

Förord

Rapporten presenterar det examensarbete som utförts under höstterminen 2021 på högskoleingenjörsprogrammet med inriktning datateknik och ekonomi vid Kungliga Tekniska Högskolan, KTH. Detta arbete motsvarande 15 högskolepoäng, och är utförd av Elyas Alyoussef på uppdrag av Fredrik Heiding, doktorand vid Network and Systems Engineering, KTH.

Grundläggande kunskaper inom datavetenskap och ekonomi kan behövas för att kunna tillgodogöra sig vissa delar av rapporten.

Kursiv text i detta examensarbete motsvarar engelska termer som inte är lämpliga att översättas till svenska.

Arbetet har utförts med handledning av Fredrik Heiding som jag vill tacka för den hjälp jag fått. Jag vill även tacka alla som har bidragit till genom att svara på enkäten eller lämna åsikter för insamling av uppfattningar.

Tekniska termer beskrivs i en ordlista på nästa sida och markeras senare i rapporten med kursiv stil.

Ordlista

Datasäkerhet: uppstår från önskan att dela på tillgängliga resurser på ett säkert sätt utan att det inträffar några digitala hot som kan vara bland annat *leakage* (läckage), *tampering* (datamanipulering) eller vandalisering och störning av systemet funktionalitet [1].

Webbapplikationer: applikationer som kan köras på webben genom att erbjuda olika tjänster för användaren [1].

Skadlig programvara: all programvara som har utformats för att fungera på ett skadligt, oönskat sätt, utan informerat medgivande från datorägaren eller användaren [1].

Ransomware: skadlig programvara som lagrar data från en datoranvändare och som släpps mot en lösen [2].

SOC står för *Security Operation Center*: En SOC fokuserar vanligtvis inte bara på säkerhetsoperationer (som hantering av säkerhetsenheter) utan också på hot- och sårbarhetshantering, proaktiv övervakning och incidentkvalificering [2].

Mimikatz [3] är en öppen källkodsapplikation som används för att se och spara autentiseringsuppgifter på ett system.

LaZagne [4] är ett verktyg med öppen källkod som används för att återställa lagrade lösenord på ett system.

RAT (Remote Administration Tool) [5] är ett program som tillåter en användare att fjärrstyra en annan dator.

sssssssssssssssssss

Innehållsförteckning

1 Inledning

I detta kapitel beskrivs bakgrund, problemställningen som ligger till grund för detta examensarbete tillsammans med motivering och förklaring. Det presenterar också målsättningen med examensarbetet samt de avgränsningar som inträffade.

1.1 Problemformulering

Internetanvändningen växer snabbt med stort behov att kunna dela data med andra. Därmed behöver även kunskap inom cybersäkerhet växa snabbt för att garantera ett säkert sätt att dela på resurserna. Moderna organisationer lägger generellt mycket tid på att förbättra sitt digitala skydd. Även privatpersoner blir allt mer medvetna om vikten av cybersäkerhet och vilka potentiella konsekvenser deras digitala handlingar kan leda till. Detta är en rimlig effekt av det ökande antalet cyberattacker som sker över hela världen, både riktade mot individer och organisationer. Ransomware har kommit att dominera den nuvarande data-säkerhetsdiskursen. Därför hålls företag av alla storlekar som offer i den moderna varianten av detta brott.

Även om medvetenheten om cyberattacker i allmänhet ökar, kanske allmänhetens åsikter om vad som är farligt respektive säkert, inte alltid är i linje med den faktiska sanningen. Vissa cyberattacker kan uppfattas som mycket farliga, medan de egentligen kan övervinnas ganska enkelt. Andra hot kan uppfattas som ofarliga, medan de i själva verket kan vara förödande.

Cyberattacker kan leda till stora ekonomiska konsekvenser för hela samhället i stort, för enskilda verksamheter och även för privatpersoner varvid är det viktigt att förstå och studera dessa konsekvenser. Arbetet kombineras även med en studie på Coops verksamhet, som drabbades hårt av cyberattacker under sommaren 2021. Studie med Coop har till syfte att veta hur cyberattacker påverkade verksamheten ur ett ekonomiskt perspektiv.

1.2 Målsättning

Målet med detta examensarbete är att kategorisera information om hur allvarliga olika cyberattacker mot webbapplikationer är, och jämföra denna riskbedömning med hur allvarliga allmänheten tror att de är. Huvudmålet är att jämföra allmänhetens uppfattning av webbaserade cyberattacker mot hur farliga experter anser att de är. Målen med denna studie är att kunna få en kvantifierbar (mätbar) data om allmänhetens, IT-intresserades samt experters uppfattningar av olika cyberattacker. Utöver detta görs en kortare analys av de ekonomiska konsekvenserna

av cyberattacker för samhället i stort samt med en studie som tar upp attacken mot Coop som ett exempel för enskilda företags konsekvenser.

1.3 Avgränsningar

Tidsaspekten för detta examensarbete är begränsad. Därför har inga större fördjupningar utförts, utan rapporten begränsades till en grundläggande studie.

Deltagandegraden var lägre än den förväntade med tanke på delningar på sociala medier.

Dataanalysen gjordes med endast en metod som är konstant jämförande metoden.

Andra svårigheter har inträffat för att kunna hitta experter som är intresserade att svara på frågor då formuläret inte var riktad till definierad grupp, utan urvalet av personerna var systematiskt.

2 Teori och bakgrund

Detta kapitel tar upp bakgrunden till examensarbetet med sammanfattning av den forskning som gjorts tidigare inom ämnesområdet som är aktuella för arbetet.

Organisationer utsätts för riktade och allt mer sofistikerade cyberattacker som resulterar i dataintrång, betydande driftstörningar, ekonomiska förluster och andra långsiktiga konsekvenser, enligt *Tweneboah-Koduah S, Atsu F, Prasad R* [6]

G. Coulouris, J. Dollimore, T. Kindberg och G. Blair [1] hänvisar till några digitala hot som kan uppstå mot delad data, så som avlyssning (*eavesdropping*), maskering (*masquerading*), manipulering av meddelanden (*message tampering*), återuppspelning eller *denial of service*.

Cyberattacker och utpressning är egentligen inte ett teknologiskt problem, utan de är ett brott. *Orange Cyberdefense* relaterar cyberangripare till ett specifikt politiskt, ekonomiskt och kulturellt sammanhang. Ökningen av cyberattacker drivs främst av sociala och kulturella drivkrafter. Vidare ligger konvergensen av teknologi och ekonomi som en grund för dessa attacker [2].

På *Orange Cyberdefense* [2] relateras de olika risker och cyberattacker till varje applikation i sig. Med andra ord måste undersökningar och studier göras för en specifik applikation för att kunna definiera och identifiera möjliga risker. Beroende på applikationen och vad den innehåller för känslig data kan en rangordning på hur farliga de möjliga attackerna är göras. Experter på *Orange Cyberdefense* menar att i komplexa system kommer det finnas många olika faktorer som samverkar med varandra för att definiera och ordna riskerna.

Ett vanligt tillvägagångssätt för att genomföra en cyberattack är att angriparen utnyttjar systemets svagheter för att ta sig in och kunna röra sig fritt, enligt *Orange Cyberdefense* [2]. Detta inkluderar att en slutanvändare kan bli utsatt för bland annat:

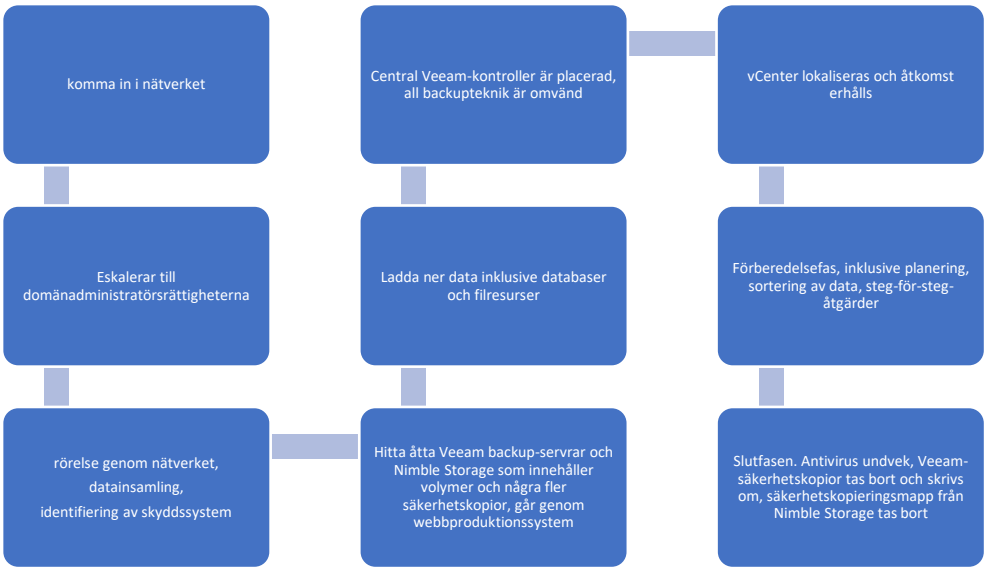
- Nätfiske (*phishing)*; att få användaren att avslöja personlig information, såsom lösenord eller kreditkortsnummer.
- Social ingenjörskonst (*social engineering*); att manipulera personer till att göra olika handlingar eller avslöja hemlig information, i stället för att själv göra intrång.
- Lösenordssprayning (*password spraying*); att angriparen testar de vanligaste användarlösenorden på ett stort antal konton.
- *Brute force* tekniker mot utsatta *RDP*-servrar; *RDP* står för *Remote Desktop Protocol*, med denna attacktyp försöker angriparen att få obehörig åtkomst till ett konto genom att gissa lösenordet.

Det är dock inte bara användare som kan riskeras, utan även själva systemet kan skadas genom att använda lokala privilegieskaleringssårbarheter (*PrivEsc*). Detta gör att angriparen lättare kan komma åt autentiseringsuppgifter, samt skapa skadlig

kod, ta kommando/kontroll, sidorörelser, tjänstemanipulation och slutligen kryptering, menar *Orange Cyberdefense* [2].

ContiLocker-teamet på *Orange Cyberdefense* [2] har presenterat ett flödesschema för en ransomware attack. Figur 2.1 beskriver hur en attack kan se ut enligt teamets erfarenheter. Syftet med denna tidslinje är att visa att en bekräftad ransomware faktiskt är det sista steget i en lång och komplex kedja av händelser.

Enligt *Orange Cyberdefense* [2] börjar attacken med extern spaning, där angriparen försöker hitta möjliga sårbarheter i systemet och komprometterade referenser utanför offrets informationssystem. Sedan ska samlad information och sårbarheter användas för att kunna komma in i systemet (*phishing*), med hjälp av ett legitimt inloggningskonto på fjärråtkomst och skadlig programvara (spam). Därefter när angriparen väl är inne i systemet börjar den inre spaningen genom att försöka identifiera säkerhetslösningar och upptäcka domänens servrar. Ett nytt steg börjar med det som kallas för *Privilege Escalation* där andra applikationer kan användas som Mimikatz eller LaZagne. Sedan får angriparen mer flytande för att kunna kontrollera och styra systemet med hjälp av bland annat RAT. Till sist är det möjligt för angriparna att utnyttja offret genom kryptering av tillgängliga data eller kopiera offrets identifikation och destruktion.



Figur 2.1 visar en attack steg för steg enligt *ContiLocker*-teamet efter att angriparen har kommit in i systemet [2].

G. Coulouris, J. Dollimore, T. Kindberg och G. Blair [1] hänvisar till en annan störning genom att inleda distribuerade *denial-of-service-attacker* (DDoS) mot ett offer. Detta resulterar i en överbelastning av fysiska resurser genom att göra många meningslösa anrop på tjänster eller meddelandeöverföringar i ett nätverk. DDoS kan vara särskilt utmanande för ett system som redan har blivit attackerat och försöker återhämta sig från den föregående attacken. DDoS kan också skapa stora störningar

på vissa applikationer där ett driftstopp kan vara extremt skadlig, såsom inom hälso- och sjukvård eller finansiella tjänster.

En annan attack som kan vara en favoritingång till ransomware är *Cryptojacking*. På senare tid har populariteten för kryptovalutor som Bitcoin ökat kraftigt. För att skapa nya enheter av kryptovalutor, måste komplexa matematiska beräkningar utföras [7]. En användare som slutför en beräkning belönas med ett litet pris av den kryptovalutan. För att öka sina vinster använder sig angriparen av andras enheter och elektrisk kraft. Detta kallas *Cryptojacking*. Med andra ord utvinner angriparen illegala kryptovalutor, genom att använda offrets dator, datorminne och processorkraft för att generera nya enheter, menar Pranshu Bajpai och Richard Enbody [8]. Cryptojacking kan använda komplexa metoder för att utföra hela arbetet utan att upptäckas, och enligt en studie upptäcks endast cirka 50 procent av dessa attacker.

Som en följd av kryptovalutors popularitet, ökar en attacktyp som kallas för SIM-byte (SIM swapping). SIM står för subscriber *identity module*, och är ett sätt som angriparen använder för att ta över ett konto, genom att lura en mobiloperatörsanställd att omdirigera en abonnents telefonnummer till en hackers SIM-kort. Detta gör det möjligt för angriparen att avlyssna offrets 2FA-koder vilket hjälper till att hitta de privata nycklar som används för att komma åt ett kryptovalutakonto, enligt *Cybercrime Magazine* [9].

OWASP [10] listar löpande de tio mest kritiska säkerhetsriskerna och sårbarheter för webbapplikationer.

- OWASP anger Broken Access Control, det vill säga möjligheten för en användare att agera utanför sina avsedda behörigheter, som den mest förekommande risken för webbapplikationers säkerhet under 2021.
- Kryptografiska fel det vill säga att känsliga data kan bli exponerade och även leda till att ha inflyttande över systemet, kommer på andra platsen.
- På tredje plats kommer injektion, som betyder att en användare medvetet kan mata in information för att komma åt känslig information.
- Sedan kommer osäker design, där utvecklarna inte har tänkt på hotmodellering, säkra designmetoder, inte heller en bra infrastruktur när de byggde applikationen.
- Utöver dessa nämner OWASP andra risker som: säkerhetsfelkonfiguration, föråldrade sårbarheter och komponenter, identifierings- och autentiseringsfel, programvara och dataintegritetsfel, säkerhetsloggning och övervakningsfel samt förfalskningar på efterfrågan från serversida.

TrustNet [11] presenterar de mest förekommande attacker för webbapplikationer där *Cross-site scripting (XSS)* rankas som den vanligaste attacktypen. XSS påverkar webbapplikationens säkerhetsfelkonfiguration genom att en angripare laddar upp en bit skadlig skriptkod till webbplatsen som i sin tur kan användas för att på något sätt skada webbapplikationen. På andra plats rankas SQL-injektion (SQLI). På tredje plats rankas bana traversering som också förekommer på grund av injektion och

felaktigt skydd av data som har matats in och resulterar i att angriparen kan få åtkomst till information som är lagrad på enheters hårddiskar. Sedan kommer Inkludering av lokal fil på fjärde plats, det vill säga att en webbapplikation tvingas att köra en skadlig fil som angriparen skickar till systemet. Sist på listan kommer *DDoS* attacker.

2.1 Relaterade studier

Denna sektion presenterar de relevanta studier som tidigare gjort och är relaterade till detta arbete.

Det finns en del studier som tar upp cybersäkerhet och försöker hitta lösningar genom att bland annat analysera ramverk för cyberriskbedömning och andra risker som kan inträffa ett system som (Kamalanathan K. et al. 2020 [12]) studie eller att använda AI (artificiell intelligens) tillsammans med maskininlärningsteknik för att uppnå bättre cybersäkerhet så som (Abhinav J et al. 2021 [13]; Anand H et al. 2019 [14]) studie.

För att mildra konsekvenserna som kan uppstå på grund av cyberattacker, har andra studier även gjort etiska principerna inom IT-säkerhet och hackning, som (Fredrik Heiding, Robert Lagerström 2021 [15]), genom att lära personer som arbetar med cybersäkerhet, med etisk kunskap, hur och när de ska använda sina förvärvade erfarenheter.

Nuförtiden blir fler analoga enheter digitala, detta kallas för IoT-enheter. Även användning av IoT-enheter ökar snabbt, både i antal och funktionalitet. Därmed måste IoT-applikationer utformas på säkert sätt då enheterna är kopplade till internet och kan utsättas för olika attacker och hot. Några studier, som (Angelo F. et al. 2017 [16]), tar upp hur dessa applikationer kan utformas på ett säkert sätt. Andra studier, bland annat (Heiding F. et al. 2020 [17]), undersöker hur säkerheten ska förbättras i dessa enheter.

3 Metoder

I detta avsnitt ges en beskrivning för vägen från problemet i avsnitt 1.2 till att kunna uppfylla målen i avsnitt 1.3.

För att besvara problemformuleringen har en litteraturstudie samt enkätundersökning utförts. Litteraturstudien gjordes för att definiera och studera tidigare arbeten om säkerhetsrisker för webbapplikationer och cyberattacker samt möjliga ekonomiska konsekvenser av attacker. Vidare har en enkätundersökning gjorts i syfte att samla uppfattningar om cybersäkerhet.

Enkätundersökningen gjordes med hjälp av ett Google-formulär. Formuläret skrevs på engelska för att inte vara begränsad till svensktalande personer. Detta formulär finns även som en bilaga på slutet av denna rapport. För att gruppera enkätdeltagarna fokuserade insamlingen även på tre grupper som är:

1. Personer som anser sig vara experter inom säkerhet och cyberattacker.
2. Personer som arbetar med- eller studerar IT men som inte har fokus på cybersäkerhet.
3. Personer utan särskilda kunskaper inom IT.

Utformning av undersökningen har baserats på Georgiadou et al. 2020 [18] studie, då den var avsedd att samla uppfattningar om cybersäkerhet under SARS-CoV-2-pandemin. Detta betyder att ett antal kriterier behövde uppfyllas såsom tidslängd, tillgänglighet, och tydlighet.

- Tidslängd: för att öka deltagandet för undersökningar utan personlig vinning bör denna typ av enkät vara kort och lätt att besvara.
- Tillgänglighet: eftersom många personer i nuläget arbetar hemifrån behövde undersökningen digitaliseras. En digital enkät möjliggjorde också att personer över hela världen kunde delta.
- Tydlighet: Undersökningen riktade sig inte till en definierad population. Detta betyder att deltagarna inte nödvändigtvis är bekanta med tekniska termer och informationssäkerhet. Följaktligen behövde frågorna vara enkla med hjälptext för att förklara använda termer för att tydliggöra frågorna.

Med hänsyn till ovanstående skapades ett webbaserat frågeformulär med totalt 18 frågor. Varje fråga gjordes med syfte att få en generaliserad feedback med möjlighet att lägga till kommentarer. En första version av frågeformuläret gjordes. Därefter fick fem personer med olika tekniska kunskaper granska och förbättra enkäten. Detta gjordes med syfte att testa undersökningens validitet genom att se till att alla ovanstående kriterier uppfylldes.

Eftersom syftet bakom insamlingen inte var att definiera populationen exakt blev urvalet av personerna systematiskt. Enkäten delades på sociala medier under två veckor, från 23 november 2021 till 8 december 2021, och personerna fick delta genom att svara på frågorna i formuläret.

Valet av frågorna i undersökningen har baserats på Nora Cate Schaeffer och Jennifer Dykema studie [19]. Författarna menar att efter förståelse av bakgrunden bör frågorna utformas för att vara en grund för framtida studier. Detta betyder att frågorna bör formuleras för att nå examensarbetets mål samt för att vara en grund för kommande studier. Därför bör frågorna undersöka deltagarnas

- uppfattningar om personliga- och företagsrisker samt medföljande ekonomiska konsekvenser,
- kännedom om olika cyberattacker och anledningarna bakom dem
- uppfattningar om allvarlighetsgrad för specifika cyberattacker och hur troligt det är att de kan påverka ett företag.

Professor Schuman [20] menar att det går att använda sig av både öppna och stängda frågor i en enkät. Enkätundersökningen valdes att utforma på detta sätt. Svarsalternativen fanns för att först ge personer som inte har bra kännedom om området olika svarsalternativ att välja mellan. Vidare för att få användbara svar och därmed för att kunna hantera svaren på ett bra sätt. Möjligheten att lägga till kommentarer fanns för att inte begränsa deltagarnas svar.

I första delen fick personerna svara på frågor som var inriktade mot dem själva, såsom hur troligt det är deltagaren själv kommer att drabbas av en cyberattack och om det skulle inträffa, hur mycket pengar det skulle kosta.

Andra delen var inriktad mot företag och personerna fick svara på frågor som hur troligt det är att ett företag kan drabbas av en cyberattack och hur mycket pengar en attack skulle kosta.

I tredje delen fick deltagarna ange vilka huvudsakliga orsaker det finns för att utföra cyberattacker.

I den fjärde och sista delen ställdes frågor kring fyra typer cyberattacker: nätfiske, social ingenjörskonst, lösenordssprayning och *brute force* tekniker mot utsatta *RDP*-servrar. Personerna fick svara på om de kände till respektive tillvägagångssätt eller inte, samt hur allvarlig attacken kan vara och hur troligt ett företag kan påverkas av attacken.

Svaren på frågorna som tar upp olika uppfattningar (såsom hur troligt, hur farligt eller hur mycket pengar) fördelade som linjär skala från noll till fem, där noll är minsta värdet och fem är högsta. Andra frågor (som vad tror du) hade svarsalternativ med möjlighet att lägga till kommentarer till det valda svaret. Frågorna presenteras i **Tabell 3.1** uppdelat i fyra kategorier. Formuläret i sin helhet finns i bilaga 1.

Tabell 3.1 visar ställda frågor i formuläret.

Del 1	• Hur troligt tror du att du kan drabbas av en digital attack? • Hur mycket pengar tror du att en attack kan kosta dig?
Del 2	• Hur troligt tror du att ett företag kommer att påverkas av en digital attack? • Hur mycket pengar tror du att en attack kan kosta den drabbade verksamheten?
Del 3	• Vad tror du är de huvudsakliga anledningar bakom cyberattacker? Följande svarsalternativ fanns: ekonomisk, politisk, sociokulturell och teknologisk, med möjlighet att lägga till andra anledningar.
Del 4	Frågorna berörde fyra typer cyberattacker: nätfiske, social ingenjörskonst, lösenordssprayning och *Brute force* tekniker mot utsatta *RDP*-servrar. För varje attacktyp fick man följande frågor: • Kort förklarning till attacktypen och med frågan om personen hade kännedom till den sedan tidigare • Hur skadligt tror du att attacken är? • Hur troligt tror du att ett företag kommer att påverkas av denna attack.

För analys av enkätundersökningen har den konstant jämförande metoden använts [21], som är mer kopplad till den kvantitativa forskningen än den kvalitativa, där varenda ny fynd eller uppfattning jämförs med befintliga fynd och information. Glaser och Strauss (1967) hänvisar till den konstant jämförande metoden som följande "*constant comparative method of qualitative analysis*." [22].

Konstant jämförande metoden använder sig ut av ständig jämförelse mellan data som samlas och data som redan finns som en kvalitativ data. Dessa ständiga jämförelser bidrar till forskningens validitet. Jämförelserna är oftast förknippade med induktiva resonemang snarare än deduktiva resonemang, då de är som en iteration eller som Silverman (1993) menar "*analytic induction*" [23]. Med andra ord kan man säga att metoden förknippas med den idiografiska (*idiographic*) filosofin som är relaterad till forskning och vetenskapliga fakta, snarare än den nomotetiska (*nomothetic*) filosofin som är relaterad till allmänna eller universella normer eller lagar, och förhållningssätt.

Denna metod kombinerar textkodning i en mindre systematisk och hård grad än andra metoder såsom innehållsanalys. Glaser och Strauss [22] menar att metoden, till skillnad från metoder som analyserar all tillgängliga data på djupet såsom analytisk induktion, inte kräver övervägande av all tillgängliga data. Samt att det inte finns begränsningar till en definierad typ eller definierade fall. Därför anses denna metod vara särskilt lämpad för detta arbete eftersom metoden kan tillämpas med

hjälp av olika typer av kvantitativa information såsom intervjuer, insamlingar, och artiklar.

För att genomföra litteraturstudien har, utöver artiklar och böcker från KTH Biblioteket, även material hämtats följande källor:

- *Orange Cyberdefense,* som definierar sig som Europas ledande leverantör av säkerhetstjänster. De hjälper företag att bygga ett säkrare system och har mer än 25 års erfarenhet inom informationssäkerhet.
- *MITER ATT&CK®,* som är en global kunskapsbas baserade på verkliga observationer och används som en grund för utvecklingen av specifika hotmodeller och metoder med syfte att lösa problem för en säkrare värld.
- *Varonis,* som är en säkerhetsleverantör för mer än 7000 kunder och fokuserar på att säkra data mot möjliga cyberattacker.
- *McAfee,* som är ett välkänt antivirusprogram som skyddar applikationer, nätverk och enheter över hela världen.
- *TrustNet,* som är en global leverantör för säkerhet, konsulttjänster och efterlevnads tjänster sedan mer än 15 år.
- Cybersecurity Ventures, som är världs ledande inom cybersäkerhets forskning och cyberekonomi. Cybercrime Magazine publicerar Cybersecurity Ventures rapporter och studier.

4 Resultat

I detta kapitel presenteras examensarbetets resultat. Under sektion 4.1 beskrivs resultat från litteraturstudier. Under sektion 4.2 och 4.3 presenteras resultaten av enkätundersökningen, detaljerat respektive sammanfattat. Därefter presenteras resultat om cyberbrottsligheters ekonomiska konsekvenser i hela världen i sektion 4.4. Avslutningsvis presenteras resultaten från analysen över hur cyberattacker påverkar enskilda företag i sektion 4.5, med Coop som exempel.

4.1 Resultat från litteraturstudier.

För att kunna förstå varför cyberattacker finns, studerar *Orange Cyberdefense* [2] de olika anledningar bakom cyberattacker, det vill säga om anledningen till utveckling av detta problem är mer politisk, ekonomisk, sociokulturell eller teknologisk. Resultatet av denna studie visar att sociokulturella och tekniska faktorer spelar störst roll för denna typ brottslighet. Vidare kommer cyberutpressning att finnas kvar eftersom samhället har byggt och fortsätter att bygga ett tekniklandskap som i själva verket inte kan skyddas från komplicerade attacker.

För att kunna kartlägga vilka attacker som kan inträffa i ett system, behöver det aktuella systemet studeras med syfte att identifiera de tillgångar som kan vara intressanta för angriparen samt för att upptäcka aktiva attacker och svagheter menar *Orange Cyberdefense* [2].

90 procent av alla rapporterade attacker härrör från nätfiske och social ingenjörskonst, det vill säga genom att skicka e-postmeddelanden för att locka sina mottagare att klicka på en länk, öppna ett dokument eller vidarebefordra information till angriparen eller någon annan obehörig, enligt John P. & Mello, Jr [24].

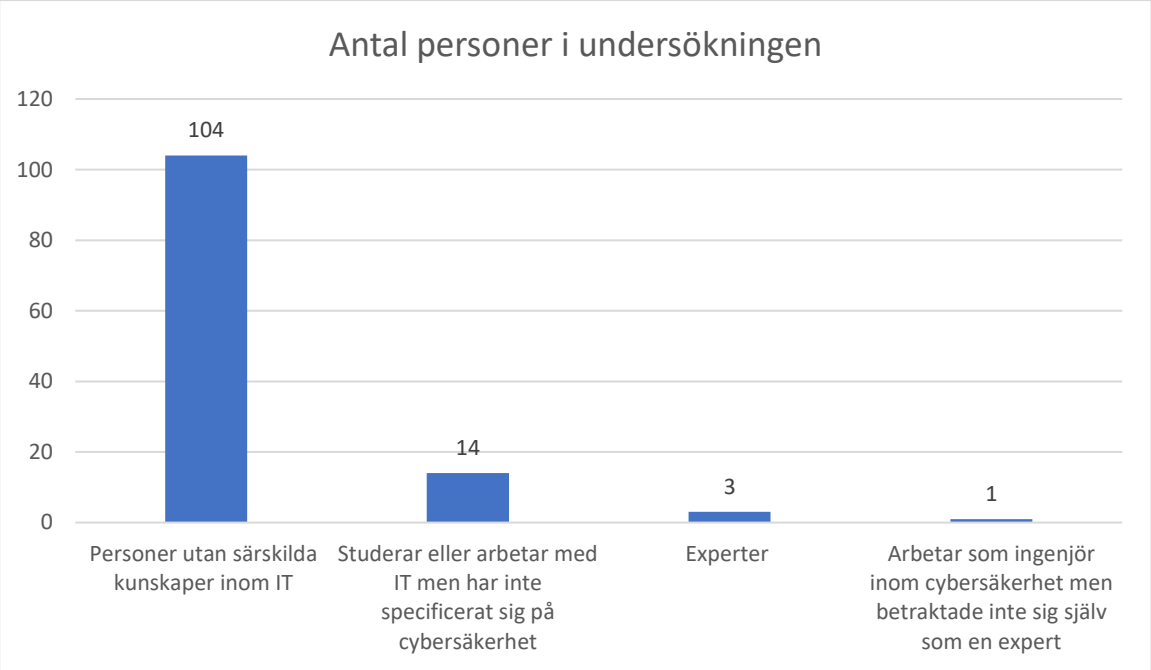
Vad beträffar försäkring mot cyberattacker, visar en studie att 68 procent av amerikanska företag inte har någon form av försäkring mot cyberattacker, enligt *Cybersecurity Ventures [9]*. Däremot visar en undersökning från Wall Street Journal år 2018 [25] att en majoritet av de mest folkrika städerna i USA har cyberförsäkring eller funderar på att köpa den.

Inom EU finns en dataskyddsförordning sedan 2018, GDPR (General Data Protection Regulation), som hjälper till att sprida förståelse för cyberattacker genom att se till att företag, myndigheter, organisationer med flera, lagrar användardata på ett säkert sätt [26]. Samtidigt visar en rapport av Enterprise Risk Magazine [27], att cybersäkerhet är den största risken som organisationer i hela Europa sannolikt kommer att möta under de kommande åren.

4.2 Resultat från enkätundersökning

I detta avsnitt presenteras resultaten från enkätundersökningen samt ett urval av deltagarnas kommentarer. När det råder enighet om ett svar presenteras svaret direkt. I detta fall där svaren från deltagargrupperna skiljer sig mycket åt presenteras svaren med diagram med syfte att underlätta förståelse för dessa svar.

Totalt deltog 122 personer i undersökningen. En majoritet av dem, 104 personer eller ca 85 %, ansåg sig inte ha särskilda kunskaper inom IT och IT-säkerhet. Övrig fördelning var 14 personer som studerar eller arbetar med IT, dock ej med cybersäkerhet specifikt, 3 experter samt 1 person som arbetar som ingenjör inom cybersäkerhet, men som själv inte betraktar sig som expert. Se även Figur 4.1.



Figur 4.1 visar antal deltagare i undersökningen.

För att studera och analysera svaren med hjälp av konstant jämförande metoden kommer jämförelserna göras uppdelat på formulärets fyra delar. Svaren från personen som arbetar som ingenjör inom cybersäkerhet, men som själv inte betraktar sig som expert, kommer grupperas med experterna svar. Detta då personen bedöms ha direkt kontakt med experter. I övriga resultat kommer de tre grupperna benämnas

- Allmänhet: personer som saknar särskilda kunskaper inom IT och IT-säkerhet.
- IT-intresserade: personer som arbetar med- eller studerar IT men som inte har fokus på cybersäkerhet.
- Experter: personer som är experter inom säkerhet och cyberattacker.

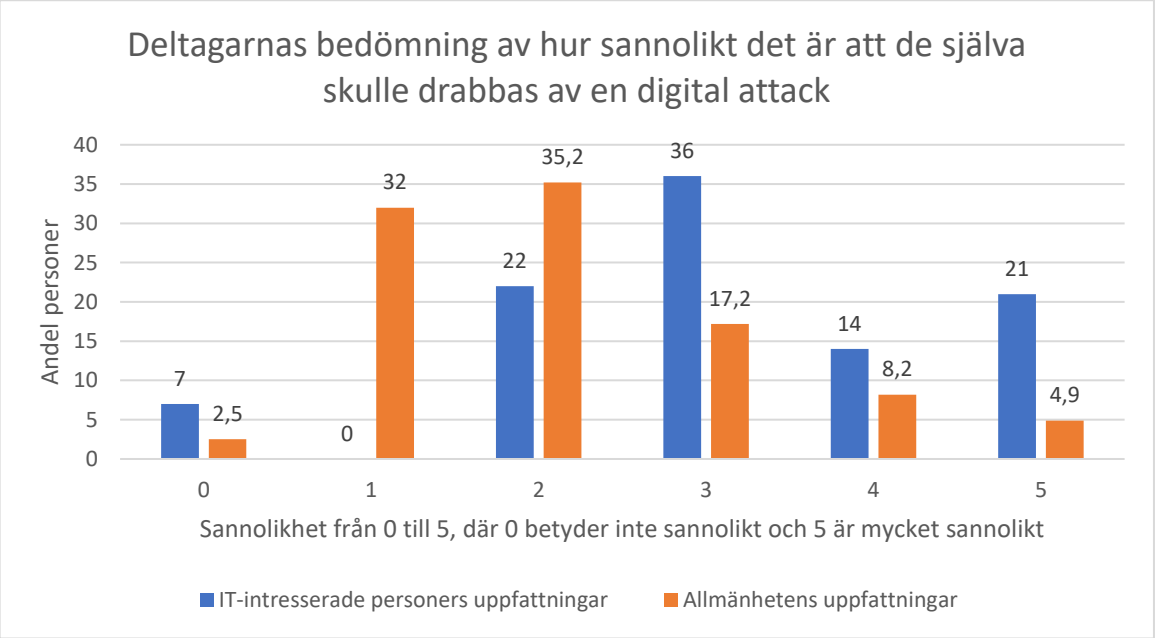
4.2.1 Uppfattningar om personliga risker

På frågan om hur troligt experterna tror att de, som enskilda personer, kan drabbas av en digital attack, blev svaret 3, med andra ord bedöms sannolikheten vara medelhög.

Figur 4.2 visar de samlade svaren för både allmänheten och IT-intresserade personer, där frågas om hur troligt personerna tror att de kan drabbas av en digital attack. IT-intresserade personer svarade som följer: 7 procent valde 0 (ingen sannolikhet), 22 procent valde 2 (måttlig sannolikhet), 36 procent valde 3 (medelhög sannolikhet), 14 procent valde 4 (hög sannolikhet) och 21 procent valde 5 (mycket hög sannolikhet).

En kommentar från de IT-intresserade personerna var från en person som tidigare drabbats av en digital attack, där dennes inloggningsuppgifter och annan kontoinformation läckt ut. Efter attacken väljer personen mer ovanliga och komplexa lösenord.

En annan kommentar var att plattformar och sociala medier som personen använder är hotade av cyberattacker men att personen inte tror att hen personligen är ett mål för angriparna. En annan person menade att det mesta av värdefulla data numera är digitaliserat och varje attack kommer att påverka hen direkt.



Figur 4.2 visar en jämförelse av allmänhetens- och IT-intresserade personers uppfattningar om möjlighet att en individ kan drabbas av en digital attack.

Allmänhetens svar på frågan var följande: 2,5 procent valde 0 (ingen sannolikhet), 32 procent valde 1 (låg sannolikhet), 35,2 procent svarade 2 (måttlig sannolikhet), 17,2 valde svaret 3 (medelhög sannolikhet) samt 8,2 valde 4 (hög sannolikhet) och 4,9 valde 5 (mycket hög sannolikhet). Några kommentarer lades till på denna fråga

från allmänheten såsom att en person inte tror att en attack kan drabba hen direkt då personen inte är känd.

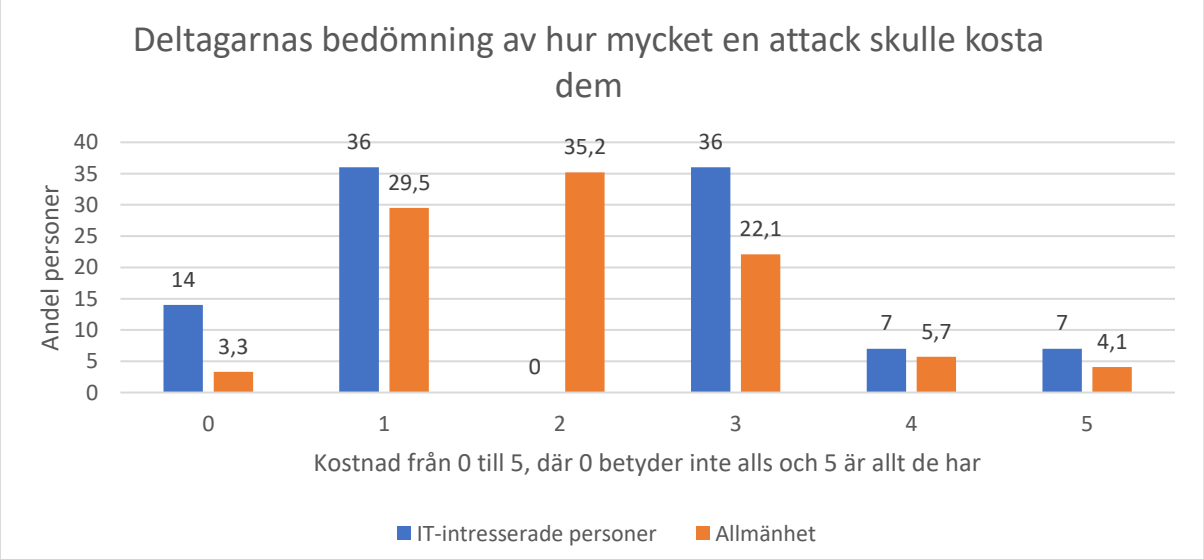
En annan kommentar var från en person som använder applikationer som möjliggör att en stor mängd personligdata kan samlas in, till exempel *Google* eller *TikTok*. Samma person menar att hen är medveten om att sin data i princip är offentlig och att lösenorden kan läcka då och då för dessa applikationer. Däremot är hen mindre orolig för attacker som är inriktade på känslig data så som bankkonto.

Vid jämförelse av svaren från de tre grupperna ses följande medelvärden:

- 3 eller medelhög sannolikhet enligt experter
- Olika svar från IT-intresserade personers där majoriteten valde 3 och svaret i genomsnitt blev 3,13. Därför används 3 eller medelhög sannolikhet.
- Olika svar från allmänheten där majoriteten valde 2 och svaret i genomsnitt blev 2,11. Därför används 2 eller måttlig sannolikhet.

Figur 4.3 visar hur mycket både IT-intresserade och allmänhet tror att en attack kan kosta dem. Experterna svarade enhälligt 1, med andra ord bedömde experterna den ekonomiska påverkan vara liten. En kommentar till denna fråga var att experten själv valt att vidta åtgärder mot attacker, så som att säkerhetskopiera sin information vilket leder till att ett ransomware kommer vara verkningslöst. En annan tillägger att känslig information som kan användas för att orsaka ekonomiska förluster, så som *BankID,* är bevakad av säkerhetsprogramvara och hade det inte varit säkert nog skulle förluster varit mycket större.

Bland de IT-intresserade var det 14 procent som valde svaret 0 (ingen ekonomisk påverkan), 36 procent valde 1 (liten ekonomisk påverkan) samt 36 procent valde 3 (medelstor ekonomisk påverkan), 7 procent valde 4 (stor ekonomisk påverkan) och



Figur 4.3 visar samlade svar för IT-intresserade personer och allmänhet om hur mycket pengar en attack kan kosta.

7 procent valde 5 (allt de har). En person berättade att individuella ekonomiska förluster är något som hen har svårt att uppskatta.

Även allmänheten hade varierade svar på frågan om hur mycket pengar de bedömer att det skulle kosta en individ som Figur 4.3 visar. Där 3,3 procent valde 0 (ingen ekonomisk påverkan), 29,5 procent valde 1 (liten ekonomisk påverkan), 35,2 procent valde 2 (måttlig ekonomisk påverkan), 22,1 procent valde 3 (medelstor ekonomisk påverkan), 5,7 procent valde 4 (stor ekonomisk påverkan) och 4,1 procent valde 5 (allt de har). Med detta svar följde några kommentarer såsom att banker i Sverige är välskyddade och det inte är lätt att hacka dem. En annan kommentar bekräftade tilltron till banker och menade att det enda sättet att hen kan föreställa sig att förlora pengar på, är om spelkonton skulle bli attackerade.

Resultatet för den här frågan kan sammanfattas som följande:

- Experter svarade 1 eller liten ekonomisk påverkan
- IT-intresserade gav olika svar men där majoriteten valde 1 eller 3, varvid svaret blev 2,07 i genomsnitt. Därför används 2 eller måttlig ekonomisk påverkan.
- Allmänheten gav också olika svar men där majoriteten valde 2, varvid svaret blev 2,09 i genomsnitt. Därför används 2 eller måttlig ekonomisk påverkan.

4.2.2 Uppfattningar om företagens risker

I andra delen, som fokuserar mer på företag, svarade alla experter 5 på frågan om hur troligt de tror att företagen kan drabbas av en cyberattack. Detta innebär att de bedömer att det är mycket hög sannolikhet för ett företag att bli utsatt för av en cyberattack.

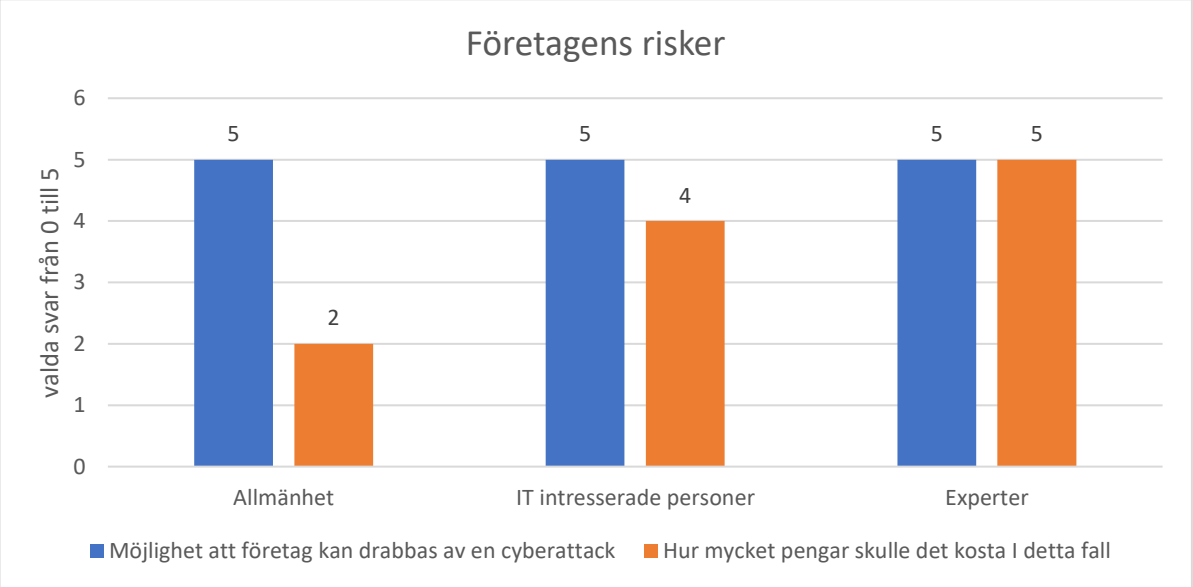
En expert skrev en kommentar, där denne menar att attacker sker hela tiden, men att inte så många attacker är sofistikerade nog för att faktiskt orsaka allvarlig skada. Som svar på hur mycket pengar det kan kosta ett företag ifall en attack har inträffat, blev svaret 5. Så även mycket höga ekonomiska konsekvenser kan förekomma, menar experterna. En expert menade att utöver attacker som är sofistikerade och kan orsaka skador, förekommer även attacker som inte är sofistikerade, så som *DDoS,* men som ändå kan orsaka stora kostnader för företagen.

Som svar på hur troligt IT-intresserade personer tror att företagen kan drabbas av en cyberattack blev avrundat medelvärde 5, vilket betyder att även de tror att risken är mycket stor för företag att bli drabbade av cyberattacker. En person menade att företag påverkas olika av en cyberattack beroende på dess storlek. En annan kommentar var att en digital attack kan stoppa verksamheten totalt. Som svar på frågan om hur mycket pengar det kan kosta företag blev avrundat medelvärde 4, vilket betyder att de anser att höga ekonomiska förluster för attackerade företag kan förekomma. Till denna fråga fanns några kommentarer, såsom att om angriparna fick åtkomst till bankuppgifter för ett företag, skulle företaget antagligen drabbas av

en ekonomisk törn. En annan person menade att en cyberattack även kan ha en inverkan på allmänhetens syn på det berörda företaget eftersom de kommer att vara mindre pålitliga ur ett IT-säkerhetsperspektiv. Ytterligare en person tillägger att företagets förluster beror på den specifika bransch som företaget verkar inom men det generellt kan vara kostsamt att ersätta eller återställa förlorade data efter ett intrång.

På frågan om hur troligt allmänhet tror att ett företag kan drabbas av en cyberattack, blev avrundat medelvärde 5. Det betyder att även allmänheten bedömer att det är mycket troligt att ett företag drabbas av cyberattacker. En kommentar på frågan belyser att allt nuförtiden blir mer digitalt och av detta skäl kan en attack kosta företagen mycket pengar. Som svar på hur mycket en attack kan kosta företagen blev avrundat medelvärde 2. Med andra ord bedömer allmänheten att företag inte förlorar mycket pengar vid en cyberattack. En kommentar på frågan var att företagen förmodligen har bra säkerhetssystem men att små förluster ändå kan förekomma.

Figur 4.4 nedan sammanfattar svaren på frågorna om företagens risker när det gäller både risken att en cyberattack inträffar ett företag och de ekonomiska



Figur 4.4 visar det avrundade medelvärdet för respektive fråga med avseende på företagens risker.

förlusterna.

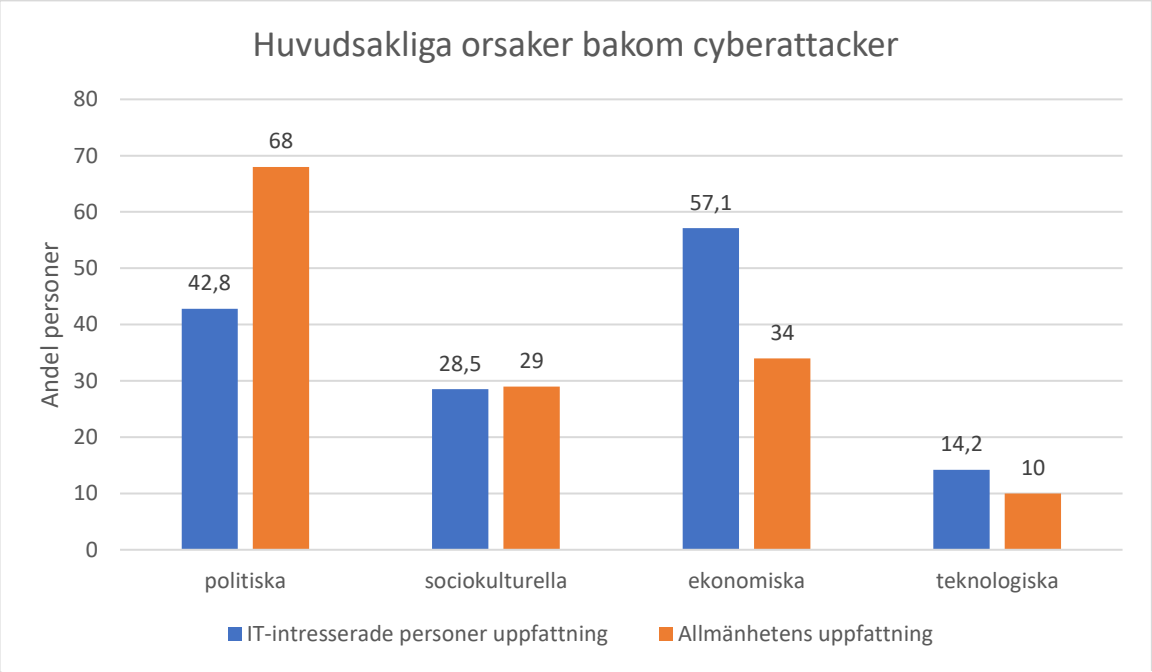
4.2.3 Uppfattningar om huvudsakliga orsaker bakom cyberattacker

I tredje delen frågas om vilka huvudsakliga orsaker det finns bakom cyberattacker. Experter bedömer att den ekonomiska aspekten vara den viktigaste orsaken bakom cyberattacker. I en kommentar belyser en av dem att alla aspekter alltså politiska, sociokulturella, ekonomiska och teknologiska, kan vara huvudsakliga beroende på

vem som attackerar och vem som attackeras. Även andra orsaker kan finnas, så som att visa upp sina förmågor på att förstöra andras system eller med andra ord för kaxighets skull.

Enkätdeltagares uppfattning skiljer sig från *Orange Cyberdefense* som kom fram till att sociokulturella och tekniska faktorer är huvudorsaker bakom cyberattacker.

Figur 4.5 visar allmänhetens- och IT-intresserade personers uppfattningar om vilka orsaker som är huvudsakliga för cyberattacker. Observera att flera svarsalternativ kunde väljas. IT-intresserade personer bedömer den ekonomiska orsaken som viktigaste då den fick mer än 57 procent. Sedan kom politiska orsaker med 42,8 procent, därefter med 28,5 procent kom sociokulturella orsaker och sist kom teknologiska orsaker med 14,2 procent.



Figur 4.5 visar huvudsakliga orsaker bakom cyberattacker enligt både allmänheten och IT-intresserade personer

Allmänhetens uppfattningar var också delad. Bland dem uppgav 68 procent politiska orsaker vara viktiga, 34 procent uppgav ekonomiska orsaker som viktiga, efter det kom sociokulturella orsaker med 29 procent och sist teknologiska med 10 procent.

Sammanfattningsvis konstateras följande:

- Experterna bedömer att de ekonomiska faktorerna är de huvudsakliga orsakerna bakom cyberattacker
- Över 50% av de IT-intresserade bedömer att ekonomiska anledningar är den huvudsakliga orsaken bakom cyberattacker
- Nästan 70 procent av allmänheten anger politiska orsaker som huvudsakliga för cyberattacker

4.2.4 Uppfattningar om olika cyberattacker

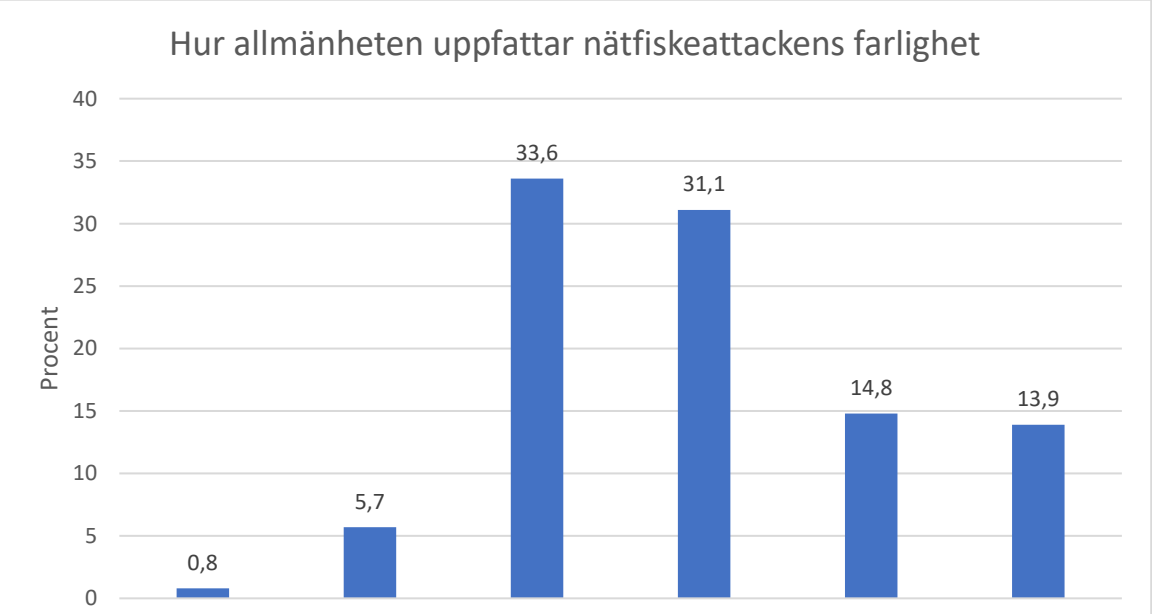
I enkäten berördes fyra typer cyberattacker: nätfiske, social ingenjörskonst, lösenordsspraynings och *Brute force* tekniker mot *RDP*-servrar. I följande avsnitt presenteras resultaten för var och en av dem.

4.2.4.1 Nätfiske

Experter anser enhälligt att nätfiske är ett mycket vanligt tillvägagångsätt för en attack. I en kommentar skrev en av dem att hantering av denna attack beror på personalens kunskap och beteende, samt hur mycket tid och intresse personalen investerar i att motarbeta denna attack. Svaret för attackens allvarlighet bedömdes som 4 av experterna, med andra ord bedömde experterna allvarlighetsgrad för attacken som hög. Svaret för hur troligt det är att ett företag ska utsättas för en nätfiske-attack bedömdes till 5. Detta betyder att de ansåg en mycket hög sannolikhet för detta.

Mer än 90 procent av de IT-intresserade hade kännedom om nätfiskeattacker och de svarade 5 på hur allvarlig den är. Detta betyder att de bedömer attacken som mycket farlig. Samt 4 var svaret på hur troligt det är att en nätfiskeattack kan inträffa, med andra ord det finns en hög sannolikhet för detta.

Av allmänheten svarade 23 procent att de hade kännedom om nätfiskeattacker. **Figur 4.6** visar svarsfördelning för hur allvarligt allmänheten bedömer att nätfiske är, där 0,8 procent svarade 0 (inte skadlig alls), sedan 5,7 procent valde 1 (låg



Figur 4.6 visar allmänhetens uppfattning om nätfiskeattack farlighet.

farlighet), 33,6 procent valde 2 (farligheten är måttlig), 31,1 procent valde 3 (medel) som svar samt 14,8 valde 4 (farlig) och 13,9 valde 5 (mycket farlig).

Utöver detta valde majoriteten 5 som svar på hur troligt det är att en nätfiskeattack mot ett företag kan inträffa. Detta betyder att de ansåg en mycket hög sannolikhet att en nätfiskeattack kan inträffa ett företag. Kommentar till denna fråga var att denna typ av attack är ganska vanlig och att det även kan riktas mot privatpersoner. Till exempel, genom e-post, där äldre personer eller personer med liten IT-vana kan löpa en stor risk.

Det avrundade medelvärdet av resultaten som rör nätfiskeattack presenteras nedan.

Allvarlighetsgrad:

- 4 eller hög enligt experter.
- 5 eller mycket hög enligt IT-intresserade personer.
- 3 eller medelhög enligt allmänheten. Ca 65% av allmänheten svarade 2 eller 3.

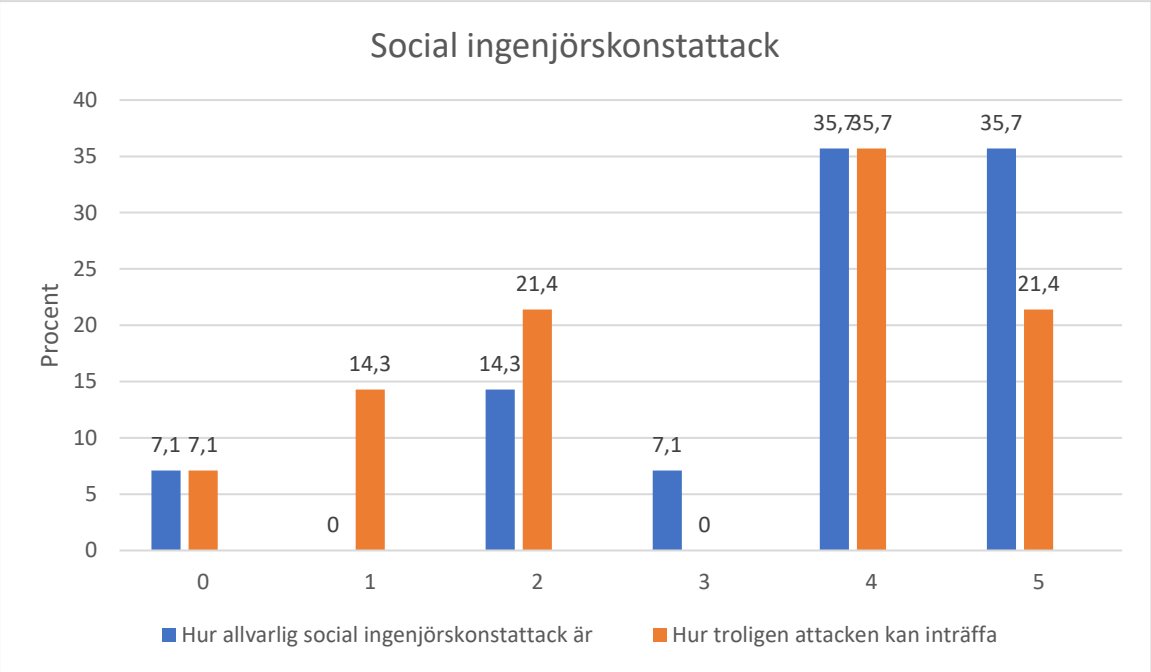
Sannolikheten att attacken kan inträffa:

- 5 eller mycket hög sannolikhet enligt experter
- 4 eller hög sannolikhet enligt IT-intresserade personer.
- 5 eller mycket hög sannolikhet enligt allmänheten.

4.2.4.2 Social ingenjörskonst

För social ingenjörskonst svarade experter 5 på både allvarlighetsgrad och sannolikheten att ett företag drabbas. I en kommentar menade en av dem att människor kan vara naiva och därmed anses denna attack vara mycket allvarlig och svaret var 5. Samt att det är en mycket hög sannolikhet för det ska inträffa.

Bara 40 procent av de IT-intresserade personerna hade kännedom om social ingenjörskonst. Svaren var mer fördelade både vad beträffar hur allvarlig attacken är och hur troligt det är att attacken kan inträffa. **Figur 4.7** visar svaren, där 0 (inte alls farlig/ingen sannolikhet att inträffa) valdes av 7,1 procent på båda frågorna. För bedömningen av attackens allvarlighetsgrad valdes 1 (låg farlighet) av 0 procent, 2 (måttlig farlighet) av 14,3 procent, 3 (medel farlig) av 7,1 procent och 35,7 procent på både val 4 (farlig) och val 5 (mycket farlig).

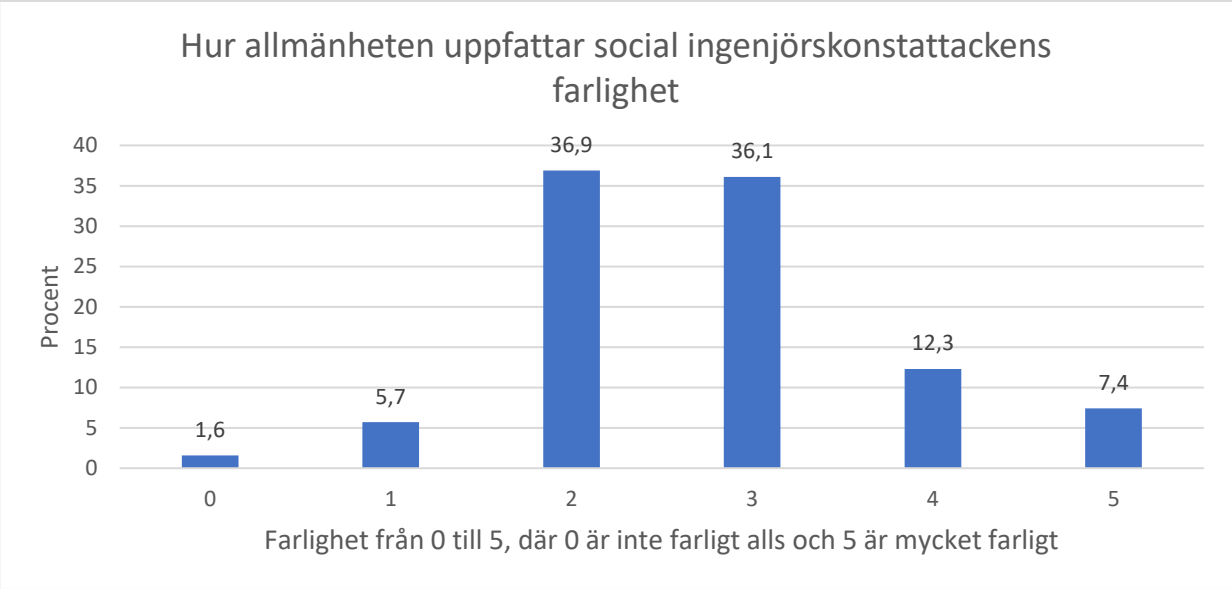


Figur 4.7 visar IT-intresserade personer svar om social ingenjörskonstattack.

Som bedömning för hur troligt det är att attacken kan ske valde 14,3 procent 1 (låg sannolikhet), 2 (måttlig sannolikhet) av 21,4 procent, 3 (medelhög sannolikhet) av 0 procent, 4 (hög sannolikhet) av 35,7 procent och 5 (mycket hög sannolikhet) av 21,4 procent.

En kommentar om social ingenjörskonst var att den oftast är inriktad på personer med låga tekniska färdigheter, där de i högre grad skulle anförtro känslig information om de uppmanas att göra det.

Social ingenjörskonst var en mindre känd attacktyp med mer än 86 procent som inte känner igen attacken. Svaren på hur allvarlig allmänheten tror att denna attack är som **Figur 4.8** visar. Där 1,6 procent valde 0 (inte farlig alls), 5,7 procent valde 1 (låg farlighet), 36,9 procent valde 2 (måttlig farlighet) samt 36,1 procent valde 3 (medelfarlighet), 12,3 procent svarade 4 (farlig) och 7,4 procent svarade 5 (mycket farlig).



Figur 4.8 visar allmänhetens svar på hur allvarlig social ingenjörskonstattack döms vara.

Som svar på hur troligt det är att en social ingenjörskonstattack kan inträffa valde majoriteten av allmänhet 4 (hög sannolikhet), men bara 13,9 procent kände till denna attacktyp sedan tidigare. En person kommenterade att attacken verkar oviktig och ger mindre vinster för en angripare.

Det avrundade medelvärdet av resultaten som rör ingenjörskonstattack presenteras nedan.

Attackens allvarlighetsgrad:

- 5 eller mycket farlig enligt experter.
- 4 eller farlig enligt IT-intresserade personer. En majoritet valde både svaren 4 och 5.
- 3 eller medelfarlig enligt allmänheten.

Sannolikheten att attacken kan inträffa:

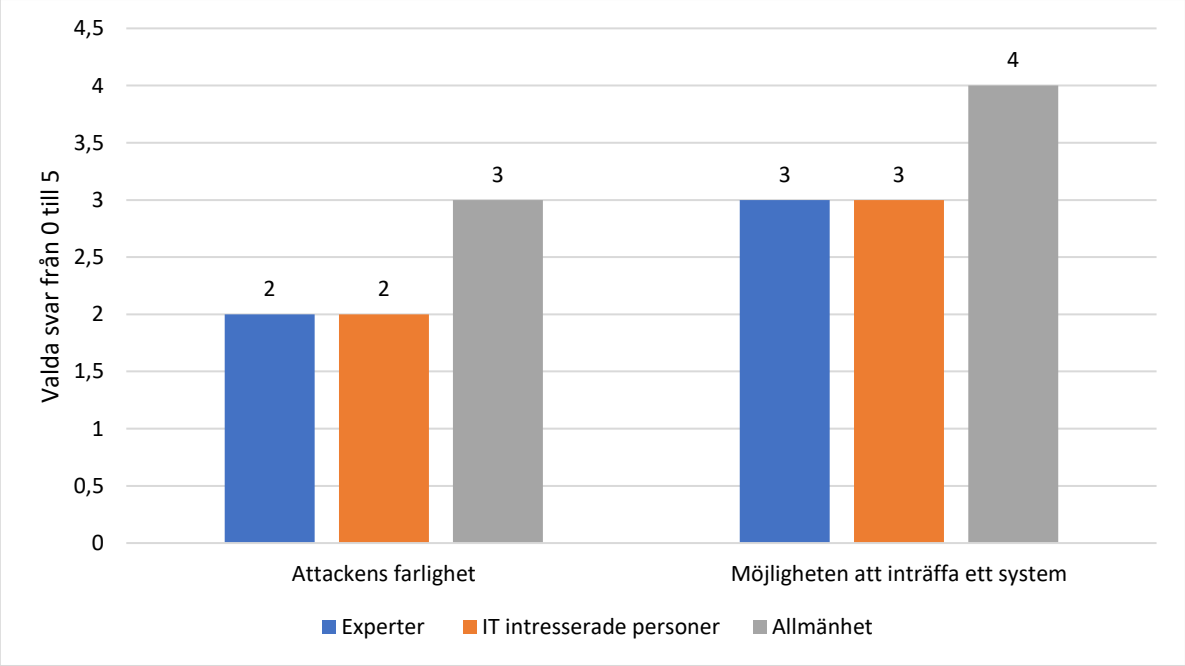
- 5 eller mycket hög sannolikhet enligt experter.
- 3 eller medelhög sannolikhet enligt IT-intresserade personer.
- 4 eller hög sannolikhet enligt allmänheten.

4.2.4.3 Lösenordssprayning attack

För lösenordssprayning svarade experter 2 på hur allvarlig den attacken är, en måttlig farlighetsgrad. En expert menar att lösenordssprayning allvarlighet beror på hur lätt det är att eskalera åtkomsträttigheter. Vidare svarade experter 3 på frågan om hur troligt attacken kan hända, med andra ord finns det medelhög sannolikhet att attacken kan inträffa ett företag enligt experter.

Denna attack var välkänd bland de IT-intresserade då mer än 90 procent hade kännedom till den sedan tidigare. Resultatet visar att personerna valde 2 (måttlig allvarlighetsgrad) som svar på hur allvarlig attacken är. De svarade i genomsnitt 3 (medelhög sannolikhet) på hur troligt det är att denna attack kan hända. En kommentar på denna attack var att detta problem kan relativt enkelt undertryckas genom att se till att effektiva säkerhetsåtgärder används så som kontoåterhämtning via kundsupport och tvåfaktorsautentisering.

En femte-del av allmänheten kände igen lösenordssprayning som attacktyp och majoriteten valde 3 som svar på hur farlig attacken är eller att attacken är medel farlig. Vidare valdes 4 (hög sannolikhet) i genomsnitt som svar på hur troligt en sådan attack kan inträffa mot ett system. En kommentar var att en individ med information som inte är särskild viktig kan välja ett enkelt förutsägbart lösenord, men ett företag inte bör göra det. **Figur 4.9** sammanfattar resultaten som insamlingen visar för allmänhet, IT-intresserade och experter.



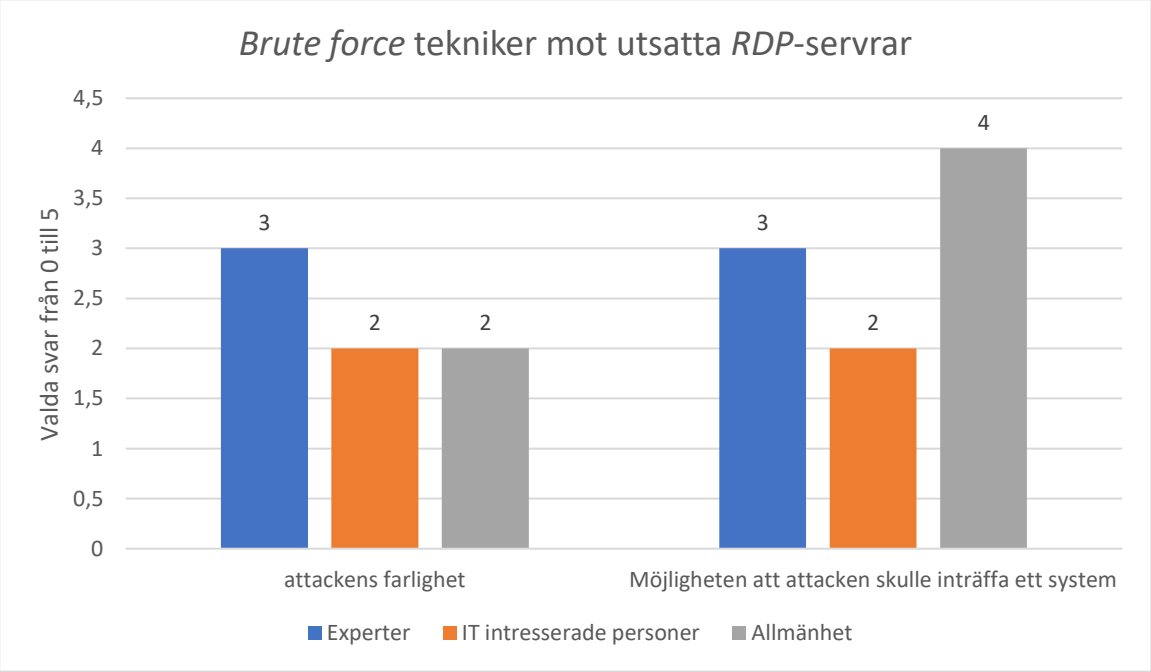
Figur 4.9 visar insamlingens resultat om lösenordssprayning.

4.2.4.4 *Brute force tekniker mot RDP-servrar*

I kommentarer menar experterna att denna attacks allvarlighetsgrad beror på respektive system och hur lätt det är att eskalera åtkomsträttigheter som tidigare nämnts i resultatet för lösenordssprayning. Denna attack fick 3 som svar både på hur allvarlig den är och risken att attacken kan drabba ett företag, med andra ord ansåg experter denna attack som medel farlig och har medelhög sannolikhet att inträffa ett företag.

Även denna attacktyp var känd bland IT-intresserade personer då mer än 80 procent kände igen den sedan tidigare. Både på hur allvarlig den anses vara och hur troligt den kan inträffa var svaret 2 i genomsnitt, med andra ord ansåg IT-intresserade attacken med måttligt farligt och måttlig sannolikhet att inträffa ett system.

Däremot var det bara 17 procent av allmänheten som hade kännedom om *Brute force* tekniker mot *RDP*-servrar. Där valdes 2 i genomsnitt som ett svar på frågan om hur farlig attacken är (måttlig) och 4 på hur sannolikt denna typ av attack kan inträffa ett system (hög sannolikhet). **Figur 4.10** nedan visar resultaten uppdelat på allmänhet, IT-intresserade personer och experter.



Figur 4.10 visar en sammanfattning för insamlingens resultat om Brute force tekniker mot RDP-servrar attack.

4.3 Sammanfattning av uppfattningarna

I Tabell 4.1 presenterar det avrundade medelvärdet av svaren från deltagare i respektive grupp. presenteras en sammanställning av de tre gruppernas uppfattning

i respektive fråga. Värdet som presenteras är ett avrundat medelvärde av svaren från deltagare i respektive grupp.

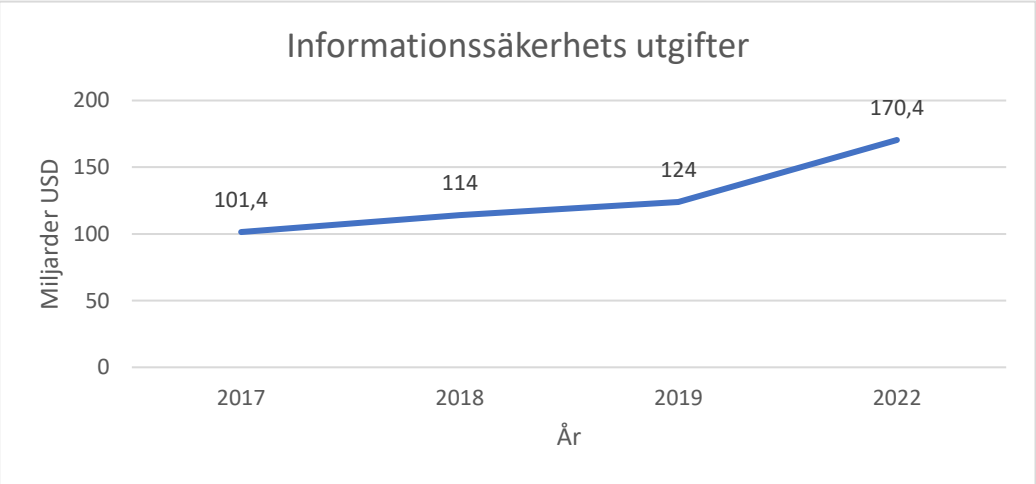
Tabell 4.1 presenterar det avrundade medelvärdet av svaren från deltagare i respektive grupp.

		Experter	IT-intresserade Personer	Allmänhet
Del 1	Personliga risker	3 - medel	3 - medel	2 - måttlig
	Personliga kostnader	1 - liten	2 - måttlig	2 - måttlig
Del 2	Ett företags risker	5 - mycket hög	5 - mycket hög	5 - mycket hög
	Ett företags kostnader	5 - mycket hög	4 - hög	2 - måttlig
Del 3	Cyberattackers huvudsakliga orsaker	Ekonomiska	Ekonomiska	Politiska
Del 4	Nätfiskeattackers allvarlighet	4 - hög	5 - mycket hög	3 - medel
	Nätfiskeattackers sannolikhet att inträffa	5 - mycket hög	4 - hög	5 - mycket hög
	Social ingenjörskonsts allvarlighet	5 - mycket hög	4 - hög	3 - medel
	Social ingenjörskonsts sannolikhet att inträffa	5 - mycket hög	3 - medel	4 - hög
	Lösenordssprayningss allvarlighet	2 - måttlig	2 - måttlig	3 - medel
	Lösenordssprayningss sannolikhet att inträffa	3 - medel	3 - medel	4 - hög
	Brute force teknikers allvarlighet	3 - medel	2 - måttlig	2 - måttlig
	Brute force teknikers sannolikhet att inträffa	3 - medel	2 - måttlig	4 - hög

4.4 Cyberattacker ur ett ekonomiskt perspektiv

En studie av Steve Morgan [9], visar att år 2015 uppsteg de ekonomiska effekter orsakade av cyberattacker till 3 biljoner dollar. De ekonomiska effekterna inkluderar uteblivna intäkter, kostnader för att stävja attacken, lösensummor, med mera. Vidare förutspås att kostnaderna för cyberbrott kommer att kosta världen 6 biljoner dollar år 2021. Denna kostnad är större än kostnaden på grund av alla naturkatastrofer skador under ett år. Eller med andra ord, om cyberbrotts skador skulle simuleras som ett land, skulle det vara världens tredje största ekonomi efter USA och Kina. Förluster för annonsörer, orsakade av bedrägeri uppskattas till 19 miljarder dollar år 2018. Forskarna uppskattar att denna siffra kommer att stiga till 44 miljarder dollar år 2022.

Figur 4.11 visar utgifter relaterade till informationssäkerhets år 2017 och 2018 samt prognos för 2019 och 2022 visar utgifter relaterade till informationssäkerhet, vilket är en del av cybersäkerhet. År 2018 uppgick kostnaderna till 114 miljarder dollar, en ökning med 12,4 procent från år 2017 (101,4 miljarder dollar). Vidare bedöms marknaden växa till 170,4 miljarder dollar år 2022, enligt prognosen från *Cybersecurity Ventures* [9]. Vidare ökad den totala finansieringen för riskkapital inom cybersäkerhetsområdet från nästan 4,5 miljarder dollar år 2017, till mer än 5 miljarder dollar år 2018, en ökning med 20 procent, Steve Morgan [9].

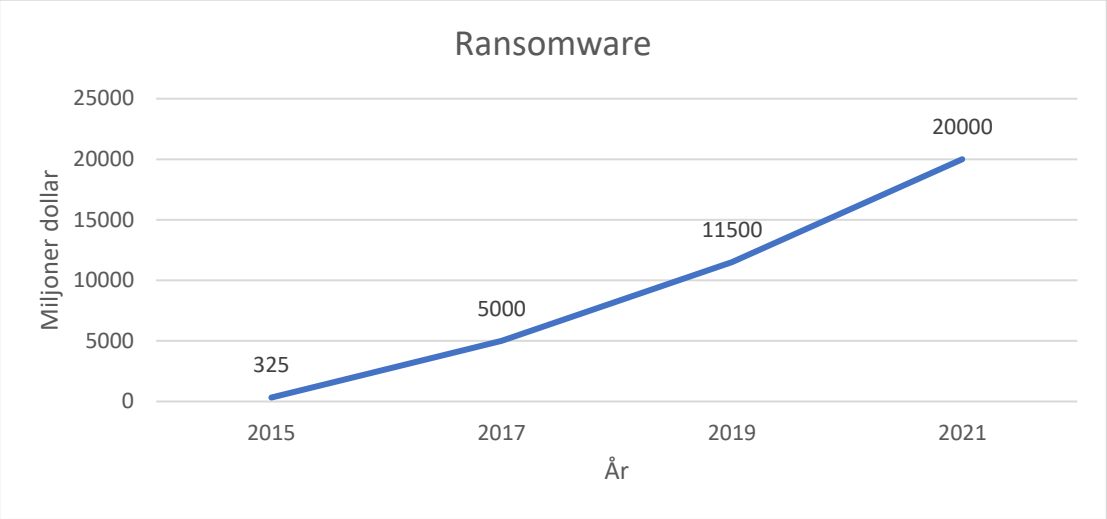


Figur 4.11 visar utgifter relaterade till informationssäkerhets år 2017 och 2018 samt prognos för 2019 och 2022. [9]

År 2016 uppgick kostnaden för cyberförsäkringar till knappt 1,5 miljarder dollar. Marknadsprognoser, enligt *Cybersecurity Ventures* [9], sträcker sig från 14 miljarder dollar år 2022 till 20 miljarder dollar år 2025. En ökning med 18,5 miljarder dollar till år 2025 från år 2016.

Figur 4.12 visar kostnader för *ransomware* under senaste åren. Kostnaden år 2015 var 325 miljoner dollar, ökade till 5 miljarder dollar år 2017 och år 2019 uppgick

kostanden till 11,5 miljarder dollar. Experter uppskattade 2019 att *ransomware* kommer att nå 20 miljarder dollar år 2021, enligt *Cybersecurity Ventures* [9]. Även antale *ransomware* attacker ökar. Från en attack var 40:e sekund år 2016 till var



Figur 4.12 visar skadekostnader för *ransomware* senaste åren.

11:e sekund år 2021.

Studierna visade att företag i Asien och Stillahavsområdet, utsätts för sex cyberattacker varje minut, enligt Cisco [28]. Studien år 2018 visar också att de ekonomiska förlusterna i Asien och Stillahavsområdet kan nå 1 745 biljoner dollar år 2021 på grund av cyberattacker.

Kostnader för att utbilda anställda i cyber- och informationssäkerhet, förutspås uppgå till 10 miljarder dollar år 2027 globalt, jämfört med cirka 1 miljard dollar år 2014, enligt John P. & Mello, Jr [24].

Cyberattackers konsekvenser stod i fokus i en studie genomförd av Steve Morgan [9], chefredaktör på *Cybercrime Magazine*. Författaren fann att cyberbrott räknas som en låg brottslighet, eftersom attackerna inte rapporteras. Orsaken till detta är bland annat på grund av förlägenhet, tron att en brottsutredning inte kommer att leda någonstans eller rädsla för att tappa kundernas förtroende. Enhetschefen vid *FBI:s Internet Crime Complaint Center (IC3)* anser att antalet rapporterade cyberbrott representerar endast 10-12 procent av det faktiska antalet som begås i USA varje år.

Forskare har enhälligt visat att cyber-kriminalitet är en stor utmaning under de kommande två decennierna. Cyberattacker är den snabbast växande brottsligheten i världen och de ökar i storlek, blir allt mer sofistikerade och kostnaderna för dem ökar menar Steve Morgan [9].

4.5 Coop; ett exempel på hur cyberattacker kan påverka verksamheter

På kvällen den 2:a juni 2021 tvingades en svensk butikskedja, Coop, att fysiskt stänga de flesta butiker i Sverige, då kassasystemet inte fungerade på grund av en cyberattack. Experter har enhälligt visat att Coops kassahaveri är kopplat till det amerikanska mjukvaruföretaget *Kaseya*, som är en av Coops leverantörer rörande kassasystemet, enligt SVT Nyheter [27].

Kaseya drabbades av en ransomware-attack av hackergruppen R Evil som begärde en lösensumma på 70 miljoner dollar för att låsa upp *Kaseyas* system, enligt SVT Nyheter [27]. Ungefär samtidigt som *Kaseya* attackerades, slutade Coops kassasystem att fungera.

SVT har intervjuat Mikael Westerlund [27], som är teknisk chef hos dataleverantören Globalconnect. Mikael menar det var många verksamheter i världen som drabbades av den här attacken, i varierade grad, då *Kaseya* är ett internationellt mjukvaruföretag. Coop drabbades dock hårdare än andra. Mikael menar att orsaken till attacken var ekonomisk vinning då angriparna begär en lösensumma. Dessvärre blir det inte bara en ekonomisk förlust i form av förlorade intäkter för företaget utan det skadar även företagets varumärke.

IT-säkerhetsexpert David Jacoby, som SVT intervjuade i samband med attacken [27], anser att ”attacken är unik i sitt slag”. Han menar att om en leverantör drabbas av en attack så kommer även leverantörens kunder att drabbas. Han menar vidare att outsourcing av IT-tjänster kan skapa sårbarheter i system och därmed öka risken för lyckade cyberattacker.

Therese Knapp, presstalesperson för Coop, säger i en intervju med SVT [29] att det var första gången detta hände; att alla deras butiker i Sverige behövde stänga tills de hittat en lösning på problemet. Hon menar att de på Coop beklagar att kunderna inte kunde handla i Coops butiker under denna tid de jobbade med problemet.

Magnus Johansson, VD och koncernchef för Coop Sverige, berättar i en intervju med SVT [30] att Coop tappade enorma ekonomiska värden och att de jobbade intensivt med att få kassasystemet att fungera igen utan att tänka på de ekonomiska förlusterna. Vidare i SVT:s intervju berättar Mattias Wallen, Cyberchef *SRS security*, att beräkningar uppskattar att Coop tappade omkring 100 miljoner i omsättning för varje dag de hade stängt. Ytterligare kostnader kommer förmodligen uppstå till följd av bland annat kostnader för återställning av IT-systemet, leverantörskontrakt som inte följdes och varor som kunde säljas färska. Dessutom riskerar Coop att tappa kunder även efter incidenten.

5 Analys och diskussion

I detta kapitel analyseras och utvärderas examensarbetets resultat i relation till målsättningen och den modell och de lösningsmetoder som använts. Genom att använda konstant jämförande metoden kan man observera att många aspekter av den insamlade uppfattningar visar betydande överlappning. Medan klassificeringen av gemensamma uppfattningar belyser grunden för den gängse uppfattning för olika människogrupper.

I synnerhet var det ekonomiska perspektivet tydligt närvarande i insamlade data. Användningen av konstant jämförande metoden visar att ekonomiska vinster är sammankopplade med cyberbrottslighet.

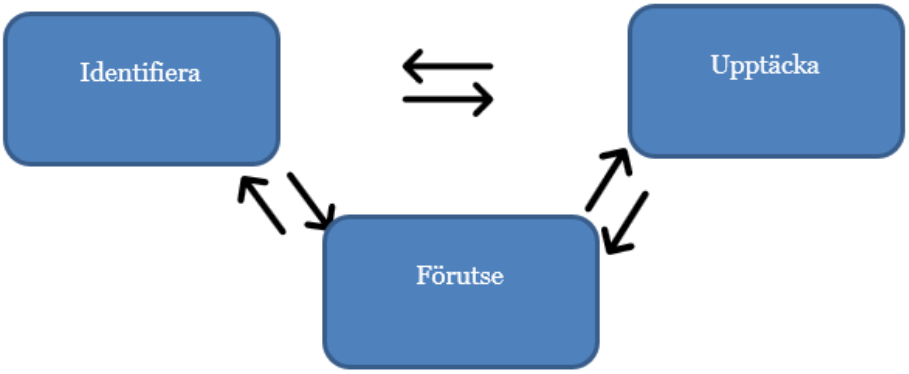
Med hjälp av denna studie kan vi betona några lärdomar som kan bidra till att förstå hur personer ser på cybersäkerhet i stort och cyberattacker i synnerhet. Eftersom cybersäkerhet utvecklas hela tiden, är det inte lätt att alltid vara uppdaterad till nya lösningar och farhågor inom cybervärlden. Samtidigt är det av största vikt viktigt att cybersäkerhet beaktas och att kunskap finns om hur man ska agera i olika situationer. Detta gäller för såväl företag som privatpersoner. Denna uppsats kan även fungera som en guide för de olika uppfattningarna om cyberattacker eftersom den ger en översikt över de idag mest relevanta cyberattackerna. Slutligen kan detta arbete användas som grund för att komplettera befintlig forskning om uppfattningar om olika cybersäkerhetsområden.

Eftersom cybersäkerhet är ett område som kräver en del kunskap samt expertis som ofta finns vid akademiska institutioner, skulle det vara fördelaktigt att veta hur andra ser på cybersäkerhet och göra fler cybersäkerhetsstudier. Fler studier skulle gynna alla områden av cybersäkerhetsforskning och särskilt statlig cybersäkerhet då offren oftast är personer som inte är kunniga inom cybersäkerhet.

5.1 Diskussion av litteraturstudien

Resultaten från *Orange Cyberdefense* visar att det är väsentligt att undersöka och studera varje applikation i sig för att definiera riskerna som kan inträffa den specifika applikationen. Detta påminner om prognoser för väder och klimat. Genom att identifiera och spåra de systemelement som kan skapa oväder i applikationen, och därmed orsaka cyberhotsklimatet, skapas förstående för de specifika hot som kan beröra det studerade systemet. Därefter kan arbete påbörjas för att förbereda och arbeta för att avvärja dessa hot.

För att diskutera vidare den metod som *Orange Cyberdefense* använder, ges i *Figur 5.1* en schematisk bild över hur de arbetar med cybersäkerhet för att skydda olika system. De anser att man först måste förstå systemet för att sedan kunna identifiera eventuella brister och de hot som kan inträffa. Därefter kan systemets utsatthet bedömas och lämpliga motåtgärder vidtas. Med andra ord att tänka som angriparen för att kunna sätta in rätt motåtgärd.



Figur 5.1 Orange Cyberdefense metod

Utifrån denna metod ses hur viktigt det är att ha en realtidsuppfattning om det föränderliga attacker, det vill säga att vara uppdaterad med den senaste forskningen inom IT-säkerhet. Detta då även angriparna kommer att utveckla sina metoder och tillvägagångssätt i takt med utvecklingen av ny teknik och komplexa system. Vidare ses vikten av att förstå det egna systemet och dess sårbarheter.

5.2 Diskussion och analys av enkätundersökningen

Generellt sett möter undersökningar människors ovilja, särskilt när det inte finns någon personlig vinning för deltagarna. Deltagandegraden var lägre än den förväntade med tanke på delningar på sociala medier. Detta kan bero på att tiden i nuläget under SARS-CoV-2-pandemin blir mer värdefull och pressen mer påtaglig i det dagliga livet. Därför måste förväntningarna justeras efter dagens situation. En djupare studie med ett större urval skulle öka tillförlitlighet av resultaten.

Med respekten för både anonymitet och integritet för deltagarna undveks frågor relaterade till nationalitet, kön eller ålder, trots att de skulle kunna främja ganska intressanta resultat. Vidare undveks fritextsvar i ett försök att hålla frågeformuläret kort och rakt på sak.

Individers uppfattningar om cyberattacker baseras på tidigare upplevda attacker och kunskaper om olika typer av tillvägagångssätt. Därför visar resultaten, i många fall, olika svar oavsett hur bra kännedom deltagarna har för olika områden i både cyberattacker och ekonomiska konsekvenser.

En kommentar från en person som arbetar med cybersäkerhet, men själv inte betraktar sig själv som expert, belyser att det kan finnas fler personer i undersökningen som valt att inte betrakta sig som en expert trots att de arbetar inom

IT-säkerhet. Det på samma sätt kan finnas personer som själva anser sig vara experter på cybersäkerhet men som i själva verket inte är det.

5.2.1 Uppfattningar om personliga risker

Resultatet visar att uppfattningen om de personliga riskerna var relativt samstämmiga mellan de tre olika grupperna och att samtliga värderar de personliga riskerna som medelstora. Dock värderar allmänheten risken som något lägre. Både experter och IT-intresserade graderade risken att själv drabbas av en cyberattack till 3 medan allmänheten graderade risken till 2.

Kommentarer på denna fråga indikerar på att medvetenheten ökar med ökad internetanvändning. Vidare finns kommentarer om att personer själva drabbats av attacker och att detta gjort att personen blivit bättre på att skydda sin data.

Även uppfattningen om de ekonomiska konsekvenser som kan uppstå efter en cyberattack mot en individ, var relativt samstämmiga. Experterna svarade 1 medan allmänheten och IT-intresserade personer svarade med 2. Skillnaden kan bero på att experterna tycks i större utsträckning lita på att banker, och andra verksamheter som sköter ekonomi, är bra skyddade från cyberattacker. Fler kommentarer pekade på och bekräftade tilltron till att viktig information skyddas.

5.2.2 Uppfattningar om företagsrisker

Resultatet från litteraturstudien visar att 68 procent av amerikanska företag inte har någon form av cyberförsäkring. Detta kan tolkas som att företag inte förstår riskerna som de står inför och hur alvarliga de kan vara. En annan anledning kan vara att tillgängliga cyberförsäkringar inte matchar företagens behov. Resultatet visar även att trots lagstiftning inom Europeiska unionen, finns det stora risker för att företag inom unionen ska drabbas av en cyberattack.

Däremot visar resultatet från insamlingen att alla tre grupper förstår att företagen löper väldigt stor risk att bli attackerade då alla grupper gav högsta möjliga gradering. Detta syns även i kommentarer till denna fråga där personer påpekar att företag kan drabbas av cyberattacker hela tiden och om företaget inte skyddar sig tillräckligt bra, kan allvarliga konsekvenser följa.

En viktig del av konsekvenserna som kan drabba ett företag är de ekonomiska effekterna. Både experter och IT-intresserade personer uppger att allvarliga ekonomiska konsekvenser kan ske ifall ett företag drabbas av en cyberattack. Experter graderade ekonomiska effekter till 5 och IT-intresserade till 4. Däremot märks en större skillnad när det kommer till allmänhetens uppfattning då de graderade det till 3. Det kan konstateras att allmänheten inte har liknande uppfattning som experter. Detta kan antingen bero på att de inte kan göra den typer av uppskattning eller att de har ett stort förtroende för företagens skydd mot cyberattacker.

5.2.3 Uppfattningar om huvudsakliga orsaker

Både experter och IT-intresserade personer bedömer att ekonomiska orsaker är den huvudsakligorsaken bakom cyberattacker. Dock visar kommentarerna från experter att orsaker kan variera beroende på situationen. Det ska jämföras med *Orange Cyberdefense* som anger sociokulturella och tekniska orsaker som huvudsakliga orsaker bakom cyberattacker.

Däremot anser allmänheten den politiska orsaken vara huvudsaklig bakom cyberattacker. Denna skillnad kan bero på att allmänheten inte har förståelse för alla cyberattacker som kan inträffa och de vinster och effekter angriparen kan uppnå.

5.2.4 Uppfattningar om olika cyberattacker

Nätfiske

Det finns en hög kännedom för denna attack bland IT-intresserade personer då mer än 90 procent av dem känner till attacken. Detta bekräftar att det är ett vanligt tillvägagångssätt för en attack. Däremot hade bara 23 procent av allmänheten kännedom om nätfiske. Eftersom allmänheten inte är insatta i IT- eller säkerhetsfrågor är det en rimlig siffra.

På frågan om allvarlighetsgrad och sannolikhet för att ett företag ska drabbas var svaren relativt samstämmiga mellan de tre grupperna, med undantag att allmänheten bedömde sannolikheten för en attack som lägre än övriga två.

Till följd av denna kännedom hade både IT-intresserade och allmänhet ett genomsnittligt svar som var nära experternas svar med en liten skillnad på svaret om attackens farlighet. Vidare hade allmänhet och experter samma svar för hur troligt det är att ett system kan drabbas av denna attack. Men IT-intresserade hade en liten skillnad på detta svar då de ansåg att attacken är ganska vanlig med betyget 4 och inte 5 som experter ansåg.

Social ingenjörskonst

Resultatet från litteraturstudier visar att en stor del av rapporterade attacker är kopplade till social ingenjörskonst. Den bilden bekräftas av expertgruppens enkätsvar. Med detta kan man förstå hur viktigt det är att utbilda användare i hur de ska upptäcka och reagera på dessa hot eftersom de kan vara ett avgörande steg i en ransomware attack. Trots detta hade bara 40 procent av IT-intresserade personer samt så lite som 13,9 procent av allmänhet kännedom om denna attacktyp.

Vidare visar resultatet att allmänheten inte uppfattar attacken som lika allvarlig då det var en skillnad mellan experters svar och genomsnittliga svaret från allmänhet med två enheter. IT-intresserade bedömer attacktypen som allvarlig, dock inte i lika hög grad som experterna.

Experterna uppskattar att sannolikheten för en sådan attack är mycket hög. Även allmänheten anger en hög sannolikhet då de graderar den till 4 medan IT-intresserade graderar den till 3.

Lösenordssprayning

Då många i enkätundersökningen kände till lösenordssprayning sedan tidigare, kan det tyda på att tillvägagångssättet är vanligt. Denna attack kan drabba internetanvändare när som helst.

Från enkätsvaren märks att många bland deltagarna har en liknande uppfattning som experter i hur de uppfattar denna attack. Detta bekräftas också av att många system numera kräver två faktors autentisering för att säkra användarnas konton. I enkätsvaren syns att alla tre grupper har en relativt samstämmig uppfattning om allvarlighet och sannolikhet för lösenordssprayning.

***Brute force* tekniker mot *RDP*-servrar**

Denna attacktyp var känd bland IT-intresserade personer där mer än 80 procent av dem kände till det sedan tidigare. Motsvarande siffra för allmänheten var 17 procent. Det belyser att allmänhet inte har en god kännedom om denna attacktyp.

Att gissa lösenordet kan vara nästan omöjlig om man använder olika typer av tecken (det vill säga bokstäver, siffror, specialtecken med mera) och har begränsad antal försök. Men ibland utgår denna gissning från information som angriparen har om kontohavare. Resultaten visar att IT-intresserade och allmänheten hade samma uppfattning gällande attackens allvarlighet och att den var lägre än experternas.

IT-intresserade uppskattade sannolikheten att attacken kan inträffa som lägre jämfört med experterna. Vidare angav allmänhet en högre sannolikhet än experters.

5.3 Cybersäkerhet utifrån de ekonomiska och sociala perspektiven

Resultatet visar att cybersäkerhet är ett globalt problem och att dess relaterade skador kostar världen enorma summor pengar. Resultatet visar även att kostnaderna ökat kraftigt under åren och att problemet därmed fortsätter att växa. Det är därför viktigt att tänka på lösningar för att undvika de olika cyberattackerna.

Cyberattacker medför inte bara enorma ekonomiska kostnader för samhället i stort utan även sociala bekymmer. Resultatet visar att en del attackerade företagen inte anmäler om de blir attackerade. Detta kan bero på flera orsaker, bland annat att företaget inte kan hitta några tekniska lösningar som löser problemet eller att de inte har förtroende för att rättsväsendet kan rädda företagets data utan att tillmötesgå angriparens krav. Därför är det mycket viktigt att ha säkra system och att anställa IT-personal med kunskap inom IT-säkerhet.

Fallet med Coop visar hur attackerna sker i verkligheten och vilka stora och allvarliga konsekvenserna, både ekonomiska och sociala, som kan följa efter en cyberattack. De sociala konsekvenserna för Coop var bland annat att kunder inte kunde köpa varor i fler dagar och det kan vara möjligt att några kunder inte längre har förtroende för dem. De ekonomiska konsekvenserna var tydliga för Coop då det förlorade stora summor i omsättning varje dag de hade stängt samt lägre antal kunder till följd av tappat förtroende. Det kan även innebära framtida ekonomiska förluster.

5.4 Cybersäkerhet utifrån en etik och miljömässig synvinkel

Bakgrunden och resultatet visar att cyberattacker kan påverka alla typer av verksamheter. Påverkan begränsas inte på systemets- och nätverk säkerhet men även på miljön. Lyckade cyberattacker mot landets infrastruktur, såsom system som kontrollerar processerna inom energi, transport, vattenhantering och andra industrier, kan skapa stora störningar, psykologiska effekter och även stora konsekvenser på vår miljö. Exempelvis kan cyberattacker mot tekniska system för oljeplattformar eller raffinaderier, skapa ett katastrofalt scenario för människor och miljö.

Det är viktigt att utbilda fler personer inom IT-säkerhet och offensiv cybersäkerhet. Om denna kunskap däremot faller i fel händer, finns risk att man i stället utbildar framtida angripare vilket kan leda till allvarliga skador för organisationer och på samhället. Vapnet i det här fallet är kunskap, vilket är mer svårhanterat än ett traditionellt skjutvapen. Därför är det viktigt att tänka på etiska aspekter och risker vid utbildning. Detta kan uppnås genom att inkludera etiska principer i cybersäkerhetsutbildningar, för att ge etisk kunskap om hur och när dessa kunskaper ska användas.

6 Slutsatser och framtida studier

Säkerhetskultur odlas genom en lång och tidskrävande process som påverkas av olika faktorer med olika tyngd. Dess grundvalar ligger på den säkerhetsmedvetenhet och beredskap som uppvisas under alla omständigheter och som förvandlas och anpassas över tid och förändringar.

Resultatet visar att upplevd uppfattning om hur farliga de olika cyberattackerna är för individen skiljer sig, oavsett om individen är en expert, IT-intresserad eller en person som inte är intresserad av IT och säkerhet. Dessutom varierar även den ekonomiska uppfattningen för cyberattacker. Dessa variationer bland deltagarnas uppfattningar visar att informationssäkerhet, även om den gradvis utvecklas, har en lång väg tills den blir en obruten del av affärsverksamheten och arbetskraftens verklighet.

Eftersom en persons uppfattningar kan bero på upplevda hot om cyberattacker, kan framtida studier på allmänhetens uppfattning analyseras genom att först mäta upplevd svårighetsgrad och sårbarhet om cyberattacker och sedan relatera dem tydligt till individens uppfattning.

Framtida forskning kan använda en liknande process för att undersöka andra aspekter av cybersäkerhet och hur olika personer uppfattar dessa aspekter. En forskargrupp kan exempelvis intervjua personer för att säkerställa förståelsen för olika aspekter och sedan ställa frågor. Då kan man samla mer information och ställa följdfrågor om personernas uppfattningar för att säkerställa att forskaren själv har uppfattat personens tankar på ett rätt sätt. Forskning på en definierad population kan även göras där populationen har flera olika upplevelser och även fler personliga frågor kan ställas om bland annat kön, ålder och nationalitet. Vidare kan undersökningen använda sig av fler metoder för att analysera data i syfte för att dra nytta av resultaten från varje metod och därmed bättre förstå deltagarnas uppfattningar med sina upplevelser.

Informationssäkerhet och motsvarande kultur måste utvecklas och anpassas för att erbjuda de lösningar som behövs till den nya verkligheten. Genom att odla och uppmuntra medarbetarnas medvetenhet i säkerhetsfrågor, genom kontinuerliga utbildningsprogram och aktivt deltagande i moderna säkerhetssimuleringar kan företag minska risker och effekter av cyberattacker. Cyberbrottslighet utvecklas genom att utnyttja varje möjlighet som uppstår, och det borde också företagens cybersäkerhetskultur göra. Fallet med Coop, visar på hur viktigt det är att vidareutbilda IT-personal och säkerställa bra informationssäkerhet internt i företaget, i stället för att ha olika leverantörer som sköter delar av systemet. Med detta kan företagen undvika att hamna i en situation där de blir sekundära offren och få känslig information exponerad eller vara beroende av det primära offret för produkter eller tjänster.

Källförteckning

[1] G. Coulouris, J. Dollimore, T. Kindberg och G. Blair, ”DISTRIBUTED SYSTEMS Concepts and Design”, Fifth Edition, 2012, s. 75, 381–419, 466–469.

[2] Orange Cyberdefense, ”Beating ransomware: A comprehensive guide to tackling the cyber extortion threat” (2021) https://orangecyberdefense.com/global/white-papers/beating-ransomware/. Hämtad 2021-11-15.

[3] Varonis, ”What is Mimikatz: The Beginner’s Guide”, (2020), https://www.varonis.com/blog/what-is-mimikatz/. Hämtad 2021-11-18.

[4] MITRE ATT&CK, ”LaZagne”, (2021), https://attack.mitre.org/software/S0349/. Hämtad 2021-11-18.

[5] McAfee, ”What is a Remote Administration Tool (RAT)?”, (2015) https://www.mcafee.com/blogs/privacy-identity-protection/what-is-rat/. Hämtad 2021-11-18.

[6]Tweneboah-Koduah S, Atsu F, Prasad R. ”Reaction of stock volatility to data breach: an event study”. Journal of Cyber Security and Mobility, (2020), https://journals.riverpublishers.com/index.php/JCSANDM/article/view/1169.

[7] Pranshu Bajpai, Richard Enbody, ” Cryptojacking Spreads across the Web”, (2018), https://www.scientificamerican.com/article/cryptojacking-spreads-across-the-web/. Hämtad 2021-11-25.

[8] Pranshu Bajpai och Richard Enbody, ” Cryptojacking Spreads across the Web”, (2018), https://www.scientificamerican.com/article/cryptojacking-spreads-across-the-web/. Hämtad 2021-11-25.

[9] Steve Morgan, ”2019/2020 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics”, Cybercrime Magazine, (2019), https://cybersecurityventures.com/cybersecurity-almanac-2019/. Hämtad 2021-11-24.

[10] OWASP, ”Top 10 Web Application Security Risks”, (2021), https://owasp.org/www-project-top-ten/. Hämtad 2021-11-22.

[11] TrustNet, ” Common Web Application Attacks”, (2021), https://www.trustnetinc.com/web-application-attacks/. Hämtad 2021-11-23.

[12] Kamalanathan Kandasamy, Sethuraman Srinivas, Krishnashree Achuthan och Venkat P. Rangan, ” IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process”, (2020), https://link.springer.com/content/pdf/10.1186/s13635-020-00111-0.pdf. Hämtad 2022-01-14.

[13] Abhinav Juneja,Sapna Juneja,Vikram Bali,Vishal Jain,Hemant Upadhyay, ”Artificial Intelligence and Cybersecurity: Current Trends and Future Prospects”, (2021), https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119761655.ch22. Hämtad 2022-01-14.

[14] Anand Handa,Ashu Sharma,Sandeep K. Shukla, ” Machine learning in cybersecurity: A review”, (2019), https://wires.onlinelibrary.wiley.com/doi/abs/10.1002/widm.1306. Hämtad 2022-01-14.

[15] Fredrik Heiding, Robert Lagerström, ” Ethical Principles for Designing Responsible Offensive Cyber Security Training”, (2021), https://link.springer.com/chapter/10.1007%2F978-3-030-72465-8_2. Hämtad 2022-01-14.

[16] Angelo Furfaro, Luciano Argento, Andrea Parise, Antonio Piccolo, ” Using virtual environments for the assessment of cybersecurity issues in IoT scenarios”, (2017), https://www.sciencedirect.com/science/article/pii/S1569190X16302374?casa_token=zXcYkIY1E78AAAAA:lJbEwVFkyuMQ_CLJceEOSTvuSKsEd_Rn5fvffw4ffYsnPM1QDvIkIWTMGLWdbwPila3b2w9JaA. Hämtad 2022-01-14.

[17] Heiding F., Omer M., Wallström A. , Lagerström R., ” Securing IoT devices using geographic and continuous login blocking: A honeypot study”, (2020), https://www.scopus.com/record/display.uri?eid=2-s2.0-85083023600&origin=resultslist&sort=cp-f&src=s&st1=Securing+IoT+Devices+using+Geographic+and+Continuous+Login+Blocking%3a+A+Honeypot+Study&st2=&sid=ba335111ed0b4bcf4cef536048e34673&sot=b&sdt=b&sl=100&s=TITLE-ABS-KEY%28Securing+IoT+Devices+using+Geographic+and+Continuous+Login+Blocking%3a+A+Honeypot+Study%29&relpos=0&citeCnt=0&searchTerm=. Hämtad 2022-01-14.

[18] Georgiadou, Anna, Spiros Mouzakitis, och Dimitris Askounis,” Designing a cyber-security culture assessment survey targeting critical infrastructures during covid-19 crisis”, (2020). International Journal of Network Security & Its Applications (IJNSA) 13 (1): 33–50. https://doi.org/10.5121/ijnsa.2021.13103.

[19] Schuman, H. (2008). Method and Meaning in Polls and Surveys. Harvard University Press

[20] Nora Cate Schaeffer, Jennifer Dykema,” Questions for Surveys: Current Trends and Future Directions”, (2011), https://academic.oup.com/poq/article/75/5/909/1824254?login=true. Hämtad 2022-01-21.

[21] SAGE ResearchMethods, ”Constant Comparison In: The SAGE Encyclopedia of Social Science Research Methods” (2004) https://methods.sagepub.com/reference/the-sage-encyclopedia-of-social-science-research-methods/n161.xml. Hämtad 2021-11-01.

[22] Glaser, B., & Strauss, A.(1967). The discovery of grounded theory. Chicago: Aldine.

[23] Silverman, D.(1993). Interpreting qualitative data: Methods for analysing talk, text, and interaction. London: Sage.

[24] John P. & Mello, Jr. ” Security Awareness Training Explosion”, (2017), https://cybersecurityventures.com/security-awareness-training-report/. Hämtad 2021-11-25.

[25] Scott Calvert och Jon Kamp, ”More U.S. Cities Brace for ‘Inevitable’ Hackers”, The Wall Street Journal, (2018), https://www.wsj.com/articles/more-cities-brace-for-inevitable-cyberattack-1536053401. Hämtad 2021-11-29.

[26] EUR-Lex, ”The general data protection regulation applies in all Member States from 25 May 2018”, (2018), https://eur-lex.europa.eu/content/news/general-data-protection-regulation-GDPR-applies-from-25-May-2018.html. Hämtad 2021-11-29.

[27] Enterprise Risk Magazine,” CYBERSECURITY IS THE SINGLE BIGGEST RISK FOR 2019”, (2019), https://enterpriseriskmag.com/cybersecurity-single-biggest-risk-2019/. Hämtad 2021-11-29.

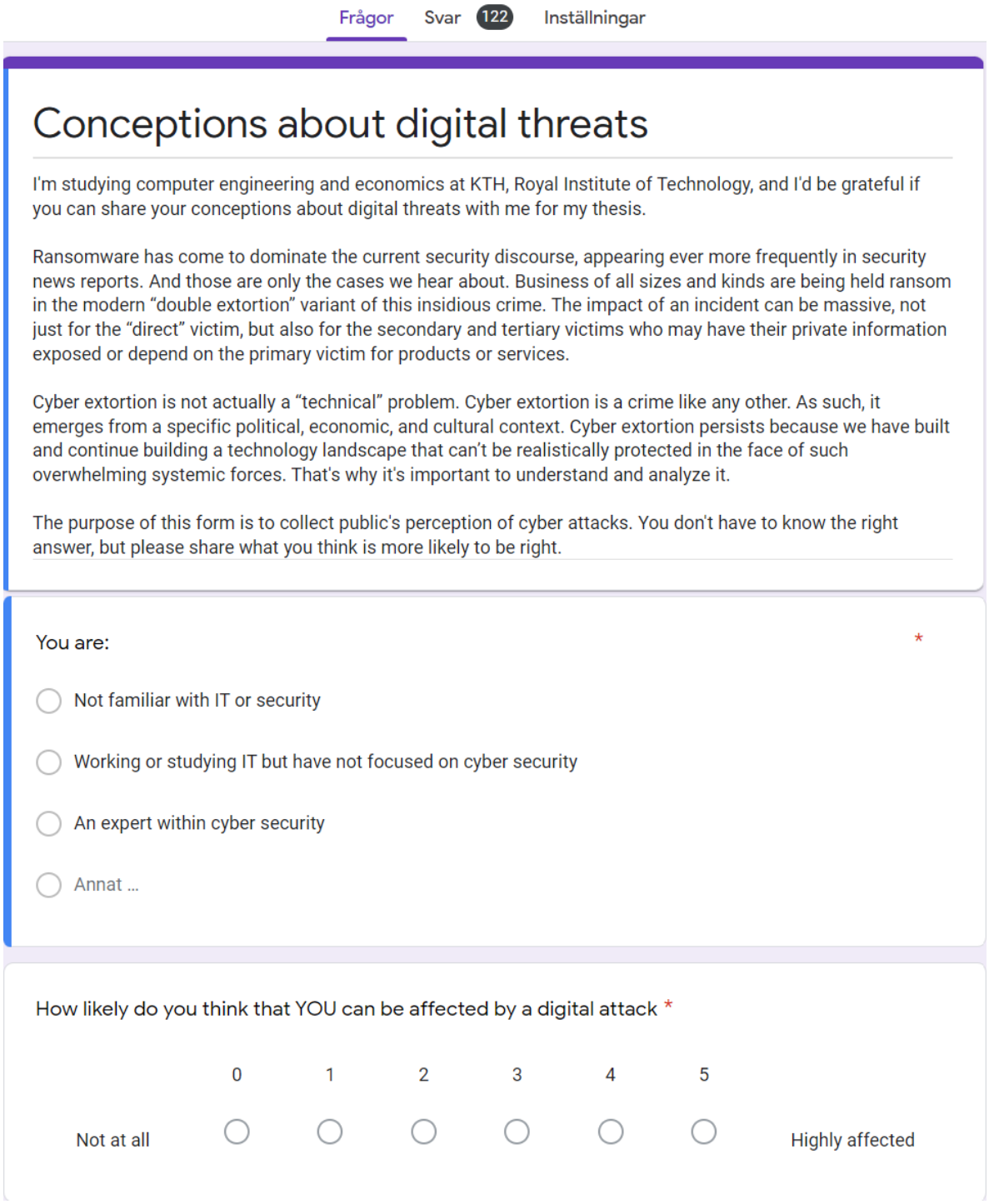
[28] Cisco, ”Cisco 2019 Asia Pacific CISO Benchmark Study Statistic”, (2019), https://www.cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html. Hämtad 2021-11-25.

[29] Dante Thomsen, Eneida Berisha och Gilda Hamidi-Nia, SVT Nyheter, ” Expert om attacken som sänkt Coop: ”Utpressning mot detaljhandeln har exploderat” ”, (2021), https://www.svt.se/nyheter/inrikes/it-attacker-och-utpressningar-mot-detaljhandeln-allt-vanligare. Hämtad 2021-11-30.

[30] Sandra Killgren, SVT Nyheter, " Coops vd: ”Kommer tappa enorma ekonomiska värden” ", (2021), https://www.svt.se/nyheter/inrikes/hundratals-coop-butiker-vantas-oppna. Hämtad 2021-11-30.

Bilagor

Bilaga 1: visar Formuläret som formuläret som har använts för att samla in uppfattningar. Länk till formuläret: https://forms.gle/WYz2BkCQQJ2ANqzZ9. Nedan kan man se bilder på frågorna som fanns i formuläret.



Comments about your answer:

Lång svarstext

How much money do you think an attack can cost you? *

	0	1	2	3	4	5	
Nothing	○	○	○	○	○	○	All you got

Comments about your answer:

Lång svarstext

How likely do you think that a business will be affected by a digital attack. *

	0	1	2	3	4	5	
Not at all	○	○	○	○	○	○	Highly affected

Comments about your answer:

Lång svarstext

How much money do you think an attack can cost the affected business? *

	0	1	2	3	4	5	
Nothing	○	○	○	○	○	○	All they got

Comments about your answer:

Lång svarstext

What do you think the main/real context of the criminal to do cyber attacks? *

- [ ] Political
- [ ] Sociocultural
- [ ] Economic
- [ ] Technological
- [ ] Annat ...

Phishing is an attack which has the purpose of getting the user to disclose personal information, such as passwords or credit card numbers. *

- ○ I am not familiar with this attack
- ○ I am familiar with this attack

How harmful do you think Phishing is? *

	0	1	2	3	4	5	
Can be overcome quite easily	○	○	○	○	○	○	Very dangerous

How likely do you think that a business will be affected by a phishing attack. *

	0	1	2	3	4	5	
Not at all	○	○	○	○	○	○	Highly affected

Comments about your answer:

Lång svarstext

Social engineering is an attack which has the propose of manipulate people into committing various acts or revealing secret information, instead of breaking in themselves. *

- I am not familiar with this attack
- I am familiar with this attack

How harmful do you think Social engineering is? *

	0	1	2	3	4	5	
Can be overcome quite easily	○	○	○	○	○	○	Very dangerous

How likely do you think that a business will be affected by a Social engineering attack. *

	0	1	2	3	4	5	
Not at all	○	○	○	○	○	○	Highly affected

Comments about your answer:

Lång svarstext

Password spraying; this attack occurs when the user password is common and then the attack tries to access a large number of accounts with a few common passwords. *

- I am not familiar with this attack
- I am familiar with this attack

How harmful do you think Password spraying is? *

	0	1	2	3	4	5	
Can be overcome quite easily	○	○	○	○	○	○	Very dangerous

How likely do you think that a business will be affected by a Password spraying attack. *

	0	1	2	3	4	5	
Not at all	○	○	○	○	○	○	Highly affected

Comments about your answer:

Lång svarstext

Brute force; the attack tries to gain unauthorized access to an account by guessing the password. *

- ○ I am not familiar with this attack
- ○ I am familiar with this attack

How harmful do you think Brute force is? *

	0	1	2	3	4	5	
Can be overcome quite easily	○	○	○	○	○	○	Very dangerous

How likely do you think that a business will be affected by a Brute force attack. *

	0	1	2	3	4	5	
Not at all	○	○	○	○	○	○	Highly affected

How likely do you think that a business will be affected by a Brute force attack. *

	0	1	2	3	4	5	
Not at all	○	○	○	○	○	○	Highly affected

Comments about your answer:

Lång svarstext

Thanks for your time!

If you have any questions please feel free to send me an email :)
elyasa@kth.se