LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

IT-säkerhetens påverkan på distansarbetets uppskalning

En kvalitativ studie om hur IT-säkerheten har påverkats av distansarbete

Kandidatuppsats 15 hp, kurs SYSK16 i Informationssystem

Författare: Alexander Nilsson Sump
Oliver Ilijason

Handledare: Benjamin Weaver

Rättande lärare: Markus Lahtinen
Magnus Wärja

IT-säkerhetens påverkan på distansarbetets uppskalning:
En kvalitativ studie om hur IT-säkerheten har påverkats av distansarbete

ENGELSK TITEL: The impact of IT security in regards to the upscaling for telework: A qualitative study about the teleworks influence on IT security

FÖRFATTARE: Alexander Nilsson Sump och Oliver Ilijason

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Osama Mansour, PhD

FRAMLAGD: maj, 2022

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 94

NYCKELORD: Distansarbete, Informationssäkerhet, IT-säkerhet, Molntjänst, CIA-triaden, TTAT

SAMMANFATTNING:
Distansarbete är en term som kommit att bli allt vanligare sedan Covid-19 pandemins början, och nu arbetar organisationer med att hitta sin nya identitet gällande tillvägagångssätt för arbete. Detta har lett till nya utmaningar för IT-säkerheten hos samtliga branscher då man nu bör se över sina rutiner, riktlinjer och tekniker för att förse sina anställda med vad de behöver för att arbeta ostört även hemifrån. Andra typer av dataintrång har uppdagats till följd av detta, och företag behöver se till att man sköter sin säkerhet nu mer än någonsin. Molntjänster är ett ämne som möjliggör för distansarbete, samtidigt som det kan väcka oro då organisationer måste förlita sig på sina leverantörer att sköta *Confidentiality, Integrity & Availability* i linje med sig själva. Vi har undersökt dessa områden genom kvalitativt arbete där fyra organisationer blivit intervjuade med kunskap inom IT. Sammanfattningsvis har organisationer generellt klarat av dessa utmaningar bra genom att luta sig mot den existerande medvetenheten inom företagen samtidigt som att en bra grund av *Confidentiality & Integrity* redan existerade. Vidare ser man nya trender som uppdagas då man på ett permanent plan behöver fastställa IT-säkerheten då hybridarbete är här för att stanna.

Förord

Vi vill börja med att tacka samtliga respondenter som tog sin tid att besvara våra frågor och funderingar ur deras perspektiv och erfarenheter, vilket gjorde denna uppsats möjlig. Deras kunskap och inblickar på IT och IT-säkerhet hjälpte oss förstå hur organisationer arbetar och utför sina säkerhetsåtgärder samt hur detta har påverkats till följd av flytten till distansarbete.

Alexander Nilsson Sump & Oliver Ilijason

Innehåll

Figurer

Tabeller

1 Introduktion

1.1 Bakgrund

IT-säkerhet är inget nytt ämne, men sedan introduktionen av hemarbete har möjligheten för dataintrång ökat och cyberattacker ökar frekvent, eventuellt som en påföljd av hemarbete under Covid-19 pandemin (Eklund, 2020). Ett dataintrång är både dyrt och tidskrävande för organisationer då ett svenskt företag i snitt spenderar sju miljoner SEK och 66 dagar för att återhämta sig efter ett dataintrång (IT-Finans, 2017). Truesec, som är ett IT-säkerhetsföretag, kom fram till att under 2020 kostade cyberattacker svenska företag mellan 20-22 miljarder SEK (Eklund, 2020). Samtidigt investerar svenska företag under 8% av sin IT-budget på just IT-säkerhet (IT-Finans, 2017).

Vid hemarbete presenteras en rad problem där åtkomst och tillgänglighet av system och data är något som arbetsgivare på bredare front bör erbjuda. Kopplingen till hemarbete, IT-Säkerhet och åtkomst av system/data möjliggör att fokusera på säkerheten vid datahantering, där en teori om *Confidentiality, Integrity & Availability* faller in (Andress, 2014, s.5-6). Ett alternativ som presenterar lösningar för åtkomst och tillgänglighet är implementeringen av molntjänster inom organisationer för att underlätta den anställde och dennes arbetsuppgifter, men det kan även betyda att det finns ännu en part, molntjänstleverantörer, i ledet som kan bli påverkad av dataintrång (Mandal och Khan, 2020).

Hemarbete har blivit vanligare och till en gräns ett krav för många, därav behöver arbetsgivaren erbjuda detta för att locka till sig så många kandidater som möjligt. Nu är det flera som ställer krav på att möjligheten för distansarbete ska finnas, och vi har nyligen sett chefer på exempelvis Apple sluta då man satt nya riktlinjer att distansarbete är ett minne blott (Titcomb, Millard, Warrington, Wallace, Wallace, Titcomb & Rees, 2022). Genom att kunna erbjuda en hybridlösning för sina anställda bör därför IT-systemen i en organisation vara kompatibla, detta genom användningen av VPN-tjänster och molntjänster som förser anställda att komma åt sina jobbuppgifter lika enkelt hemifrån som på kontoret (Razmerita, Peroznejad, Pantelli & Kärreman, 2021).

1.2 Problemområde

Med anledning att hemarbete blivit allt vanligare finns det bevåg för arbetsgivare att säkerställa IT-säkerhet som håller en lika hög standard oavsett om den anställde befinner sig fysiskt på det faktiska kontoret eller jobbar hemifrån. Arbetsgivaren bör även kunna säkerställa att sina anställda har åtkomst till samtliga system och data de behöver för att utföra sitt jobb på ett effektivt sätt hemifrån.

En problematik som uppdagas är frågeställningen; hur organisationer ska jobba för att sin respektive IT-säkerhet håller tillräckligt hög standard, både ur perspektivet där IT-systemen ska motverka attacker, samt hur medarbetare bör agera varsamt genom att aktivt förstå innebörden.

För att nå en hög standard i en organisations IT-säkerhet kan man ta hjälp av *Confidentiality, Integrity & Availability*, då dessa är en viktig del av informationssäkerhet och hur man från en teoretisk ståndpunkt kan diskutera ämnet (Andress, 2014, s.5-6). Teorin kan även hjälpa organisationer förstå hur de tre aspekterna kan komma att påverka IT-säkerheten av skiftet till hemarbete.

Då det finns en korrelation mellan medvetenhet av potentiella risker inom IT-säkerhet och en motivationen att undvika dessa, möjliggörs en potentiell följd där utveckling av utbildningar och riktlinjer före flytten till hemarbete har en inverkan på IT-säkerhetsperspektivet (Liang & Xue, 2009). Medvetenhet och erfarenhet är också ett ämne som kan presentera en roll av hur hemarbetet upplevs mellan olika individer.

1.3 Forskningsfråga

Flytten till distansarbete som följd av Covid-19 pandemin har presenterat organisationer med nya utmaningar om såväl åtkomst av system och data för den anställde samtidigt som dataintrång och cyberattacker har ökat.
Med detta som grund har vår forskningsfråga formuleras som följande:

Vilka aspekter av IT-säkerheten har påverkats till följd av distansarbetets uppskalning?

1.4 Syfte

Syftet med denna uppsats är att undersöka tankesätt samt trender involverat vid distansarbetets inverkan på IT-säkerhet. Vilka åtgärder som organisationer vidtar för att försäkra att ingen annan än behöriga individer har tillgång till specifik information och system. Vidare är syftet att se över hur medvetenhet och erfarenhet inom IT-säkerhet, distansarbete och datahantering på en organisationell nivå har påverkat hantering av flytten till distansarbete.

1.5 Avgränsningar

Distansarbete och IT-säkerhet öppnar upp för flertalet aspekter, därav kommer denna uppsats fokusera på IT-säkerhet i frågan om potentiella hot mot den givna organisationen i den givna aspekten, till exempel cyberattacker. Vidare kommer vi fokusera på hur medvetenhet och erfarenhet inom IT-säkerhet, distansarbete och datahantering har spelat en roll för organisationer vid flytten till distansarbete. Vi inriktar också våra intervjuer på organisationer som har en bättre förståelse för IT-säkerhet och datahantering.

2 Litteraturgenomgång

Litteraturgenomgången består av de studier, data och teorier som berör ämnet och har utförts för att skapa en bredare kunskap och uppfattning gällande ämnet. Inledningsvis introduceras information om distansarbete före såväl som under Covid-19 pandemin och IT-säkerhetens potentiella brister på sådant arbete. Följt beskrivs Informationssäkerhet med ämnena Molntjänster, Typer av angrepp och Preventiva medel mot nämnda angrepp. Vidare beskrivs Informationssäkerhet inom organisationer med ISO-standarder och utbildningar för att avsluta med teorier inom IT-Säkerhet och informationssäkerhet där TTAT och CIA-Triaden beskrivs.

2.1 Övergång till distansarbete

2.1.1 Distansarbete före Covid-19

Hemarbete har funnits även före pandemin i flertalet branscher, huvudsakligen för ökad flexibilitet och en form av balans i arbetslivet kontra privatliv. Organisationer har använt möjligheten med distansarbete för att öka sin konkurrenskraft, men samtidigt reducera kontorsytan genom att erbjuda anställda hemarbete några dagar i veckan (Felstead, Jewson, Phizacklea & Walters, 2002). Samtidigt har anställda även drivit frågan genom sina preferenser att jobba hemifrån, och på så sätt uppnå ett flexibelt arbete. I huvudsak har detta dragit till sig familjer som inte varit intresserade eller haft möjligheten att bosätta sig på ny ort; men också för att locka spetskompetenser organisationen har behov av och därför inte fastställa ett mandat där individen behövt flytta för att jobba på kontoret (Bryant, 2000). En studie på 273 högutbildade individer från expertis inom ingenjörer, revisorer, försäljning och marknadsföring kom fram till att arbetsuppgifter dessa individer utförde presterade bättre under distansarbete när man utförde arbete som inte krävde någon form av samarbete (Golden & Gajendran, 2018).

Organisationer får en större utmaning att övervaka sina anställda och behöver lita på att arbetsuppgifter sköts och färdigställs hemifrån på samma sätt som de görs på kontoret, vilket kan krocka med kulturer som arbetar åt ett mer hierarkiskt håll, eller chefer som känner behov av att övervaka när och hur länge sina anställda arbetar. Arbetsgivaren är rädd att arbetstagaren utvecklar incitament genom att lägga ner mindre tid och energi på arbetsuppgifterna än man tidigare gjort, vilket kan resultera i sämre slutprodukter (Rupietta & Beckmann, 2017).
Man har framställt fyra nyckelkompetenser som ska bilda ett lyckat distansarbete som samtliga parter också ska kunna vara nöjda med. Dessa fyra nyckelfaktorer är; fastställa beteenderiktlinjer, utveckla tillit, koordinera information och slutligen använda media. Genom att fastställa riktlinjer som anställda ska agera efter, och att man samtidigt sätter gränser för vad som är accepterat ur ett arbetsperspektiv klarlägger man första faktorn. Genom att koordinera information i en organisation ser man till att samtliga arbetsuppgifter håller en

förutsedd standard. Utvecklingen av tillit mellan arbetsgivare och arbetstagare är högst relevant då man arbetar mot ömsesidiga mål, där båda parter bör både respektera varandra som går hand i hand med tillit. Användningen av media ska finnas för att organisationen ska kunna samarbeta och hålla kontakt ur ett digitalt sammanhang (Makarius & Larson, 2017).

2.1.2 Distansarbete under Covid-19

Även om en del organisationer tidigare tillät sina anställda att arbeta hemifrån fanns det fler organisationer före covid-19 pandemin som inte hade den möjligheten eller intresset. Organisationer som i regel inte tidigare erbjudit distansarbete antogs en större utmaning när man från den ena dagen till den andra skickade hem sina anställda och inte hade några bestämda åtgärder för hur distansarbete skulle gå till (Richter, 2020). Anställda kände flera osäkerheter inför omställningen till ett fullständigt digitalt arbete, bland annat då de öppnade upp för högre ansträngning och stressfylldhet, svårigheter att anpassa sig till digitala lösningar, digitala möten och högre självständighet och självdisciplin. En studie visade på att distansarbete har medfört stress och obalans då anställda, ofta familjer, får det svårt att fokusera i hemmiljö om man inte tidigare utsatt sig för det ur ett arbetsperspektiv, i synnerhet visade kvinnor, både med och utan barn högre stress och obalans än andra (Amis & Greenwood, 2020).

Distansarbete var inte bara en negativ aspekt, utan det öppnade även dörrar för förbättringar som vissa organisationer innan pandemin listat ut, som att anställa specialister utanför sin lokala närhet, och att många arbetsuppgifter kan öka koncentrationen för individuella uppgifter (Razmerita, L. et al. 2021). En studie visade att över 73% hade en positiv inställning för hemarbete gentemot resterande 27% som hade en negativ syn. I samma studie visade över 60% förtroende, förväntan och glädje för kulturen med distansarbete. Då studien gjordes på ett globalt plan fastställde man att erfarenheterna man fått av hemarbete väger mer positivt än negativt (Dubey och Tripathi, 2020).

2.1.3 IT-säkerhetens potentiella brister vid hemarbete

Övergången till hemarbete har skapat nya möjligheter för förövare som vill åt företagshemligheter eller annan data som de inte har behörighet till. Det finns flertalet kryphål en förövare kan använda till sin fördel, där bland annat följande kryphål kan utnyttjas (Mandal och Khan, 2020).

Identifikator
Dålig eller ingen användning av identifikator via tredjepart, som tillåter anställde komma åt arbetsuppgifter i en organisations system (Mandal och Khan, 2020).

Användning av hemnätverk
Uppkopplingen till en organisations resurser via molntjänster eller liknande kan bli attackerade genom en anställds osäkra hemnätverk. Detta kan vara ens internetleverantör (ISP) som inte hanterar protokoll som ska säkra integriteten hos sina kunder, vilket kan resultera i *Spoofing* (användningen av en förfalskad eller lånad identitet) (Mandal och Khan, 2020).

Exponering av resurser
Vid fall där man inte utbildar anställda om riskerna och hur man bör agera och behandla data

kan det leda till felanvändning och omedvetenhet (Mandal och Khan, 2020).

Brist på uppgradering
När en organisation inte förnyar sina riktlinjer för säkerhet då hemarbete blir det nya vanliga blir det snabbt en ond spiral. Detta genom en för liten budget på säkerhet (Mandal och Khan, 2020).

Attacker genom *Social Engineering*
En av de mest frekventa attackerna som sker idag. Det fungerar genom att förövaren lurar en individ att avslöja känslig information som lösenord, personnummer och annan känslig information den attackerade har tillgång till (Mandal och Khan, 2020).

Nätfiske *Phishing*
En del av *Social Engineering* där man utnyttjar social media (Email, Facebook, WhatsApp mm) där förövaren framställer sig vara en betrodd person, exempelvis en chef eller annan individ med förtroende, som behöver åtkomst till känslig data, och får vad hen vill då det ser trovärdigt ut om det kommer från den specifika individen (Mandal och Khan, 2020).

Ransomware Attacks
En *Ransomware* attack utförs av en förövare som på något sätt fått tillgång till ett företags system eller data. Förövaren låser tillgången med hjälp av kryptering för att sedan begära kompensation för att företaget skall få tillbaka tillgången igen, därav namnet *Ransomware* eller utpressningsprogram (Eklund, 2020).

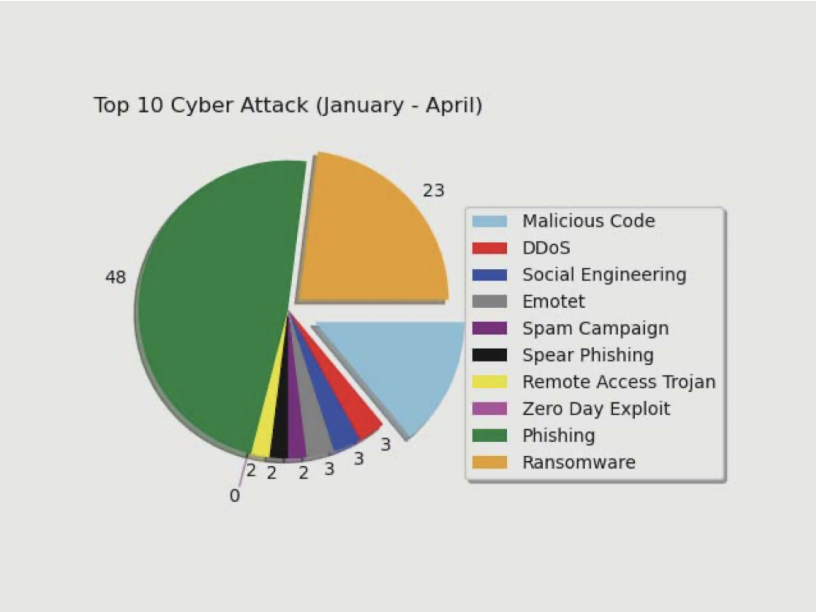
2.2 Informationssäkerhet

2.2.1 Molntjänsters inverkan på informationssäkerhet

En nyckelfaktor som många företag anpassar i sin organisation är molntjänster som hjälper samtliga att ha tillgång till information var man än befinner sig vilket tar bort kravet att förse sig med en egen serverhall som ska kontrolleras, säkerställa en hög standard och kunna vara i drift dygnet runt. Detta medför en trend i minskad investering på hårdvara bland organisationer där målet slutligen är att byta ut dessa investeringar från hårdvara till outsourcing av molntjänster. Vid en undersökning efter första vågen av Covid-19 svarade 51% av respondenterna att man planerade en övergång från sin egen hårdvara till molntjänster, för hantering av data. Molntjänster genererar högre trafik då samtliga i en organisation behöver komma åt sina program och information, vilket även ökar risken för dataintrång vid hög användningsgrad då alla kommer åt sina arbeten på olika platser (Mandal och Khan, 2020). En undersökning gjord av Verizon, 2020, visade att från Mars till Juni samma år blev 474 unika dataintrång rapporterade världen över (Verizon, 2020). I mars 2020 släppte Microsoft siffror om att deras molntjänst fått en ökad i användningsgrad med 775% (McAfee, 2020).

Processen mellan implementation av molntjänst och tidigare lösning kan medföra säkerhetsrisker då all data kommer överföras mellan befintlig lösning till molntjänsten. Detta gör att man förlitar sig på sin internetleverantör att hålla datan som laddas upp säker utan att obehöriga individer kan komma åt den. Internetleverantören för en organisation ska ses som opålitlig då denna är utanför organisations omfattning, likt sin molntjänstleverantör. Under den specifika tidsramen när överföring av data sker kan man se ökad frekvens av försök till

dataintrång, då förövare kan följa upp när de ser att höga nivåer av data skickas mellan få mottagare och sändare. Det finns risker även efter implementationen av molntjänster som är exklusivt för just molntjänster, till detta hör oförmögenheten att själva kontrollera sitt datacenter och fulländat förlita sig på sin molntjänstleverantör vilket blir en riskanalys om möjligheten för dataintrång via leverantörers system (Mandal och Khan, 2020).



Figur 2.1: Top 10 Cyber Attacks (ITC Secure, 2020)

Några av de vanligaste attackerna finner sig i samlingsordet nätfiskeattacker, även känt som Phishing/nätfiske, där de vanligaste attackerna inom molntjänster är följande; *Man-in-the-Middle Attack* där förövaren placerar sig mellan en användare och applikation för att övervaka och få tillgång till personuppgifter, kreditkort med mera (Imperva, u. å.), *Cross-Site Scripting* där förövaren applicerar ett illvilligt programmeringsskript på en betrodd hemsida (Kirsten, u. å.), *SQL Injection* där förövaren gömmer kod i ett skript som skapats för att förstöra en databas (W3schools, u. å.), samt *Replay Attacks* där förövaren får tillgång till data som skickas över ett nätverk mellan sändare och mottagare, och i sin tur skickar samma data igen för att bli auktoriserad på samma sätt som den verkliga sändaren (Saxena, 2020).

2.2.2 Preventiva medel för molntjänster

Att införa riktlinjer för att motverka dataintrång är att rekommendera. Riktlinjerna ska verka som en tillräckligt hög tröskel för förövaren att komma åt information som den inte har behörighet till, vilket i sin tur kan leda till skadegörelse. Detta kan vara både enkla riktlinjer som man kan använda på individuell nivå, exempelvis lösenordshanterare och säkerhetskopiering av data till en extern hårddisk. På den organisationella nivån kan man ofta lägga mer resurser genom exempelvis blockering av externa minneskort, exempelvis minneskort och extern hårddisk, i dess hårdvara, som arbetsdator och mobiler. Detta kan man uppnå genom att låsa organisationens hårdvara från att installera och godkänna något annat än dess officiella utrustning eller som organisationen godkänt när det kommer till installationer av programvaror. Att klarlägga en tydlig hantering för anställda hur man på en individuell nivå ska arbeta för att motverka intrång, vilket man kommer långt på genom att ha kritiskt tänkande för något som känns eller låter orealistiskt (Mandal och Ali Khan, 2020).

2.3 Informationssäkerhet inom organisationer

Den mänskliga faktorn står som den huvudsakligt felande faktorn vid lyckade intrång som resultat av angrepp mot informationssystem. Denna faktor används som en grundprincip av individer som utvecklar just skadlig programvara (Kobis, 2021). För att kunna förebygga dessa eventuella angrepp och intrång väljer många organisationer att använda sig av framtagna ISO-Standarder som utbildning i informationssäkerhet, för att försöka att minimera den mänskliga faktorn.

2.3.1 ISO-Standarder

Till vanligheterna arbetar organisationer ofta med standarder och policys för en given situation. Informationssäkerhet är inget undantag, ofta använder man standarder som följer ISO-protokoll, *Internationella standardiseringsorganet,* inom specifikt IT-säkerhet används bland annat: *ISO/IEC 27001 Information Security Management* (ISO 27001) som finns att tillämpa och används ofta som grund för många organisationers informationssäkerhet (Monev, 2020).

Standarden är en del av ISO 27000-serien, även kallad ISO27k, som innehåller informationssäkerhet standarder för organisationer oberoende av storlek som berör en bred aspekt av informationssäkerhet och är inte begränsat till endast tekniska problem (Najib, Sumaryono, Nugroho, & Putra, 2018).

ISO 27001 består av en lista säkerhetskrav som organisationer ska uppnå för att enligt rätt praxis följa standarden (Najib et al. 2018). Nästkommande standard, ISO 27002, ger riktlinjer för bästa praxis om kontroller inom informationssäkerhet (Monev, 2020). Tredje standarden vid namn ISO 27003 ger riktlinjer och vägledning för dem nämnda kraven som förmedlas under ISO 27001 (Najib et al. 2018).

2.3.2 Utbildningar inom Informationssäkerhet

Utbildning inom informationssäkerhet är ett effektivt sätt att skapa medvetenhet hos de anställda inom en organisation och har stor påverkan på individens faktiska beteende rörande informationssäkerhet och riskerna som finns (Stefaniuk, 2020). Följden när organisationer erbjuder utbildningar resulterar i att de anställda får högre medvetenhet och agerar därav i enlighet mot säkerhetspolicys och andra områden utbildningarna täcker. Några exempel där utbildningar främjat säkerhetstänkande hos anställda är minskade fall av: förlorad data från bärbara enheter, användandet av enheter till både arbetsrelaterade och personliga bruk, delande av inloggningsinformation med kollegor eller låta information existera synligt i allmänt utrymme (Stefaniuk, 2020).

Det bör noteras att även om organisationer investerar i utbildningar på sina anställda i större utsträckning inom informationssäkerhet ser man ändå en ökning i lyckade intrång till följd av den mänskliga faktorn. Detta kan bero på olika faktorer som: Allmänt slarv, bristande efterlevnad av säkerhetspolicies, men även om organisationen i fråga inte lyckas uppmärksamma hur man på bästa sätt ska nå fram till sina anställda utifrån ett utbildningsperspektiv. Detta kan bero på att den anställda tar del av en stor mängd olika andra utbildningar vilket kan leda till låg motivation och svårigheter att ta in samtlig informationen

samtidigt som man ska försöka komma ihåg vad som sagts (Alshaikh, Maynard, Ahmad, & Chang, 2018).

För att kunna maximera motivation och hitta en gemensam grund föreslås det att använda sig av utbildningar där man håller gruppdiskussioner och workshops för att få en mer interaktiv utbildning. En interaktiv typ av utbildning främjar adoptering av kollegors positiva beteende rörande informationssäkerhet samt att anställda känner en högre mening i att delta under utbildningen, vilket återigen engagerar dem att lära sig mer om ämnet (Khan, Alghathbar, Nabi & Khan, 2011).

2.4 Teorier inom IT-Säkerhet och informationssäkerhet

Här presenteras en teori om individens tillvägagångssätt vid IT-säkerhetsrisker och hot samt en vägledande teori för säkerhetsriktlinjer, processer och procedurer inom informationssäkerhet.

2.4.1 Technology Threat Avoidance Theory

Technology Threat Avoidance Theory (TTAT) har avsikten att se till individens engagemang gällande potentiella säkerhetsrisker inom IT. Detta baseras på den upplevda risken eller hot för hur man bör agera gentemot dessa baserat på ett antal givna variabler (Liang & Xue, 2009).

Man ger ett antal påstående om individens motivation och tankeväg när det kommer till säkerhetsrisker inom IT. Dessa baseras på vad individen har för tidigare erfarenhet inom IT och vilken grad man informerats om de potentiella riskerna samt metoderna som finns att förse sig med för att undvika dessa (Liang & Xue, 2009).

Ett påstående är att individen inte utreder hanteringen av en potentiell säkerhetsrisk innan man har informerats, undersökt eller skapat erfarenhet av det givna problemet eller hotet. Här presenteras två olika tillvägagångssätt för att hantera potentiella säkerhetsrisker, ett problemfokuserat och ett känslofokuserat tankesätt. Det problemfokuserade ser till en inställning av logiskt tänkande och problemlösning, där man söker grundproblemet och vidtar skyddsåtgärder för att motverka riskerna. Detta kan uppnås genom installation av säkerhetsmjukvara på enheter/hårdvara, inaktivera *cookies* eller uppdatera sitt lösenord vid jämna mellanrum (Liang & Xue, 2009).

När man ser till det mer känslofokuserade tankesätten, speglar detta sig som en reaktion och kan uttryckas som känslor om fatalism, förnekelse eller hjälplöshet inför det givna problemet eller de hot som kan uppstå. Detta tillvägagångssätt ändrar inte den objektiva verkligheten och har ingen påverkan på de potentiella säkerhetsriskerna men kan däremot hjälpa individen att mentalt hantera dessa (Liang & Xue, 2009).

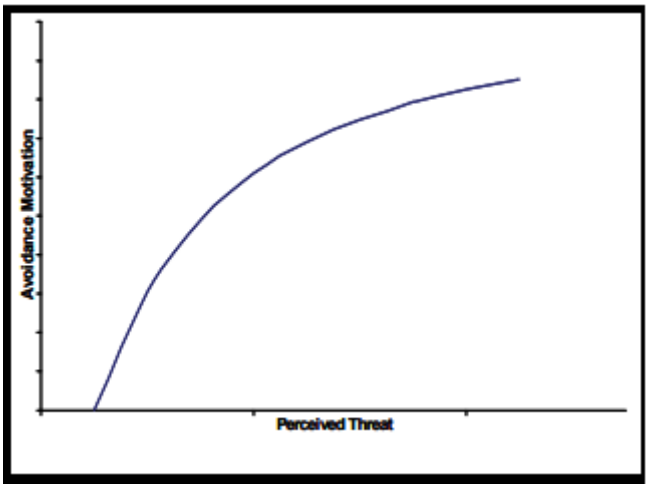
Det problemfokuserade tankesättet tenderar vara det första tillvägagångssättet vid rationellt tänkande där ett antal tillgängliga säkerhetsalternativ vägs mot varandra för att finna den som minskar hotet på bästa sätt. Om individen inte kan finna ett lämpligt säkerhetsalternativ tillgänglig i sitt repertoar så tenderar individen att se till det känslofokuserade tankesättet som en utväg istället (Liang & Xue, 2009).

Ett annat påstående är att ju mer informerad eller erfaren individen är om de potentiella riskerna eller hoten som kan påverka denne, desto större blir också upplevelsen om potentiella hot och risker inom IT. Detta speglas tydligast bland de som varken är informerade om risker/hot eller direkt påverkats av liknande händelser, då de lågt informerade inte heller har någon upplevelse av att dessa kan påverka individen direkt (Liang & Xue, 2009).

Man presenterar även nyckelvärden till varför individer väljer att använda sig av säkerhetsåtgärder som till exempel: om individen känner sig säker på att den givna säkerhetsåtgärden kommer motverka den avsedda risken eller hotet på ett effektivt sätt. Det finns även den ekonomiska aspekten där motivationen skapas när individen ser att säkerhetsåtgärdernas potentiella kostnader står sig lägre än de potentiella kostnaderna som hoten eller riskerna kan orsaka (Liang & Xue, 2009).

Individer som upplever att man kan motverka och undvika risker/hot visar också högre motivation till användningen av skyddsåtgärder samtidigt som de är mindre motiverade att gå mot det känslofokuserade tankesättet. Samma grundregel gäller vid motsatt situation där individer som upplever att en risk eller ett hot inte går att undvika tenderar inte heller att använda sig av skyddsåtgärder utan letar sig snarare istället åt det känslofokuserade tankesättet (Liang & Xue, 2009).

I modellen nedan presenteras relationen mellan de upplevda riskerna och hoten i korrelation med motivationen att undvika dessa med hjälp av att använda säkerhetsåtgärder. Man kan se att motivationen för undvikandet av hot och risker avtar desto större hotet eller risken upplevs vara av individen. Men att de upplevda riskerna och hoten har en direkt relation i motivationen till att undvika dessa, vilket i sin tur leder till faktiska handlingar i form av implementation av säkerhetsåtgärder som nämnda tidigare i det problemfokuserade tankesättet (Liang & Xue, 2009).



Figur 2.2: The Curvilinear Relationship between Perceived Threat and Avoidance Motivation (Liang, 2009)

2.4.2 CIA-Triaden

CIA-Triaden är en modell som presenterar tre huvudsakliga ämnen för att kunna förstå och diskutera informationssäkerhet på ett djupare plan, samt stödja säkerhet gällande data som

modellen fokuserar på. Modellen nedan presenterar tre kategorier: *Confidentiality, Integrity & Availability* (Andress, 2014, s.5-6).

Figur 2.3: CIA-Triaden (Andress, 2014, s.5)

Den första punkten, *Confidentiality*, handlar om sekretess och skydd av känslig information som till exempel personlig information. *Confidentiality* ser till möjligheten att skydda data med genom användningen av behörighetskrav på den givna data som önskas extraheras där endast den individen som har behörighet också har unik tillgång. De största hoten som läggs på denna typ av skydd är kompromissade lösenord på grund av till exempel dataintrång eller lösenordsfiske då skyddsåtgärden oftast förlitar sig på lösenord. Denna typ av skydd är en viktig del av sekretess som helhet men endast en aspekt (Andress, 2014, s.6).

Den andra punkten som nämns är *Integrity* och denna syftar till integriteten av den given data och hur denna både kan bevaras i sitt korrekta stadie utan att manipuleras av obehöriga inmatningar av data. *Integrity* ser även till bevaringen av den befintliga datan i den mån om att datan i fråga inte ska kunna bli raderad av såväl obehöriga som behöriga inmatningar och i det fall att detta skulle ske skall den raderade datan kunna återskapas. Här är det vanligt att ovannämnda *Confidentiality* används för att nå den efterfrågade integriteten på den givna datan i form utav behörighetskrav för nämnda inmatningar (Andress, 2014, s.6-7).

Den sistnämnda punkten, *Availability*, ser till just detta, tillgängligheten på den givna data som önskas att extraheras ur ett mer praktiskt sett. Finns det potentiella förhinder eller risker med tillgängligheten av datan såsom problem med den fysiska infrastrukturen och/eller IT-infrastrukturen som förhindrar eller försvårar tillgängligheten på data (Andress, 2014, s.7).

Med denna hjälp av denna modell kan man se till och diskutera informationssäkerhetens problem från en mer strikt modellerad synvinkel där samtliga aspekter kan övervägas, *Confidentiality, Integrity & Availability,* för att utveckla säkerhetspolicys, processer och procedurer inom informationssäkerhet.

2.5 Litteratursammanfattning

För att bygga en grund till den empiriska datainsamlingen, så följer nedan en litteratursammanfattning indelad i Kategorier som har undersökts ovan, de Undersökningsområde inom nämnda kategorier, samt den litteratur som används och har hittats gällande dessa område och kategorier (Se Tabell 2.1).

Tabell 2.1: Litteratursammanfattning

Kategori	Undersökningsområden	Litteratur
Distansarbete	● Före Covid-19	Felstead, Jewson, Phizacklea & Walters (2002), Bryant (2000), Golden & Gajendran (2018), Rupietta & Beckmann (2017), Makarius & Larson (2017)
Distansarbete	● Under Covid-19	Richter (2020), Amis & Greenwood (2020), Razmerita, L. et al. (2021), Dubey och Tripathi (2020)
Distansarbete	● IT-säkerhetsbrister	Mandal och Khan (2020), Eklund (2020)
Informationssäkerhet	● Molntjänster	Mandal och Khan (2020), Verizon (2020), McAfee (2020), ITC Secure (2020), Imperva (u. å.), Kirsten (u. å.), W3schools (2022), Saxena (2020)
Informationssäkerhet	● Preventiva medel	Mandal och Khan, 2020

Informationssäkerhet	● ISO-Standarder	Kobis (2021), Monev (2020), Nejib et al. (2018)
Informationssäkerhet	● Utbildningar	Kobis (2021), Stefaniuk (2020), Alshaikh, M. et al. (2018), Khan, B. et al. (2011)
Teorier inom IT-Säkerhet och informationssäkerhet	● TTAT	Liang & Xue (2009)
Teorier inom IT-Säkerhet och informationssäkerhet	● CIA-Triaden	Andress (2014)

3 Metod

Under detta kapitel presenteras den metod vi valt för att samla in den empiriska data vi använt för denna studie. Här presenteras även urvalet av organisationer och respondenter som gjorts för att sedan presentera detaljerna gällande intervjuerna utförda såsom en intervjuguide, bearbetningen av data samt etiken rörande samtliga.

3.1 Metodval

För att få en större och djupare kunskap inom området så bestod det initiala arbetet av en litteraturstudie som skulle komma att vara grund till såväl vårt huvudsakliga forskningsområde och forskningsfråga som till den faktiska empiriska datainsamlingen och deras struktur. För att kunna utföra mer forskning på området samt få en bättre insikt om hur pandemin har påverkat IT-Säkerheten inom de svenska organisationernas så valde vi även att utföra en egen datainsamling. Denna insamling som är vår praktiska metod ska bestå av kvalitativa studier och detta i form av intervjuer.

Då avsikten var att få en djupare förståelse för organisationernas olika reaktioner såväl som individens reaktion anser vi att denna typ av studie är mer relevant då detaljer och nyanser prioriteras och låter respondentens uppfattningar och känslor presenteras på ett mer öppet vis med få begränsningar (Jacobsen & Hellström, 2002). Detta kräver även djupare och mer detaljerad information och denna typ av information kan anses känslig för de givna organisationerna vilket gör att denna typ av insamling lämpar sig bättre. Detta då respondenterna kan vara mindre benägna att delge sig om sådan information om de efterfrågas att skriva ner sina svar utan att träffa oss som intervjuare i till exempel ett svarsformulär (Oates, Griffiths & McLean, 2022).

Denna typ av intervju öppnar även upp för följdfrågor och diskussioner som inte nödvändigtvis behöver hålla sig till en given intervjuguide vilket bidrar till att resultatet kan komma att bli åt en mer objektiv synvinkel och verklighetstrogen än till exempel vid studier som använder sig utav enkäter med förbestämda statiska frågor utan möjlighet till följdfrågor samt diskussioner där resultatet kan tolkas beroende på given synvinkel (Jacobsen & Hellström, 2022).

Denna metod är mycket resurskrävande då dessa intervjuer tar lång tid att genomföra, transkribera samt analysera vilket medför att antalet respondenter för vardera given studie, beroende på de resurser som är tillgängliga, är väldigt få. Det medför i sin tur att det kan vara svårt att generalisera resultatet på en större skala och dra slutsatser baserat på detta (Oates, Griffiths & McLean, 2022).

3.2 Urval

För att utföra denna kvalitativa studie krävdes att ett urval av såväl organisationer som respondenter inom dessa organisationer utfördes innan någon organisation kontaktades för att få så relevant information och kunskap om ämnet som möjligt.

3.2.1 Urval av organisation

När vi såg till vilka typer av organisationer vi önskade intervjua såg vi till organisationer där IT och/eller IT-säkerhet, samt känslig information, var av stor vikt. Dessa typer av organisationer ansåg vi vara av hög relevans då de är mest närvarande inom riskerna för IT-säkerhet och därmed också de mest utsatta på grund utav arbetsskiftet som kom med pandemin. Dock, för att kunna upptäcka potentiella inkonsekvenser, hade vi för avsikt att intervjua olika organisationer med olika mål, dels organisationer från den privata sektorn såväl som en organisation från den offentliga sektor. Här var avsikten att skapa en tydligare och opartisk bild över hur direktiv och riktlinjer nyttjas oberoende av organisationens syfte.

3.2.2 Urval av respondent

Vid urvalet av respondenter från de givna organisationerna löd samma tankesätt som nämnt ovan där respondenten har IT och/eller IT-säkerhet inom sitt ansvars- eller kunskapsområde för att få så relevanta resultat som möjligt och även möjligheten att kunna hämta aktuell information om ämnet och respondenternas inverkan i de svenska organisationernas syn på IT-Säkerhet.

3.2.3 Organisationer och respondenter som medverkar i studien

Baserat på ovanstående urval började vi ta kontakt med organisationer i våra nätverk för att fylla rollen om ett företag som behandlar en stor mängd känslig information såväl som ett företag där säkerhet i allmänhet var av stort fokus. Utöver detta försökte vi även ta kontakt med kommuner och universitet för att kunna ha med en aspekt av organisationer som inte har vinstdrivna initiativ. Tyvärr fick vi dock ingen respons från organisationerna inom myndigheter. Vidare gjordes ett antal kontaktförsök med olika organisationer och potentiella respondenter inom dessa organisationer, vilket ledde fram oss till följande som medverkat i denna studie:

Organisation 1: ***Pwc Sverige***

PwC Sverige (PricewaterhouseCoopers) är ett revisions- och konsultföretag med cirka 295000 anställda i över 150 länder varav runt 2800 är anställda i sverige (PwC, u. å. a). Bolaget etablerades år 1999 som följd av en fusion mellan Öhrlings Coopers & Lybrand och Price Waterhouse (PwC, u. å. a). PwC Sverige behandlar mycket känslig information såväl internt som om deras kunder, 2021 till exempel arbetade PwC med 84% av Global Fortune 500 företagen (PwC, u. å. b) och har därför ansetts högst relevanta i denna studie.

Organisation 2: ***Assa Abloy***

Assa Abloy är en koncern inom lås-, säkerhet och dörrlösningar med cirka 51 000 anställda i över 70 länder (Assa Abloy, u. å.). Utöver ovan nämnda affärsområden sysslar Assa Abloy även med mobila och biometriska identitetskontroll system samt annan typ av säker identifiering (Assa Abloy, u. å.). Bolaget etablerades år 1994 som en följd av en fusion mellan Securitas och Metras Oy:s låsverksamheter Assa och Abloy (Assa Abloy, u. å.).Assa Abloy har säkerhet som sitt huvudsakliga affärsområde och hanterar även här känslig information såväl internt som om deras kunder och anses därför också högst relevanta i denna studie.

Organisation 3: ***Grade AB***

Grade är ett svenskt företag med 40 anställda som utvecklar och levererar bland annat sitt Talent Management System kallat Grade-plattformen (Grade, u. å.). Grade grundades år 1995 som en del av ett projektarbete vid Lunds Universitet men har sedan dess progressivt gått över till företagskunder, framförallt efter 2015 (Grade, u. å.). Grade har kunder såsom Telenor, Transportstyrelsen och Göteborgs Stad med flera och arbetar i IT-branschen och programutveckling vilket gör att de därför ansetts relevanta i denna studie.

Organisation 4: ***Know e AB***

Knowe är ett svenskt företag grundat 2013 med 17 anställda som arbetar inom IT-branschen och programutveckling och levererar digitala lösningar till deras kunder som består av privata såväl som kommunala företag inom bland annat sjukvården (Knowe, u. å.). Eftersom att Knowe arbetar i ovannämnda bransch med material som kan anses känsliga så har de därför ansetts relevanta i denna studie.

Tabell 3.1: Respondenter

Namn	Yrkesroll, Titel	Erfarenhet inom IT	Organisation	Intervjutyp, Längd	Datum och tid	Appendix
Respondent 1 (R1)	Systemtekniker /Utvecklare	12 år	PwC Sverige	Videomöte 30 min	28 April 2022 Klockan 10:00	A
Respondent 2 (R2)	Global Cyber Security Operations Manager	25 år	Assa Abloy	Videomöte 50 min	3 Maj 2022 Klockan 08:30	B
Respondent 3 (R3)	Product Owner	15 år	Grade AB	Videomöte 35 min	6 Maj 2022 Klockan 14:00	C
Respondent 4 (R4)	VD	25 år	Know e AB	Videomöte 25 min	10 Maj 2022 Klockan 15:00	D

3.3 Intervjuer

Intervjuerna hölls på distans för att dels minska resurserna som krävs från båda parter men även öppna upp för alternativ av organisationer som inte befinner sig i närområdet och därmed utöka de potentiella urvalet av respondenter (Oates, Griffiths & McLean, 2022). Utöver detta känner vi att denna metod lämpar sig bättre i kontexten av detta arbete där distansarbetet och distanskommunikation är i fokus.

Eftersom att en inspelad intervju är det ideella slag av rådata för kvalitativa metoder så kommer detta vara av prioritet vid våra intervjuer och samtliga intervjuer kommer att spelas in (Jacobsen & Hellström, 2002). Vi kommer även att, i den mån som går, använda oss av videomöten snarare än endast telefonsamtal för intervjuerna eftersom man lättare kan uppfatta hur respondenten känner kring ett ämne och hur långt man kan gå vid till exempel fördjupningsfrågor beroende på respondentens ansiktsuttryck och kroppsspråk med mera (Oates, Griffiths & McLean, 2022; Jacobsen & Hellström, 2002).

För att kunna strukturera intervjuerna på förhand och tala om relevant information för denna studie så skapades en intervjuguide. Utgångspunkten är en semi-strukturerad intervju där vi kommer att huvudområden och delområden samt frågor kopplade till dessa men där ordningen på frågorna kan komma att förändras under intervjuernas gång för att få ett bättre flyt i konversationen (Oates, Griffiths & McLean, 2022). Denna typ av intervju innefattar även nya frågor som kan komma att dyka upp baserat på respondenternas svar vilket kan fördjupa informationen och även relevansen av denna (Oates, Griffiths & McLean, 2022).Om man inte skulle välja att strukturera dessa intervjuer på förhand finns det en risk att resultatet blir nästintill omöjligt och/eller komplext att analysera (Jacobsen & Hellström, 2002).

3.3.1 Intervjuguide

Intervjuguiden är baserad på litteratursammanfattningen (Se Tabell 2.1) med tre övergripande kategorier: Distansarbete, Informationssäkerhet samt Teorier inom IT-Säkerhet och informationssäkerhet. Under dessa följer vi sedan litteratursammanfattningen återigen med Undersökningsområden där relevanta frågor har tagits fram baserat på litteraturgenomgången och vår forskningsfråga.

För att få relevant information om respondenten samt organisationen som respondenten arbetar för lades även en Introduktionsdel till där konsensus efterfrågas för att kunna använda ovan nämnd information. En kort introduktion av studien och forskningsfrågan presenteras även innan intervjun för att informera respondenten översiktligt om vad intervjun kommer att handla om.

Samtliga frågor och följdfrågor, utöver Introduktionsdelen, kan komma att ändras eller tas bort och ytterligare frågor kan komma att läggas till under samtalets gång för att nå den öppenhet som dessa intervjuer är avsedda att ha. Nedanstående Intervjuguide (Se Tabell 3.2) skall alltså inte anses som ett manus utan som stöd för att hålla konversationen runt rätt ämne och för att underlätta den efterföljande analysen av nämnd konversation.

Tabell 3.2: Intervjuguide

Intervjuguide

Introduktion

- Är det okej att vi spelar in denna intervju, och att vi använder din titel samt organisationens namn i uppsatsen? Uppsatsen kommer senare att publiceras av Lunds Universitet.

- Vad är din titel?

- Vilken organisation arbetar du för?

Distansarbete

Före Covid-19 pandemin

- Hade ni möjlighet till hemarbete före Covid-19 pandemin?
    - Om ja, hur såg möjligheterna ut, exempelvis antal dagar i veckan, hur många skulle du säga gjorde detta? Hur såg säkerhetsåtgärderna ut vid hemarbete?(Både praktiska åtgärder samt riktlinjer)
    - Om nej, fanns det ett intresse för hemarbete från de anställda?

Under Covid-19 pandemin

- Beslutade sig organisationen om samtliga skulle arbeta hemifrån?
    - Om ja, när började man med detta?

- Fanns det anställda som inte kunde arbeta hemifrån?
    - Om ja, hur löste man detta?

- Är dem flesta positivt eller negativt inställda till hemarbete?
- Känner du att effektiviteten förbättras eller försämras vid hemarbete?
- Har säkerhetsåtgärderna förändrats på grund av flytten till hemarbete?

IT-Säkerhetsbrister vid hemarbete

- Övergången till hemarbete har medfört nya potentiella brister för IT-säkerheten, exempelvis användandet av/- och inte av auktoriseringsverktyg och uppkoppling via hemnätverk mm. Har ni märkt av ökat tryck från förövare som inriktar sig på hemarbetet och den enskilde anställda?

- Har ni märkt något skillnad på mängden eller typen av försök till dataintrång sedan flytten till distansarbete?
    - Om ja, vad tror du detta beror på och vilka typer av dataintrång har varit mest aktuella?
    - Om nej, vad tror du detta beror på?

Informationssäkerhet

Molntjänster

- Använder ni er utav molntjänster?
  - Om ja, vilken?
    - Under implementation av molntjänster så medför det också högre risk för dataintrång, hur såg ni på detta och hur motverkade ni eventuella risker?
    - Har er leverantör av molntjänst någon gång utsatts för försök till dataintrång som har påverkat er?
  - Om nej, hur arbetar ni för samtliga anställda skall komma åt era system samt data?

Preventiva medel

- Använder ni er av några typer av skydd (som lösenordshanterare och blockering av egna minneskort mm.)?
  - Om ja, vilka?
- Finns det givna riktlinjer för anställda gällande motverkandet av dataintrång?
  - Om ja, vilka?
  - Om ja, har dessa förändrats på grund av flytten till hemarbete?

ISO-Standarder

- Använder ni er utav ISO-Standarder gällande informationssäkerhet?
  - Om ja, vilken/vilka? (Till exempel ISO27k)

Utbildningar

- Har ni utbildningar gällande informationssäkerhet?
  - Om ja, hur ser upplägget ut på dessa?
  - Om ja, vad är frekvensen på dessa?
  - Om ja, har något utbildning utförts i samband med flytten till hemarbete?
    - Om ja, på vilket sätt skiljer den sig från övriga utbildningar?
  - Om nej, är det något ni har övervägt att införa?

Teorier inom IT-Säkerhet och informationssäkerhet

TTAT

- Hur välinformerade skulle du säga att de anställda på ert företag är gällande IT-säkerhet på en skala?
- Om företaget har gett utbildningar inom informationssäkerhet, har ni märkt någon skillnad i medarbetarnas säkerhetsbeteende? Har ni märkt en minskning eller ökning i lyckade dataintrång?
- Har ni märkt någon skillnad i medarbetarnas säkerhetsbeteende i samband med flytten till hemarbete?

- Om ja, på vilket sätt?

CIA-Triaden

- Hur arbetar ni med konfidentialitet (*Confidentiality*), använder ni er utav behörighetskrav för känslig information?
  - Om nej, hur arbetar ni på ett annat vis?

- Hur arbetar ni för att behålla integritet (*Integrity*) på den data ni erhåller? Finns det även här behörighetskrav för att göra korrigeringar eller radera viss typ av data?
  - Om nej, hur arbetar ni på ett annat vis?

- Hur arbetar ni med tillgänglighet (Availability) av data, finns den tillgänglig på ett och samma ställe men begränsad av till exempel behörighetskrav?
  - Om nej, hur arbetar ni på ett annat vis?

- Har någon av de sistnämnda, konfidentialitet, integritet eller tillgänglighet påverkats på grund av flytten till hemarbete? (Confidentiality, Integrity & Availability)
  - Om ja, på vilket sätt?

3.4 Bearbetning av data

För att lättare kunna bearbeta och sedan analysera den data som samlats in under intervjuerna med responserna så krävdes först och främst en konkret beskrivning av den rådata som vi erhållit och detta utförs i form av transkriberingar av samtliga samtal (Oates, Griffiths & McLean, 2022). Dessa transkriberingar i sitt fullo finner vi under Appendix i enlighet med Tabell 3.1. Dessa transkriberingar i sig presenterar en enorm mängd data som kan anses oöverskådlig som är svår att förstå och tyda i syftet av att analysera dessa (Jacobsen & Hellström, 2002).

För att underlätta analysen och förtydliga de transkriberade intervjuernas ämnen under samtalets gång har ett kodschema skapats (Se Tabell 3.3). Denna är, likt intervjuguiden (Se Tabell 3.2), baserad på litteratursammanfattningen (Se Tabell 2.1) med de tre tidigare nämnda övergripande kategorierna av Distansarbete, Informationssäkerhet och Teorier inom IT-Säkerhet och informationssäkerhet. Vardera kategori har givits en individuell färg för att lätt kunna urskilja ämnen under samtalet. Vidare delas kodschemat upp, likt intervjuguiden, i Undersökningsområden för vardera Kategori med en given kod för att urskilja Undersökningsområdena under samma kategori och återigen underlätta analysen och förtydliga transkriberingarna. Efter att en intervju har transkriberats kategoriseras sedan delar av samtalet med hjälp av färgkodning för att tydligt markera vart i respondentens svar kategorier berörs och sedan tillsätts en kod för Undersökningsområden för att lätt kunna urskilja mer precist vad som berörs under markerat stycke. Transkriberingarna gjordes manuellt av oss för att bli mer familjära med datan och lätt kunna identifiera teman (Oates, Griffiths & McLean, 2022) vilket sedan lätt kunde kategoriseras med hjälp av kodschemat nedan.

Tabell 3.3: Kodschema

Kategori	Kod för Kategori	Färg	Undersökningsområden	Kod för Undersökningsområden
Distansarbete	D	Grön	Före Covid-19	D-FC
			Under Covid-19	D-UC
			IT-Säkerhetsbrister	D-IT
Informationssäkerhet	I	Gul	Molntjänster	I-M
			Preventiva medel	I-P
			ISO-Standarder	I-I
			Utbildningar	I-U
Teorier inom IT-Säkerhet och informationssäkerhet	T	Blå	TTAT	T-T
			CIA-Triaden	T-C

3.5 Validitet och Reliabilitet

Som tidigare nämnt tenderar denna typ metod att generera ett lågt antal respondenter vilket medför att det kan vara svårt att generalisera resultatet på en större skala och dra slutsatser baserat på detta (Oates, Griffiths & McLean, 2022). För att försöka motverka detta har samtliga intervjuer utförts på samma vis med samma intervjuguide för att få resultat inom samma områden och sedan kunna jämföra dessa. Eftersom intervjuguiden inte är ett manus finns det skillnader på intervjuerna men de huvudsakliga områdena och undersökningsområden berörs ändå i samtliga intervjuer. Vidare har vi varit uppmärksamma på återkommande uttalanden från de olika respondenterna som arbetar inom olika branscher för att på så sätt hitta generaliserbar data. Detta kan visa på att specifik data är sannolikt generaliserbar men kan inte bevisas med säkerhet då stickprovet är för litet (Jacobsen & Hellström, 2002).

Om vi ser till tillförlitlighet som syftar till våran egen påverkan på de resultaten som erhållits så leder även här denna typ av metod till en svårighet att uppnå detta i sin struktur då vi som intervjuare kan ha en inverkan på respondenterna och deras svar till en viss grad vilket leder till att en objektivitet kan vara svårt att uppnå (Oates, Griffiths & McLean, 2022). För att försöka minska den externa påverkan på intervjuerna så har vi sett till Kontexteffekt som berör hur kontexten av intervjuerna kan ha påverkat resultatet. Till exempel var denna intervju fysiskt tog plats och om denna miljö anses ovanlig för respondenten vilket kan påverka resultatet om respondenten inte känner sig familjär med kontexten (Jacobsen & Hellström,

2002). Som tidigare nämnt används videomöten för intervjuerna vilket även här spelar en roll då respondenterna i största sannolikhet har använt sig av dessa i sitt arbetsliv under de senaste åren på grund av flytten till hemarbete till följ av Covid-19 pandemin. Detta medför en familjär miljö vilket borde medföra en så liten kontextuella inverkan på respondenterna som möjligt.

Eftersom att samtliga intervjuer spelats in kunde detta sedan användas vid transkribering vilket yrkar på reliabiliteten av datan då dessa transkriberingar inte förlitar sig på minne och kan spelas upp och kontrolleras gentemot det transkriberade innehåll som skapats från vår part (Jacobsen & Hellström, 2002).

3.6 Etik

Det finns ett par etiska grundkrav att se till vid en undersökning med respondenter och dessa är: möjligheten att inte delta i undersökningen, möjligheten att återkalla sitt deltagande i undersökning, möjligheten att kunna ge ett informerat samtycke och kravet på sekretess gällande till exempel personuppgifter (Oates, Griffiths & McLean, 2022).

Samtliga respondenter frivilligt deltagit i samtliga intervjuer genom att tacka ja på vårat utskickade mail där en kort beskrivning av huvudsakliga forskningsområde nämns. När samtalen sedan inleds introduceras samtliga respondenter till det ämne vi syftar att undersöka för att belysa ämnet som intervjun komma att beröra. Följt av detta efterfrågas samtliga respondenter innan inspelning börjar om de godkänner att vi spelar in intervjuerna och när intervjun sedan inleddes, under den introducerande delen av intervjuguiden(Se Tabell 3.2), efterfrågas även samtycke till användning av personliga uppgifter och även information om den givna organisationen vilket lämnar plats för sekretess.
En andel av resultaten syftar till mer personliga erfarenheter vilket kan skyddas genom den tidigare nämnda samtycket på användningen av personliga uppgifter. Huvudområdet i sig anses dock inte vara av stor känslighet för respondenterna i sig eftersom att denna undersöknings huvudsakliga forskningsområde syftar till arbetsplatsen och organisationens reaktioner och strukturella svar på Covid-19 pandemin inom IT-säkerhet.
Utöver detta är även kravet om att bli korrekt återgiven en viktig etisk aspekt (Jacobsen & Hellström, 2002) och för att respondenterna skall bli korrekt återgivna så tar vi hjälp utav transkriberingarna av intervjuerna som finns tillgängliga i undersökningen för att kunna få full kontext av samtalet. Dessa transkriberingar, som nämnts tidigare, har baserats på de inspelade intervjuerna för att säkerställa korrekt återgivning av respondenterna.

4 Empiri

Under detta kapitel presenteras den Empiriska data som samlats in med hjälp av intervjuer baserat på de huvudsakliga kategorier presenterade i Litteratursammanfattningen.

4.1 Distansarbete

Samtliga respondenter kunde styrka på att det fanns möjlighet till en grad hemarbete före Covid-19 pandemin, men att det huvudsakligen användes vid särskilda tillfällen som VAB (Vård Av Barn), vid sjukdom eller liknande scenarion. R2 uppskattade att i dennes arbetsgrupp utnyttjade ungefär 10-20% hemarbete i veckan, men att det skiftade vem som arbetade hemma då det exklusivt skedde när man inte hade möjlighet att ta sig till kontoret. Samtidigt som R1 menade på att det var inte förekom hemarbete i inom arbetsgruppen, även om möjligheten fanns.

Det fanns möjlighet för det, absolut. PwC har väl ändå varit ganska duktiga på att förkratta möjligheten eftersom att vi har många revisorer som är ute och åker, alla är inte alltid inne på kontoret och jobbar. Så att möjligheten att koppla upp sig remote har alltid funnits sen långt innan pandemin kom. -(R1, Rad 8).

På Grade (R3) ansågs man vara på kontoret på heltid före pandemin, men att man hade möjlighet till hemarbete som de andra om det fanns en anledning till det. R3 styrker huvudsakligen på att även om möjligheten fanns så var det inte kulturen på kontoret.

Samma tekniska möjligheter före pandemin som under pandemin men att möjligtvis dem sociala delarna gjorde att det inte var lika accepterat att jobba hemifrån. -(R3, Rad 2)

Enligt R2 var det tidigare närmsta chefen som kunde besluta om hemarbete för de som normalt arbetar på kontoret. Men även innan pandemin fanns det roller där dessa sköttes 100% på distans.

Om du tänker på den svenska organisationen så är det chefen som godkänner. Sen så kan du ju ha en hel roll som du sköter hemifrån, alltså du jobbar 100% hemifrån i ditt arbete. -(R2, Rad 8)

Know e (R4) har även innan pandemin varit inskolade i att jobba som man jobbar bäst, om det så är på kontoret eller någon annanstans så har deras filosofi varit att man ska arbeta på det sätt man är mest kreativ på. Däremot verkade organisationen mer eller mindre enbart arbeta på kontoret.

Men vi har ju alltid haft väldigt fria arbetstider att jobba när man är som mest kreativ och det har gjort att förutsättningarna sett ut att man har arbetsplatsen någonstans mobilt med sig. Så det var riggat för det. -(R4, Rad 8)

vi är ett socialt gäng och arbetade också på det sättet. Inte för att det var något krav på kontorsarbete, men utan att det var så man ville jobba och man tyckte det var kul att träffas. -(R4, Rad 14)

R4 förklarar även att deras organisation genomsyrar IT-kunniga så har de inte heller märkt något behov av att fastställa riktlinjer om hur man ska hantera sina datorer som inlogg/utlogg med mera.

Nej alltså vi har alltid haft en bra hygien i det. Alltså med inloggning och utloggning, sen har vi alltid haft separata kontorsmiljöer som vi kan vara hur dumma i som helst egentligen utan att något skulle kunna ske. -(R4, Rad 10)

Samtliga organisationer som intervjuades har sen länge använt sig av både molntjänster och VPN-tjänster redan innan pandemin som gjorde det enkelt att komma åt sina arbetsuppgifter även utanför kontoret. R3 använder även lösenordshanterare för att öka säkerheten något ytterligare, och använder sig av tjänsten "1Password", då R3 organisation kommer åt kunders databas anser de behöva någon form av hantering för att hålla sina kunders data säker.

Vi har VPN för att komma åt de tekniska miljöerna och sen är allt lösenordsskyddat såklart där vi använder en lösenordshanterare. -(R3, Rad 6)

Samtliga organisationer vi intervjuat beslöt sig för att arbeta hemifrån mer eller mindre samma dag som Folkhälsomyndigheten kom ut med sitt uttalande om att man ska arbeta hemifrån vid möjlighet. Den tuffa utmaningen R2 upptäckte med en ökning från 10-20% hemarbeten till ~100% var trycket på VPN-tjänsterna då trafiken ökade, samt att det medförde problem när deras system, för att upptäcka ovälkomna användare, plötsligt reagerade på spelkonsoler i en medarbetares hemnätverk.

Om vi tittar på min avdelning då på Cybersecurity så fick vi ju, ja vi fick, ja vad har vi 30000 till 40000 användare, vi fick ju minst 10000, 20000 hemmakontor som plötsligt dök upp på våra skärmar. För vi har ju produkter i våra datorer som scannar av och känner av okända enheter, så den funktionen fick man nästan mer eller mindre stänga av för att då hade ju ungarna Playstation och grejor som dök upp. Så vi har ju en sådan, vad ska man säga awareness-funktion som plockar upp, det är ju för att vi ska hela tiden hitta okända devicer i våra nätverk. Så att sådana, rent, det fick man ta en paus från sådana funktioner under ett till två år mer eller mindre. -(R2, Rad 28)

Samtliga respondenter berättade att deras respektive organisationer inte hade några svårigheter med att jobba hemifrån då de tekniska lösningarna redan fanns på plats, däremot svarade R2 att de har verksamhet som kräver fysiskt närvaro på kontoret, huvudsakligen var detta säkerhetsavdelningar. Inom dessa avdelningar gick man däremot ned till 10% av sin fulla styrka.

jag har ju säkerhetsteam som jag har som måste kunna sitta inlåsta när det är fysiskt säkerhet plus cybersäkerhet så att säga. Vi fick till, vissa av dem fick vi skriva speciella saker så att dem kunde jobba hemma och dem andra teamen fick gå ner på ett minimalt team så att man hade avstånd, väldigt stort avstånd. Så att en avdelning som kanske var 20 personer där satt 2. -(R2, Rad 16)

Det förekom att R3 tog sig till kontoret om man kände sig uttråkad eller hade ett möte som ansågs vara enklare att ta fysiskt. Den huvudsakliga men kortvariga problematiken med distansarbete R3 stötte på i början av pandemin var att deras licenser för sin VPN-tjänst inte var tillräckliga när man plötsligt skulle förse samtliga anställda med vars en licens. Däremot

kunde några anställda ha några uppstartsproblem som antingen inte haft möjlighet eller kunskapen om hur man skulle börja använda VPN-tjänsten organisationen fått på plats, vilket visar på att ett antal aldrig jobbat hemifrån före pandemin.

Som jag sa innan så förväntades man vara på kontoret och antalet som behövde använda VPN var ju kanske max en eller två, men när plötsligt alla skulle använda VPN-tjänsten så hade vi endast cirka 5 licenser för hela organisationen. -(R3, Rad 100)

R4 höll officiellt sitt kontor öppet under hela pandemin, men rekommenderade hemarbete vilket närmre samtliga anammade under åtminstone den tuffa perioden.

Vi höll kontoret öppet under hela pandemin, men däremot var det under perioden som samhället var som mest utsatt, då var vi mer eller mindre nedstängda även om vi faktiskt inte officiellt var det. Nästan alla jobbade konstant hemifrån under den perioden. -(R4, Rad 12)

R2 stötte också på samma problematik när det handlade om licenser för deras VPN-tjänst. Då medarbetarna plötsligt loggade in på molnet från alla möjliga platser så menar R2 att det kräver en ny syn på säkerhet och att man på längre sikt kan tvingas bygga om sitt interna nätverk.

det är ju klassiska grejer som licenser och sånt man har i tjänst som används av kanske 10% av personalstyrkan och så nu ska 100% av personalstyrkan använda den och då får man också titta på tekniken, jag menar om man har klassiskt VPN så kanske, vi gick ju upp mer och mer i molnet med utökningen så att att säga och det kräver ju en annan typ av säkerhet när hela arbetsstyrkan går ut, om några få jackar upp och connectar på daglig basis så är det väl, det kräver också att man kanske initialt måste bygga om det interna nätverket och sådana bitar också på sikt. Så det har varit, det var en tuff period, tror jag mest för nätverksteamen och så precis när vi switchade över att man hann inte med. -(R2, Rad 28)

Samtliga respondenter ser idag distansarbete som en självklarhet, jämfört med före pandemin då det var främmande att arbeta på distans, även om möjligheten fanns för alla. Man ser även kopplingen att en arbetsplats idag ska vara någon form av hybrid, där man kan träffas på kontoret någon/några dagar i veckan för att sedan arbetar på distans de andra dagarna. Anledningen till att våra respondenter vill åka in till kontoret är huvudsakligen av den sociala aspekten, att ha interaktioner med sina kollegor, och att möten som bör hållas på kontoret ses lite som en sekundär anledning och inte varför man vill arbeta på kontoret.

för min egna del så har jag väldigt svårt att tänka mig en, en arbetsplats där man inte tillåter hybridarbete. Man tappar ju mycket av den sociala interaktionen och att hänga med varandra och ha kreativa diskussioner och så. Därför är det skönt att kunna åka in till kontoret någon dag i veckan, eller två, och faktiskt träffas face-to-face och utbyta ideer och prata.-(R1, Rad 22)

R2 lägger även till att man ska se kontorsdagarna som dagar då man kompletterar sina kollegor med information och rådgivning. Man ska inte gå till kontoret för att alltid få göra sina egna uppgifter, utan att man snarare fokuserar på sina sociala interaktioner, detta både ur ett arbetsperspektiv, men även ur ett socialt perspektiv för att få prata med kollegor som inte har med arbetet att göra.

Och sen vissa som är viktiga för teamen, dem har man inte samma tillgång till som man har

fysiskt… så vi brukar säga att det blivit lite annorlunda nu när man kommit tillbaka för att vissa som är här inne, dem är så populära så dem hinner inte göra något arbete själva eftersom att det är ett sådant sug efter dem… så då brukar vi säga att när du är på kontoret så är du där för alla andra och sen om du måste göra något speciellt och riktigt liksom, så kan du, men det är jag godkänner, då kan du sätta dig hemma så du får komma ikapp med ditt eget så att säga. (R2, Rad 18)

R4 ser idag sin organisation som att några individer använder distansarbete lite mer flitigt då de funnit en bra balans vilket gjort att deras effektivitet ökat. Samtidigt ser R4 andra medarbetare som inte alls kan tänka sig arbeta hemifrån i ett post-Covid sammanhang.

Det är väldigt individuellt faktiskt, det är en spännande analys nu efteråt. Att vissa anammar detta och ser denna friheten som en fantastisk sak medans andra tycker detta varit rent smärtsamt. -(R4, Rad 22)

När det handlade om effektiviteten på arbetet var det entydigt att den sociala aspekten blev svårare att naturligt passa in under en arbetsdag, och att man fick boka in fikamöten då kalendern fylls på snabbt. Kreativiteten har varit en faktor som blivit svår att få fram naturligt, R1 styrker att det framstår enklare att utbyta idéer och föra kreativa diskussioner när man träffas fysisk. Nu försöker därför R1 och R3 med sina respektive arbetsgrupper boka in dagar då alla ska jobba på kontoret, och lämna hemma-dagarna till att utföra sina individuella och strukturerade uppgifter.

i vårt team, är att när vi träffas så försöker vi ha våra sociala aktiviteter som vi har i teamet, alltså de aktiviteter man alltid gör som ett team, typ gruppmöten och sådana saker, planerar vi in på en dag, så att allting sånt ligger under samma dag under veckan. Så att, för att det var väldigt många i teamet som uppskattar mer, alltså när man åker in till kontoret vill man träffa sina kollegor, man vill inte sitta i möten och jobba, för det kan man lika gärna göra hemifrån. -(R1, Rad 22)

R2 ansåg att hela känslan med hemarbete blev intensivt helt och hållet, även när man skulle ha ett fikamöte där man inte skulle prata jobb. Då man bokade in varje arbetstimme under dagen så hade man inte många minuter att andas och reflektera på vad som diskuterades på mötet.

initialt iallafall sen fick man ju sätta regler runt det, det var ju inget, man träffas inte normalt runt kaffet och har korridorssnack och så utan då blev det nästan att man bokade en 15 minuter, 30 minuter, och hade dem har korridorssnacken vilket gjorde att det blev väldigt, väldigt mötes intensivt i början. Så alla hade hela dagen i möte när de satt hemma och det var ju inte riktigt idéen. Så vi… jag införde att dem boka ut, vad ska man säga, man bokade ut tomrum i sin kalender för att jobba själv och implementera det. -(R2, Rad 22)

R3 nämnde att effektiviteten ökas eller sjunker med distansarbete beroende på vilken typ av tjänst man har. En tjänst där man inte är beroende av andra för att utföra sina arbetsuppgifter har rimligtvis en mer positiv inställning till att effektiviteten är högre vid distansarbete då man inte blir avbruten lika lätt på distans som på kontoret. Men tjänster likt R3 där man är högst beroende av andra kan effektiviteten sjunka då man inte har lika enkelt att komma i kontakt med någon.

Om man jobbar med programmering till exempel så tror jag att en lugnare miljö med mindre störande objekt kan vara med effektiv än en delad kontorsmiljö. Medans för min del där jag jobbar mycket med kontakt med mina kollegor så blir det inte mer effektivt. -(R3, Rad 23)

Detta enligt R4, som har en annan bild än R3, handlar inte om att vissa har olika arbetsuppgifter. Eftersom att en anställd på Know e generellt har liknande arbetsuppgifter då de flesta är utvecklare kände R4 att det var helt individuellt med de som arbetar bäst isolerade jämfört med de som arbetar bäst med andra.

Nej egentligen inte arbetsuppgifter. Det är väldigt likt här på så sätt, men däremot tror jag i hur man bedriver eller genomför sina arbetsuppgifter, vissa gör det ju helt isolerat med ett par hörlurar i öronen och andra gör det gärna genom att rådfråga och bolla idéer och sådär. Sistnämnda har då tyckt det varit mycket jobbigare att sitta hemma och de andra har tyckt det var döskönt att sitta hemma på en torsdag i sitt hemlandskap och köra på liksom. -(R4, Rad 24)

R3 beskriver även att man inte alltid vet under vilka tider sina kollegor och kunder arbetar då det kan bli lite mer flexibelt om man arbetar hemifrån, vilket skapar ytterligare trösklar för vissa arbetsuppgifter.

det är lättare att veta vem som jobbade när alla var på kontoret, medans man numera i och med att det är flexibelt att jobba hemifrån så blir också tiderna man jobbar mer flexibla så ibland vet man inte om de jobbar eller hämtar ungarna på skolan eller är hos tandläkaren osv. -(R3, Rad 26)

R1 som arbetar mer inom utveckling håller med om att effektiviteten för sig själv ökat, men att det fanns en inlärningsprocess att hitta en balans i hur länge man kan sitta under en dag för att lyckas bli utvilad och vara lika effektiv dagen därpå. Så även om effektiviteten ökade så gjorde det att svårigheten att stänga ner för dagen kunde bli svår, vilket R1 fick arbeta med under början av pandemin.

Så jag kan ju säga från början så hade inte jag, jag hade inte den strukturen jag behövde på mitt arbete för att vara, för att kunna koppla av från arbetet och så. Så det vart, det varit en väldigt konstig omställning för mig i början, det varit både, vissa dagar vart alldeles för produktiva, om man kan säga så, och andra dagar vart bara så, man vara bara så trött för att man hade suttit alldeles för länge dagen innan. Så det var, med tiden så vart det bättre, man fick upp lite bättre rutiner kring det. -(R1, Rad 24)

Ingen av våra respondenter har märkt av någon ökad säkerhetsrisk inom sina egna organisationer kopplat till pandemin och distansarbete, men de har märkt av att kommunikationen till och från klienter blivit allt vanligare ur ett säkerhetsperspektiv, dvs att förståelsen existerar på ett högre plan och att man är försiktigare.

kanske en extern utblick på vad jag har märkt från PwC kommunicerar ut till sina kunder. Att de kommunicerar ut att det är ju vanligare och det händer mer idag än vad det gjorde förut. -(R1, Rad 30)

Det potentiella hotet R2 kan se är frånvaron på kontoret när man inte lika enkelt kan fråga en kollega angående ett skumt mail där förövaren framstår vara en medarbetare. Att säkerhetshotet förändrats av anledning till pandemin är dock inget R2 märkt av.

det är sådana här fishing attacker blir väldigt, väldigt mycket mer lättare när du har mindre anknytning till arbetet, om du inte är på jobbet varje dag så kan jag skriva en jättefin Assa Abloy logga och fejkad mailadress och skicka till dig, absolut, eftersom att du… kanske lättare när du är på kontoret att fråga någon, är det här någonting som ni känner igen eller inte? Men det är mer av teoretisk art så att säga, det är inget vi har sett, vi har inte sett några trender, vi har inte sett några, vad ska man säga, större säkerhets skillnader mot normalt mot hemma under Corona-tiden. -(R2, Rad 42)

R2 styrker detta med sin erfarenhet av vilka svårigheter cybersäkerhet har idag, där det huvudsakligen handlar om slarvighet, var och hur man tillåter sin jobbmail användas i sitt privatliv till exempel.

Du behöver ju inte ha en dator för att logga in, räcker med användarnamnet och människor är människor så det är lätt, din mailadress följer med och kommer med på en föräldralista med fotbollslaget om du är slarvig och sen så har fotbollslaget inte jättestor säkerhet och det är lätt att tanka ner alla mailadresser och så vidare. Sådana här tjänster blir ju breachade rullande så det stora är väl mer att man är lite slarvig med sin företagsmail, det är väll en större risk ändå. Sen så, password idag… finns det väldigt sofistikerade att gissa, oftast när du knäcker en databas, om du loggar ju in i sådana här appar, fotbollsappar, alla möjliga privata appar eller restaurangappar eller någonting och oftast är människor människor så du har ju samma password där som du kanske har på jobbet eller liknande password du har där som du har på jobbet. Och sen så finns det ju stora, stora databaser med dem kanske 10000 mest vanliga passworden som man lägger på så det går ju kan man säga knäckandet mycket, mycket snabbare och då räcker det tyvärr idag med ett konto för att ta sig in och så. -(R2, Rad 32)

Samtliga respondenter styrker att medvetenheten hos den gemene anställda där förövare vill komma åt den anställdes uppgifter som lösenord är tydligt kartlagd. R3 minns endast ett tillfälle när en potentiell förövare uppgett sig att vara VD på Grade AB och skickat ut märkliga länkar till några anställda på organisationen.

i det fallet så kontaktade den drabbade personen VDn och frågade om det verkligen var han som skickade den länken till honom, och när det då inte var det så meddelade VDn via mail eller Teams att det kommit ett sånt mail och att man ska vara uppmärksam, men det är ju, som jag sa innan att det är svårt att vara förberedd på allt. -(R3, Rad 33)

Då man inte har någon uttalad ansvarig person för dessa händelser enligt R3 sköter man det istället internt mellan involverade parter. Det skulle möjligtvis finnas individer som arbetar med organisationens hårdvara som skulle kunna assistera vid behov, men vid detta specifika tillfälle löste man situationen internt.

man sköter det mellan varandra, det finns ju personer som jobbar mer med IT-miljön som datorer och våra servers som man kanske skulle kunna ta hjälp av, men det finns ingen uttalad som jobbar med den typen av arbete på vårt företag. -(R3, Rad 36)

4.2 Informationssäkerhet

Samtliga organisationer använder molntjänster, där de flesta större används som Google (Cloud), Amazon (AWS), Microsoft (Azure) och Alibaba (Cloud).

Ja men vi kör Microsoft rätt mycket så det är ju Azure för våran del. Vi har varit lite med Amazon osv men det är Azure huvudsakligen. Det gäller både eller egentligen alla typer av tjänster, men primärt är det virtuella servermiljöer egentligen. -(R4, Rad 41)

Hos R4 använder man sig även av serverhallar som är lokaliserade i Sverige, då de arbetar mycket med svenska sjukvården är det väldigt hög sekretess på att datan de arbetar med ska skötas rätt.

Vi jobbar ju mycket inom sjukvård osv. mycket och då är det höga krav på på avanalysering för GDPR men också patientsäkerhet just därför kör vi Sverigebaserade serverhallarna på de bitarna. -(R4, Rad 43)

Vidare är organisationen R3 arbetar för, mycket investerade i molntjänster för flera processer, och man förstår att det är en stor del i deras vardagliga arbetsgång då R3 enkelt kan berätta hur deras led ser ut när det gäller molntjänster.

Vi använder oss utav flera molntjänster, vi använder oss av till exempel Jira, det är ett ärendehanteringssystem, och de ägs av Atlassian, och där använder vi även Confluence som är ett intranätsystem. Sen använder vi oss av Trello som också ägs av Atlassian, det är en sån här board där man kan flytta lappar mellan olika kolumner. Vi använder Zendesk för ärendehantering, det är ju en molntjänst. Office 365, Microsoft, Teams för kommunikation. -(R3, Rad 39)

Likt R4 har även R3 och sin organisation lokalt baserade serverhallar som har hand om den huvudsakliga datan.

Ja det är också en typ av molntjänst, det är ett företag i Malmö som har våra servers i en serverhall. -(R3, Rad 41)

Från respondenternas vetande har ingen av deras data blivit utsatt för intrång genom att förövare kommit åt något via deras molntjänster, däremot berättade R2 att de haft kunder som råkat ut för dataintrång via sin leverantör av molntjänst.

men vi ser att en del av våra kunder har blivit träffade så att säga men vi har ju, ja, vi har ju väldigt stor kundbas så att säga. Så det har vi ju sett, allt från ransomware till credential steal så att säga -(R2, Rad 46)

R1 har inte någon direkt information från sin molntjänstleverantör om hur man skulle kommunicera ut vid fall av dataintrång hos sin leverantör, men är ganska säker på att detta skulle ske snabbt och smidigt.

Vet inte riktigt hur det där fungerar när Google blir utsatta för någonting. Men jag antar att det borde bli ganska, kommunicerat ganska fort med tanke på att då blir ju hela PwC utsatta i och med att det inte är bara sverige som är med utan det är ju hela nätverket. -(R1, Rad 38)

Beroende på vilken titel man har inom organisation som R2 arbetar för, så har man också ett större ansvar för distribuering/tillgänglighet av data. R2 har till exempel möjlighet till mer data än någon annan i arbetsgruppen som respondenten tillhör, men då R2 även finns på LinkedIn och andra sociala medier tillhör respondenten en högriskgrupp som förövare vill komma åt.

Jag vill också inte oftast ha allt på min access som chef för att jag står på LinkedIn som ansvarig för Cybersäkerhet på Assa Abloy -(R2, Rad 106)

Även de andra tre respondenterna arbetar på liknande sätt där inte alla har tillgång till samtlig data, utan man har tillgång till det man faktiskt behöver för att utföra sina arbetsuppgifter, vilket huvudsakligen är för att skydda organisationen, kunderna och dess data. Däremot kan det se annorlunda ut om man väl jobbar i ett projekt, då kan samtliga i projektet ha tillgång till samtliga system för att kunna arbeta på bästa sätt, men enligt R1 skiljer det sig från projekt till projekt. R1 berättar även att det fungerar fysiskt genom att vissa har åtkomst till vissa delar av kontoret som de flesta anställda inte har någon tillgång till.

Då man måste rapportera dataintrång till EU-kommissionen inom 72h har R2 satt upp flera sätt som en medarbetare ska kunna komma i kontakt med deras avdelning om de misstänker något. Detta är till exempel deras intranät eller andra supportsystem, och den är avsedd för att kontakta om man ens är lite misstänksam om att något som skett. Detta gör man genom att skapa en bra miljö där medarbetarna känner att de kan höra av sig även om det inte skulle visa sig vara något denna gången. R2 har en filosofi att det hellre ska kontaktas en gång för mycket än en gång för lite, då det kan vara förödande om ingen kontakt skulle ske.

Och det är okej bara om man misstänker att kontakta oss om man inte, det är väldigt viktigt att bygga en coachande miljö så att även om du inte har något som absolut, som du inte förstått, som absolut inte, att man inte klankar ner på det utan att man är coachande för det är ju de anställda som är första indikatorn och det är viktigt att dem är med på banan i alla led. Som sagt det går så snabbt idag, speciellt om du möter nationer, det går väldig, väldigt snabbt -(R2, Rad 54)

Då samtliga organisationer arbetar med VPN-tjänster för att komma åt sina system är det samtidigt det enda preventiva medlet som kopplar samman företagen. R3 arbetar i den enda organisationen som vi intervjuat där lösenordshanterare används på en organisationell nivå.

Lösenordshanterare ja, där alla konton för att komma åt lösenord man behöver ha tillgång till. -(R3, Rad 49)

R4 arbetar mer på sättet där man tar det som de kommer, då de är ett snabbt växande företag är det svårt att hinna lägga resurser på allt, och därför kan de idag förlita sig på sina brandväggar och VPN-tjänster som anses hålla en tillräckligt hög säkerhet.

Nej men alltså vi har ju brandväggar och alla dessa bitarna då, men inte något mer avancerat. Utan då är det VPN. -(R4, Rad 51)

R2 berättar att de tillåter extern hårdvara, men att allt som kopplas till hårdvara som Assa Abloy äger är samtidigt övervakat vilket gör att det är väldigt sofistikerat och de kan snabbt agera om något verkar fel.

Vi övervakar allting som stoppas in i datorerna via USB, så det är okej att ha ett USB-minne utan vi har full koll när det sticks in. Det är ju så ibland att… dem är smittade, antingen från företaget det kommer ifrån och så men det ser vi ju och hanterar och då isolerar den datorn inom någon sekund så att det inte sprider sig. -(R2, Rad 56)

R2 anser att det inte nödvändigtvis är en säkerhetsfråga när det gäller att stoppa okända USB-minnen i en dator då deras anställda kan behöva använda kunders enheter ibland, och att man hade fått fler negativa resultat än positiva.

vad har vi… snart 55000 anställda, där är alltid någon som har en smutsig USB-sticka i världen eller, det är inte så att dem har det själva utan dem får ju från leverantörer, dem ska byta ritningar och allting, men oftast kommer inte stora grejer in där utan oftast stora grejer måste det sitta en fysiskt person bakom och hacka. Sen kan du ju få en, vad ska man säga, en väg in med ett script som ligger på en USB-sticka. Idag med den säkerhet som finns så är det väldigt, väldigt svårt, det är coolt i filmer och så men, det går absolut, du vet den här klassiska man går och kastar ut en massa USB-stickor utanför företaget, sen tar dem upp det och hittar, en blänkande fin USB-sticka och stoppar in den i datorn, det finns attacker som gått till så absolut, det är klassiskt -(R2, Rad 62)

Vidare arbetar inte heller Grade (R3) med blockering av hårdvara, men att hårdvaran anställda använder kommer från samma leverantör som de har till sina serverhallar.

Vi beställer ju våra datorer från samma ställen där vi har servrarna -(R3, Rad 51)

R2 använder ett automatiserat system som byter lösenord varje timme för deras centrala system, vilket de gör för att även om någon kommer åt dessa lösenord kommer de inte fungera en liten stund senare.

Men vi har, vad ska man säga, vi har, vi bygger permlösningar som är centrala password-lösningar och det är egentligen på kontot, så kontona byter password varje timme och roterar själv passworden, speciellt när du har systemkonton och så. Så även om du kommer över ett password på ett systemkonto så, en timme senare så är det passwordet, kan du kasta det typ, för att det roterar hela tiden. Så vi försöker att bygga sådana lösningar, speciellt på då, vad ska man säga, system till system kommunikation. -(R2, Rad 56)

Denna lösningen tog man fram huvudsakligen för att en anställd inte kan hålla reda på alla olika lösenord till de olika systemen man använder. Det R2 är rädd för, är om anställda skulle ha koll på samtliga lösenord så kan det enkelt bli en ond spiral genom att dessa skrivs ned på lappar och annat som i sin tur enkelt kan bli konfiskerade av parter som inte bör komma åt dem.

du har oftast ett standard användarkonto och sen om du har någon sorts adminrättigheter så att du har ett admin konto så separerar man accessen på då. Så jag menar om jag äger mitt användarkonto som jag använder varje dag så äger du inte ditt adminkonto så att man bygger, vad ska man säga, en tierad modell av olika konto. Sen finns det servicekonto då som är system till system, ska du då som applikationsägare ha koll på dem passworden till dina system så är det oftast 20-30 konton per system, och vad gör en människa då, jo dem skriver ju ner dem någonstans eller hur? -(R2, Rad 58)

R2 tror att med Windows 11 kommer man se ytterligare säkerhetsåtgärder som blir ännu mer

sofistikerade genom att ens pin-kod lagras lokalt.

det finns ju nya tekniker här med Windows 11 och så, att istället för att ha password så har du pin-kod istället och det sparas, allting sitter lokalt så den pinkoden är ju bara din, vi kanske inte ska det här i denna, hur det funkar men det är väldigt, väldigt säkert för att då kommer du ifrån password, lite på användarnivå. -(R2, Rad 60)

R1 hänvisar till de utbildningar som organisationen tillhandager och beskriver hur denna anpassas efter vad som anses relevant varje år.

Så att det pågår alltid kontinuerlig träning utav alla medarbetare hela tiden och sen så finns det alltid en, en återkommande kurs varje år där vi går igenom saker som har förändrats, saker som är nytt, saker man behöver tänka på. -(R1, R46).

R1 beskriver vidare vilket högt fokus som läggs på just utbildningar inom säkerhet.

det läggs ner väldigt mycket tid, tanke, research och efterforskning på dem, att dem är anpassade till situationen vi befinner oss i idag. -(R1, Rad 54).

Vidare beskrivs även hur välanpassade dessa utbildningarna är, där informationen är tänkt att utbilda människor inom alla kunskapsnivåer ända ner till någon som inte alls är datorvan. R1 talar om att när utbildningen hölls vid senaste tillfälle fick de ta del av material för att kunna skapa en segregerad nätverksmiljö hemma då fokuset nu låg på distansarbete och IT-Säkerheten kring denna.

Jag har ju aldrig varit på ett ställe där man börjar prata om segregering utav nätverk hemma till exempel, för typ gemensamma personer och typ hur man kan gå tillväga för att hindra saker, så det var, det är väldigt intressant. Dem lägger, det läggs väldigt mycket tid på det och det tillhandahålls material också så att gemene man skulle kunna uppnå en segregerad nätverksmiljö hemma även om man aldrig har gjort det förut så det är lite häftigt. -(R1, Rad 54)

R2 arbetar likt där man ger kontinuerliga utbildningar men också tester runt om i organisationen för att se om sina anställda agerar på det tänkta sättet, eller om man istället bör hjälpa de förstå innebörden med dessa tester och hur de istället bör agerat. R2 anser det vara väsentligt att samtidigt hålla anställda ansvariga så bör man även förstå att cybersäkerhet inte är deras starka sida ofta, och därför ska de känna att R2 med sin avdelning finns bakom en med en hjälpande hand.

det använder man mer för att försöka testa användarnas utbildning, man trycker på användaren ganska mycket för cyberutbildning idag, allt från phishingattacker till, ja som ni sa innan med GDPR och nu kommer också Schrems 2 här från EU. Så idag får, vad ska man säga, IT användare väldigt, väldigt mycket utbildning. Sen så gör vi också fejkade phishingattacker internt, så vi skickar ut en phishingmail och sen ser vi vem som klickar på dessa och när dem då klickar på dessa och åker fast så att säga, så är där en länk till en utbildning och sen så flaggas den upp och så får dem ta phishingutbildningen en gång till. Man försöker att inte sätta dit dem, man försöker bara testa dem och coacha dem, det är viktigt -(R2, Rad 62)

R1 menar även på att det finns hjälp inom organisationen för den gemene personen som behöver hjälp att säkerställa sin IT-säkerhet i hemmet, så det inte är inriktat till insatta IT-individer.

Ja och det finns, det finns supporterande material kring det också. Så efter den sektionen är färdig så finns det, ja men om man inte vet hur man gör så kan man höra av sig hit så kan man få hjälp mer. Så att, väldigt, väldigt bra. -(R1, Rad 56)

Om man jobbar mer exponerat och externt behöver man samtidigt lägga mer tid på utbildning inom IT-säkerhet, men också att den utbildningen anpassas för den anställdes tjänst så just den ska få bästa möjliga förutsättningar säger R1 då vissa exponeras mer än andra i hans organisation.

dem får nog kompletterande utbildningar just när man sitter och kanske har extern kontakt väldigt mycket mer kanske just när man sitter i en servicedesk där man kan bli uppringd både extern och internt. Som intern personal finns det kanske bara vissa exponeringsytor man har och det är väl dem man blir tränad i. -(R1, Rad 74)

R2 talar om hur Assa Abloy senaste åren implementerat ett nytt HR-system som ska ta hand om samtlig utbildning, så allt finns samlat på ett och samma ställe. Där det positiva ligger i att chefer kan följa vilka utbildningar sina medarbetare tagit. Utbildningarna man går behöver man göra om 3 år senare då man ansett att omvärlden förändrats tillräckligt mycket och då utbildningarna gjorts om för att svara på förändringarna som skett.

Men det funkar i stort sett såhär, om du klarar en phishingutbilning eller vi har, alltså utbilning runt vad är en muta, vad är inte en muta, sådana grejer, klarar du då de utbildningarna så är du clearad för 3 år, sen efter nästa 3 år så får du en uppdaterad version av den utbildningen. Och dem är rätt så sofistikerade för att du svarar först på frågor, så när du svarar fel på en fråga, då läggs det utbildningskapitlet till som du svarade fel på, så det är rätt skönt om du skall ta om någonting att du kan svara på några enkla frågor så slipper du sitta en timme och köra utbildningen eller två, så det är rätt trevliga saker. -(R2, rad 66)

Beroende på vilken avdelning en anställd arbetar på har man olika nivåer av utbildningar på ett område man ska gå. En revisor ska inte nödvändigtvis gå en ingående kurs i hur man ska utveckla en brandvägg genom att följa en ISO-standard.

man vill ju hela tiden ge användarna mer men man får vara försiktig så att dem inte sitter i bara utbildningar och kan jobba också lite. Sen så Cyber Security avdelningen har ju dessutom ytterligare utbildningar som vi kör, vi har ju utbildningsprogram där, för att idag gäller det ju att vara ajour hela tiden. -(R2, Rad 68)

Då R3 jobbar i en mindre organisation än R1 & R2 har de inte samma resurser inom utbildning. Däremot har de dokument om de flesta relevanta utbildningarna, bland annat IT-säkerhet. De har onlineutbildningar, som uppmanar anställda att ta del av dessa dokument och man ska försöka uppdatera sig i dokumenten en gång per år.

Så som vi uppmanas att ta del av dokumenten är via en online-utbildning eller flera onlineutbildningar. Och via den så får man först ladda ner dokumentet, och efter det får man tre till fyra frågor som baseras på vad som står i dokumentet. -(R3, Rad 59)

Tanken är att man ska göra detta varje år, så man får ett certifikat som gäller ett år, sen vid

nästa medarbetarsamtal så ska man helst ha gått utbildningen igen. -(R3, Rad 63)

R4 har i dagsläget inte någon form av utbildningar inom IT-säkerhet. Det är samtidigt ett aktivt beslut men även av anledning att tiden och resurserna inte räcker till, däremot öppnar R4 för att ha något likt seminarium eller annat för att bli uppdaterade med dagens IT-säkerhet. Då anställda på Know e har gått IT-utbildningar har de hittills kunnat leva på förkunskaperna som getts under deras utbildningar. Som tidigare så känner R4 att sålänge allt flyter på bra behöver inte heller utbildning inom IT-säkerhet tidigareläggas på prioriteringslistan.

Ja om någon skulle ringt mig och sagt att vi skulle behöva ha en endagsseminarium på den så handlar det väl mer om praktikaliteten om när vi ska få till det då alla är upptagna men det är klart att det är av intresse att lyssna till. Men då får man se vad det är för område också, för oss är ju säkerhet egentligen hur kan vi säkerställa att vi, eller att alla sitter på en lagom hög nivå att inte klicka på mail liksom med bilagor i onödan. -(R4, Rad 82)

R3 har en intressant tes angående att anställda och individer generellt blir mer och mer uppmärksamma och tar åt sig hur en förövare kan tänkas agera för att komma åt något de inte ska.

men jag vet inte om motivationen till det är just hemarbete eller om det är omvärldsläget som förändrats senaste åren. Som jag sa tidigare så tror jag att kunskapen om vad det finns för olika hot har ökat för alla människor. -(R3, Rad 66)

R3 avslutar med att utbildningar förmodligen är mer kritiska om man har känslig data som förövare vill komma åt. Då Grade inte hanterar mer känslig data än exempelvis kunder mail finns det inte heller ett ökat tryck för att deras organisation ska bli mer påverkat än andra.

Jag tror det beror mycket på vad man har för typ av arbete också, och liknande branscher som den jag jobbar i eller andra mjukvaruföretag så kan den mjukvaran vara mycket mer känslig än vår är. En utvecklare i vårt företag sitter ofta inte med kunders känsliga data, det är möjligtvis deras mailadresser och liknande. Medans andra företag kan ha väldigt mycket känsligare data. (R3, Rad 69)

De två större organisationerna följer ISO-standarder när det handlar om IT-säkerhet. R1 berättar att deras interna säkerhetsavdelning mäter individer, grupper och IT-lösningar som utvecklas.

Ja, och vi blir ganska hårt mätta utav våran interna säkerhetsavdelning att vi uppnår dem olika standarderna som finns, det är därför vi har hela den hära… en granskningsprocess för alla applikationer till exempel när dem blir väldigt rigoröst granskade och ser också till att alla standarder som behöver uppnås, uppnås beroende på vilken typ av applikation det är och vilken data som finns i den. -(R1, Rad 68)

Detta löser R1 genom att få specifika mål med hur man ska gå tillväga för att följa ISO-standarder, inte för att man får på papper vilka man brutit mot, utan den interna säkerhetsavdelningen analyserar och kommer med direkta alternativ på hur man kan göra för att arbeta på rätt sätt ur ett ISO-perspektiv.

man får det inte som, den här har du brutit mot och den här har du gjort fel utan det är mer som det är det här som vi behöver rätta till, så man får mer ett mål om vart man behöver va,

inte vad man har gjort fel och enligt vilken paragraf man gjort fel. -(R1, Rad 70)

R2 följer ISO-standarder som ISO-9000 och ISO-27000 men menar på att ISO-standarder inte nödvändigtvis är något man enbart talar om när det gäller IT-säkerhet.

Det ligger ju närmare businessen, det ligger ju närmare kan man säga, fabrik och businessen så jag menar, ISO-9000, ISO-27000 och alla dem bitarna absolut finns det. Sen så, oftast så har vi inte direktförsäljning till kunder, vi säljer ju till kunder som sen säljer våra produkter men vi har säkert PCI DSS standarden någonstans och så vidare. Sen finns det rena, det är ju inte standarder på så sätt, men det finns SOC 2 regelverket som vi försöker att följa och andra, men det är mer kan man säga av kvalitetsskäl, så att vi säkerställer att vi fyllt i alla, vi har bockat alla rutor och sådana bitar. -(R2, Rad 64)

Den stora standarden R2 jobbar med nu är GDPR som R2 anser vara en djupare koppling till IT-säkerhet.

GDPR är stort, data protection, skydda våra användare så att vi följer lagar och sådana grejer för att vi samlar ju, jag ser ju allt som händer i bolaget rent krasst, för vi samlar in all den datan, idag kan du ju spåra allt en användare gör och därför är det viktigt att följa de lagarna och skydda våra användare också. -(R2, Rad 64)

4.3 Teorier inom IT-Säkerhet och informationssäkerhet

Ur utgångspunkten och teorin TTAT visar samtliga respondenter att deras organisationer och anställda har en bra bild av informationssäkerhet och att man arbetar med det som en självklarhet. Detta kan bero på att våra respondenter är insatta inom IT och har lång erfarenhet inom området.

R1 känner att både i sig själv och sina kollegor konstant har ett fokus ur ett säkerhetsperspektiv och att man inom PwC är mogna. När vi frågade om R2 känner att utbildningarna gör någon skillnad i tillvägagångssättet gällande just IT-säkerhet svarar R2 följande.

Absolut, och inte bara kanske när jag tänker och reflekterar själv utan kanske när jag jämför med kollegor som också jobbar i samma bransch… det är en väldig skillnad på fokus så absolut. -(R1, Rad 80)

R2 mäter kontinuerligt beteendet hos sina anställda med attrapper som ska likna en phishingattack, och märker tydliga skillnader på de som gått utbildningarna som ges gentemot anställda som inte ännu gått utbildningarna.

Absolut, absolut, vi mäter ju phishing eftersom att vi skickar ut fejkade phishing, vi mäter alla divisioner individuellt och de som har utbildat och promotat dem har ju mycket, mycket bättre resultat än övriga, så det är ganska tydligt vem som har gjort ett gott jobb och vem som gjort ett mindre gott jobb på dem bitarna, så det syns -(R2, Rad 96)

Av hur R3 känner är de flesta medarbetarna medvetna och kunniga tack vare deras tjänster inom IT, som mjukvaruutvecklare. De har även sin andra halva av organisationen som inte är kopplat till IT som R3 däremot inte tror är lika medvetna, men kanske att behovet inte är lika stort på den delen av verksamheten.

I och med att hälften är mjukvaruutvecklare är hälften väldigt informerade och andra hälften kanske begränsat informerade. Så om man kan svara lite både och på det? -(R3, Rad 72)

R4 arbetar i sin organisation likt IT-avdelningen på organisationen R3 är anställd på.

Ja men det här är ju en ständig frågeställning, så jag skulle vilja säga att den är tillräckligt god för att vi ska känna oss trygga i det. -(R4, Rad 57)

Däremot känner inte R1 att skillnaden är kopplad till ökat distansarbete, även om man under de senaste åren arbetat mer med säkerhet.

om det är kopplat till just att jobba hemifrån eller inte eller om det är en ren slump, det kan vara en annan sak. -(R1, Rad 82)

Kopplingen till distansarbete var tydligare till en början av pandemin för R2 då man var i en form av testperiod när inte någon hade en klar bild av hur man skulle arbeta enligt bästa praxis.

Initialt var det ju det, eftersom att många var ovana vid att jobba hemma och sen så hade vi problem initialt eftersom att det gick över en dag, över en vecka från att jobba till att vara hemma, så initialt kom det säkert en massa felkoder och sådana grejer för vissa användare som dem trodde att, du vet. Men förutom inkörningproblemen där i början som var relativt smidiga med den här storleken på företaget, så nä det kan jag inte säga att det har varit något -(R2, Rad 98)

Grade hade ett seminarium för sin utvecklingsavdelning i början av pandemin kopplat till distansarbete om några praxis som kan vara bra att tänka på och använda till sitt dagliga arbete.

Vi gick igenom innan pandemin inom utvecklingsavdelningen att alla också alltid skulle låsa sin dator innan man gick därifrån och för min del fick man mer rutin på det då och att det hänger med en hem. -(R3, Rad 79)

R4 har inte känt något ökat tryck att behöva utöka sin nuvarande datapolicy när det handlar om distansarbetet. Då man på Know e får använda sina jobbdatorer till annat än jobb kan det bli polariserat om hur säker man är om man vid ena stunden sitter med jobbrelaterade uppgifter gentemot när man sitter med nöjesinriktade ändamål.

Det är ju så att vi har haft en datapolicy, de flesta sitter på gamingutrustning yrkesmässigt också. Så liksom hybriden mellan när det är en arbetsstation och när det är en nöjesstation är inte helt klar. Och det har varit ett medvetet val från våran sida, så att vi har ju valt att separera näten, vi har liksom inte… man skulle egentligen kunna sätta upp ett snöre mellan våra kontorsnät och våra miljöer osv men vi har ju valt att smäller en dator eller liknande ska inte det heller påverka någonting annat egentligen. Så det vore synd att säga att vi har den typen av styrning, nej. -(R4, Rad 59)

Angående *Confidentiality* arbetar samtliga organisationer med behörighetskrav, detta genom att varje medarbetare inte har tillgång till system som inte behövs för att utföra sina arbetsuppgifter. R1 berättar att inte bara gör detta ur ett inom deras system, men att de även arbetar med behörighet på fysiska lokaler inom organisationen.

På just IT sidan så absolut och i system absolut, alla har inte rättighet att se allting. Sen så finns det ju också även uppdelning på… inne på kontorsbyggnaden också där vissa områden har en helt annan… alla kommer helt enkelt inte in där. -(R1, Rad 84)

R2 förklarar att de klassificerar sin data enligt en skala som kartläggs om medarbetare behöver ha tillgång eller inte.

vi klassificerar data enligt, vad ska man säga, en skala, så alla dokumenten och allting blir klassificerade. Sen har vi ju rena röda nätverk som vi säger, röda nätverk är ju att dem har ingen access in eller ut utan dem finns bara -(R2, Rad 100)

De röda nätverken R2 berättar om fungerar på så sätt att ingen kommer åt dem på något sätt förutom med direkt tillgång på plats för att styrka säkerheten.

Ingen alls, utan det nätverket finns bara på den siten, den har ingen internetaccess, ingenting, och de jobbar ju där. Sen är det ju, vad ska man säga, sen har vi ju, det är också vilken chef du är, vilken information du får tillgång till och så vidare. Så vi har många olika sätt vi skyddar känslig information -(R2, Rad 102)

När det kommer till hur R2 ska bestämma vem som ska ha rättigheter till specifika system är man relativt öppen och att utvecklarna åtminstone, har mycket att säga till om gällande olika arbetssätt utifrån deras erfarenheter beroende på projekt.

Ja, vad ska man säga, vi har våra utvecklarteam, de jobbar med en produkt så dem kanske inte är samma linje, men där finns ett produkt IT-Council som driver Cybersäkerhetsarbete också och informationssäkerhet. Men utvecklare är ju glada att göra det på sitt sätt [skratt] … det är därför man vill ha dem också, det är tyvärr så att min vill ha dem för att dem är dem, så kommer dem och, nä ni ska köra Windows nu annars så eldar dem upp huset typ och så vill dem köra sin Linux version, nä vi ska inte köra Ubuntu vi ska köra Mint och vi ska köra, du vet. Men det är härligt också, de är ju oftast hjärnorna så man får vara snälla mot dem -(R2, Rad 104)

R3 och R4 arbetar på liknande sätt där utvecklare i ett projekt har tillgång till samtlig data då de anses behöva allt tillgängligt för att kunna utföra sitt arbete fullständigt och korrekt.

I den mån vi gör det så gör vi det med kunder servers, databaser. Där har de utvecklare åtkomst fullständigt. Jag kommer inte åt detta då jag inte har de lösenorden. Varje utvecklare har individuella konton som man kommer åt servrarna så det inte finns något gemensamt konto. -(R3, Rad 82)

R4 som arbetar med mycket inom sjukvården behöver även bevisa deras möjligheter för sekretess, och utvecklare behöver godkännas av en myndighet för att få arbeta i ett projekt som har med vården att göra.

Vi har kolossalt mycket sekretessavtal som är personlighetsbundna och inte bara på företagsnivå utan så är det ju. -(R4. Rad 63)

R4 fortsätter förklara hur det fungerar med myndighetskontroller.

Vi sätter ofta ihop teams som jobbar med specifika klienter, och då genomgår de ju allt från poliskontroller tänkte jag säga, men myndighetskontroller till sekretessavtal osv. -(R4, Rad 65)

När det handlar om *Integrity* av den data som organisationerna har tillgång till, berättar R1 att den tas hand om på olika sätt från projekt till projekt, och att de inte nödvändigtvis har en satt policy om hur man arbetar generellt med integriteten.

Jag skulle säga, det gör det, men hur vet jag inte eftersom att det är lite mer utav en verksamhetsfråga kopplat till kanske uppdragen och hur det ser ut. -(R4, Rad 88)

R2 arbetar genom att beroende på vilken tjänst man har gör det också att du har mer tillgång till känslig information då man bygger ett högre förtroende med sin roll/tjänst till en gräns. Detta ska inte ses som att en chef har högst förtroende, det är snarare tjänster som kan tänkas behöva känslig data eller dylikt för att bättre kunna utföra ett arbete.

nä det har inte med linjeägande att göra utan det har med rollen i sig själv. Så till exempel, jag kan vara chef över Cybersäkerheten men jag kan kanske inte ha access till all data. -(R2, Rad 106)

Men det är rollen som avgör vilken access du har till vilken data och känslig information -(R2, Rad 108)

R3 löser frågan om *Integrity* genom att kryptera data man anser vara känslig nog.

Den datan som bedöms vara känslig i våra system är krypterad. Så att vi inte kan läsa utan att göra ett mindre intrång vilket isåfall skulle loggas om vi skulle få för oss att göra något sådant. Så datan är krypterad med en nyckel. -(R3. Rad 79)

R4 tror att deras bild av *Confidentiality & Integrity* inte förändrats till följd av GDPR tack vare att de alltid varit väldigt sekretessbelagda från sina kunder.

Märkligt nog har vi nog alltid haft en väldigt sund bild på det så vi har nog aldrig byggt lösningar som har varit på ett sånt sätt och man ska inte heller glömma det att GDPR är väldigt inriktat på där bolag med många datakällor använder för korsbefruktningar av användning av data för andra skäl än det de ämnas för. Det är för att skydda individen där, och där har vi inte varit, så vi är ganska förskonade av det. -(R4. Rad 79)

R4 styrker på hur R3 arbetar med *Integrity*, men att det förekommer att man delar sina konton då de är en relativt liten arbetsgrupp, samtidigt som man utsätter sig för fara om sin kollega skulle använda det utlånade kontot till något man inte bör.

Nänä men vi har ju, såklart om jag lånar ut mina konton till någon annan så utsätter jag mig för fara om någon annan gör något dumt så att säga, men det är ju personlighetsstyrt. -(R4, Rad 71)

R1 känner inte att *Availability* nödvändigtvis blir lägre för att man arbetar i en säker miljö, utan om man arbetar på rätt sätt når man också någon form av smidighet.

man kan uppnå smidighet i att ha en väldigt säker miljö också. -(R1. Rad 93)

R2 ser *Availability* på olika nivåer, att beroende på vilken klassificering kan det också vara en tuffare tillgänglighet, man att det är så man bör arbeta.

Ja men då får man ju tänka vilket system det är, vi klassificerar ju olika system med olika klassificeringar, vi har något som vi kallar kronjuveler, crown jewels, det är dem viktigaste applikationerna för varje division och då definierar dem det, kan vara interna affärssystem, det kan vara produkter. Så man börjar att jobba så och sen så skyddar man, säkerställer man att där finns ett skydd som är till klassen av, jag menar skulle det här bli infekterat det här, så stannar alla våra fabriker till exempel. Det är kanske inte hela världen men att starta upp alla fabriker igen så kan det kosta x-antal 100 miljoner så det är det som är problematiken och då gör man en riskbedömning efter systemet. Något som vi har som mål är att om alla de här systemen då, som är crown jewels då, alltså vi har ju flera, flera tusen applikation, men dem som kritiska för vårt levebröd så att säga, då har vi ett mål att om dem blir träffade av någonting, av någon anledning, att dem ska vara uppe och rulla inom 24 timmar och det kräver ju då att man har till exempel om vi utgår från säkerhets perspektivet, det kräver ju då att man har sin backup offline. Så att om en hackare kommer in att dem inte kan vara där i 6 månader och komma in i backupen så att sen när du lägger tillbaka backupen så lägger du tillbaka hackaren också. Så vi massa olika sådana saker där runt om systemen. AD är ju ett klassiskt sånt här där alla rättigheter finns, då har man en offline backup av AD. -(R2, Rad 112)

R3 har inte fått känslan av att *Availability* har förändrats sedan starten av pandemin, mer än precis vid starten då man hade en upplärningstid.

Vissa har haft lite problem med att få fel på sin VPN klienten men det har också löst sig ganska snabbt. Ett problem vi hade precis i början var att vi hade för lite licenser till VPN-klienten -(R3, Rad 100)

R4 arbetar med mockad data under sin testmiljö, men att *Availability* blir desto mer specifik när man går över till QA/produktion.

Vi jobbar ju alltså med utvecklingsmiljöer och då är det mockat data och där arbetar vi med en mycket mer kompakt miljö, men när man direkt går över till QA eller produktion så är det helt separerat. -(R4, Rad 75)

R2 tror att pandemin hjälpt *Confidentiality, Integrity & Availability* på ett sätt där man lagt mer fokus att få rätt på sin data och sina rutiner.

Jag tror att det har hjälpt att Covid-19 hände för att det har gått snabbare och man har, vad ska man säga, exekverat snabbare för att det har varit mer fokus på det. Sen tror jag inte det har skilt sig något nämnvärt i vad man har gjort i jämfört, det känns bara som att det har gått snabbare, en känsla bara, det är svårt att mäta men det känn som om det har fått fokus och i med Covid-19 så stannade världen upp och tänkte på lite säkerhet i två år. Jag tror att det är mer att, vad ska man säga, världen förändrades och det kom upp på agendan högt uppe, vilket gjorde att det fick mer mandat och drogs igenom snabbare, sådana här projekt -(R2, Rad 118)

5 Diskussion

Under detta kapitel kommer empirin diskuteras i korrelation med den litteratur som presenterats under Litteraturgenomgången. Strukturen följer fortsatt den som gjorts under Litteratursammanfattningen där de tre huvudkategorierna: Distansarbete, Informationssäkerhet och Teorier inom IT-säkerhet och informationssäkerhet kommer att diskuteras med deras diverse underkategorier.

5.1 Distansarbete

5.1.1 Distansarbete före Covid-19

Av att bedöma från våra respondenter har man kunnat arbeta på distans även innan pandemin, men kulturen på samtliga organisationer vi fått en insyn på har inte utnyttjat denna resurs. Några av våra respondenter talar om att kulturen varit så, och även de som inte rakt ut uttalar sig om kulturen är det en klar bild om att man helt enkelt inte arbetade på distans om man mot förmodan inte haft en grundlig anledning.

De fyra nyckelkompetenserna som handlar om beteenderiktlinjer, tillit, koordinering av information och media verkade inte vara fastställda på någon av organisationerna ur synpunkten från innan pandemin (Makarius & Larson, 2017). Av att bedöma från våra respondenter är det inte riktigt några av dessa kriterier som man uppfyllt innan det påtvingade hemarbete uppstod. R1 berättade att de har revisorer som var runt och arbetade lite överallt och därför använde sig av distansarbete, men hur detta fungerade i praktiken var R1 inte säker på. Därför kan man tänka sig att tilliten åtminstone var kartlagd på organisationen R1 arbetar på sen tidigare, de andra organisationerna kan vi inte bedöma från informationen vi tillhandahållit. Användningen av media kan från intervjuerna varit den del som är avgörande då kulturen var att befinna sig på kontoret, och kan därmed resultera i att en kollega på distans blir uteslutande från arbetsgruppen om man ifrågasätter företagskulturen. Även om det skulle vara accepterat finns risken att man blir desto mer egenarbetande då man ensam i en större arbetsgrupp har svårare att framföra sina tankar och idéer, att jämföra med om alla sitter bredvid varandra på kontoret eller i ett digitalt möte. Detta kan även bli en utmaning i framtiden när man anställer, då några kommer vilja jobba på distans och andra inte, och kunna hitta en bra lösning där alla också ska kunna framföra sin expertis. Frågan blir i slutändan vem som kommer behöva anpassa sig efter vem, antingen anställda på kontoret eller de som finns på distans, eller om man i varje arbetsgrupp på alla organisationer kommer överens om att vissa dagar i veckan är avsatta för kontoret vilket låter osannolikt.

5.1.2 Distansarbete under Covid-19

Då våra respondenter sedan tidigare använt sig av molntjänster och VPN-tjänster hade de ganska enkelt att på samma dag gå från kontoret till hemmet. R2 & R3 hade kortvariga problem då de inte hade tillgång till licenser, men det kunde man lösa snabbt. Svårigheterna för organisationer att plötsligt bestämma sig för att samtliga anställda plötsligt ska arbeta hemifrån utan att egentligen veta vad det ska leda till var en svår tröskel (Richter, 2020). Detta kommer att betyda då organisationer behöver köpa in fler licenser ökar också kostnaden för

hur deras anställda ska kunna utföra sina arbetsuppgifter. Man måste därför på något vis sätta riktlinjer för hur man ska göra med kontoret, om man ska satsa på full kapacitet på kontoret och samtidigt betala för full kapacitet när det kommer till licenser som behövs för distansarbete. Förmodligen kommer vi se att organisationer framställer någon ståndpunkt där man endast tillåter exempelvis 3 dagar på kontoret i veckan och resterande dagar på distans.

Då våra respondenter inte visade någon form av stress kopplat till att man arbetade hemifrån och att arbetslivet på något sätt gick ihop med privatliv så verkade inte stressen öka eller sjunka (Amis & Greenwood, 2020). Däremot kunde vi förstå på åtminstone R1 och förmodligen fler av våra respondenter, att obalansen i arbetslivet ökade, åtminstone i början av pandemin. Exempelvis då R1 hade svårt att både påbörja men också avsluta en arbetsdag, vissa dagar blev längre än andra vilket också kunde negativt påverka nästkommande dag. Däremot tror vi detta mestadels handlar om inskolningen i hemarbete, då R1 inte längre kände samma problem så är det relativt uppenbart att detta är något man får lära sig då man inte tidigare varit med om det och inte heller har några rutiner sen tidigare.

Även om R3 ansåg sitt jobb bli tuffare på distans då kontakten med kollegor blev tuffare tyckte samtidigt R3 att en arbetsplats bör tillåta hybridarbete och såg det som en positiv utveckling. Om anställda som huvudsakligen har arbetsuppgifter kopplade till sociala interaktioner till stor del visar förtroende för distansarbete är det förmodligen inte något som försvinner på lång sikt. Samtidigt som man förstått om anställda får bestämma så lutar det mer åt att man bör tillåta distansarbete snarare än inte (Dubey och Tripathi, 2020). Effektiviteten har vi förstått påverkas vid distansarbete både till det bättre, men även sämre. Våra respondenter hade olika teorier varför det kan vara, men faktumet att effektiviteten skiljer sig är det som står fast. Vi tror att det respondenterna talar om, att effektiviteten är bättre i hemmet då ingen stör än, men samtidigt att effektiviteten kan vara sämre i hemmet när man behöver komma i kontakt med kollegor i slutändan handlar om att organisationer bör testa hybriden som det nu talas mycket om. Vissa dagar kan förmodligen alla behöva koncentrera sig själv utan att bli störd, men att vara fast på det arbetssättet 5 dagar i veckan kan förmodligen även skapa en ond cirkel av att man skjuter det vidare till nästa dag. Om man istället fastställer någon dag i veckan till sitt individuella arbete är det också den dagen man har på sig att lösa sina uppgifter, vilket vi tror kan resultera i att man också blir mer effektiv dagen/dagarna man sitter hemma jämfört med när man åker till kontoret och sitter i möten och diskuterar med sina kollegor.

5.1.3 IT-säkerhetens potentiella brister vid hemarbete

Det var huvudsakligen R2 som kunde framföra vilka brister man kan se hos anställda när man jobbar hemifrån. Kryphålen som handlar om identifikator, hemnätverk och exponering var inte något tydligt problem för någon av respondenterna vi talade med (Mandal och Khan, 2020). Den stora skillnaden R2 nämnde var att de tillfälligt inaktiverade flera funktioner i sina system som var tänkta att analysera enheter som var uppkopplade i nätverk med Assa Abloys hårdvara för att motverka intrång. Samtidigt som en cybersäkerhetsavdelning ska hålla koll på alla anställda på ett kontor, skulle de nu behöva hålla koll på samtliga anställda, men också samtliga enheter varje hem använder vilket kan leda till överbelastning på en avdelning som inte är skapad för den mängden belastning. Det kan även innebära att förövare enklare kommer genom säkerheten då resurserna är begränsade, i fallen vid våra respondenter hade de klarat sig undan eller möjligtvis lyckats stoppa förövarna ändå. Men risken har utan tvekat

ökat, samtidigt som man inte ökar sin budget på IT-säkerhet när man måste omkonstruera mycket från grunden är man plötsligt i en sits då man är benägen till attacker än tidigare.

R2 berättade däremot att de nästan exklusivt ser typer av Social Engineering-attacker både i deras organisation men även hos deras kunder. Flera studier visar samtidigt på att Social Engineering är den mest frekventa attacken, där en studie visar på 48% kommer från Nätfiske och på andra plats kommer "Ransomware" på 23% (ITC Secure, 2020). De två typerna av attacker R2 talade om var just Nätfiske och Ransomware, vilka också är de två vanligare attackerna globalt. Även R1 berättade att PwC gått utbildningar som fokuserar mer på Nätfiske än något annat visar att organisationer har en klar bild om hur verkligheten ser ut och lägger sina resurser på många korrekta sätt när det kommer till IT-säkerhet. Därför var det också intressant att höra från de mindre företagen som inte är tillräckligt stora för att hantera en dedikerad cybersäkerhetsavdelning, utan där får man istället försöka vara påläst för sin egna del och ta ännu lite mer ansvar om man vet att man inte på samma sätt har vinden i ryggen från en avsatt avdelning för IT-säkerhet.

5.2 Informationssäkerhet

5.2.1 Molntjänster

Samtliga respondenter beskrev en användning av molntjänster som till exempel Google (Cloud), Amazon (AWS) och Microsoft (Azure). Både respondent 3 och respondent 4 beskriver även ett användande av lokala serverhallar med en typ av molntjänst som accesstyp även här för att minska beroendet på en stor molntjänstleverantör och därmed minska riskerna för intrång (Mandal och Khan, 2020). Detta användande av molntjänster beskrivs som en redan etablerad arbetssätt från samtliga respondenter men respondent 2 beskriver en trend uppåt utav användandet av molntjänster inom organisationen. Respondent 4 pekar användandet av molntjänster och lokala servrar till sekretess och GDPR snarare än något som skulle ha en grund i uppskattningen av distansarbete. Ökningen av 775% som Microsoft presenterade (McAfee, 2020) verkar alltså inte innefatta de organisationer som vi intervjuat i någon stor grad.

Vid ökad användning av molntjänster ökar även risken för dataintrång (Mandal och Khan, 2020), samtliga respondenter beskriver dock att de inte upplevt något större antal försök till dataintrång. Detta kan kopplas till ovanstående stycke då molntjänster redan var utbrett använda inom organisationerna och därför inte medför någon märkbar ökad risk sedan flytten till distansarbete.

Respondent 1 och respondent 2 beskriver en medvetenhet av den ökade mängden data intrångsförsök som varit aktuell sedan pandemin och flytten till hemarbete tagit plats (Eklund, 2020). Respondent 1 beskriver till exempel en kommunikation om just ökade dataintrångförsök till sina kunder men visste inte om det är något som organisationen i sig varit utsatta för. Respondent 2 beskriver att en del av deras kunder har blivit utsatta för sådana attacker och pekar på att deras organisation har en väldigt stor kundbas där de ser ett antal olika typer av attacker som använts gentemot deras olika kunder.

5.2.2 Preventiva medel

För att försvåra dataintrång kan man se till vilka riktlinjer de olika organisationerna använder sig utav för att undvika skadegörelse (Mandal och Khan, 2020). Alla organisationer har en grundläggande princip gemensamt, användandet av VPN som en grundläggande riktlinje, men utöver detta skiljer det sig beroende på organisation. Respondent 1 beskriver till exempel en stark, tydlig och återkommande utbildning i vilka riktlinjer som finns vid eventuella försök till dataintrång, dock en avsaknad utav lösenordshanterare. Vidare beskriver respondenten ett väldigt stor fokus på just att försvåra intrång inom organisationen eftersom att de hanterar en stor mängd känslig information vilket styrker tydligheten på just hanteringen av potentiella dataintrång (Mandal och Khan, 2020).

Respondent 2 beskriver en stor mängd olika verktyg och rekommendationer som används för att minska riskerna för dataintrång. Till exempel använder sig organisationen av en awareness-funktion på samtliga datorer där okända och potentiellt skadliga enheter upptäcks för att arbeta proaktivt med frågan. Denna var organisationen dock tvungna till att i princip helt aktivera med flytten till hemarbete då det presenterades en stor mängd okända enheter från familjemedlemmar som inte kunde urskiljas gentemot skadliga enheter. Dock övervakas även USB enheter på samtliga datorer på organisationen för att kunna upptäcka smittade enheter och kunna isolera dessa datorer för att minska den potentiella intrång som kunnat ske. Organisationen använder sig inte heller av någon extern lösenordshanterare, inte som en del av riktlinjerna iallafall, utan ser istället till egenutvecklade lösenordsroterare för system till system kommunikation.

Organisationen som respondent 3 använder sig, till skillnad från de andra ordinationerna, av lösenordshanterare för samtliga konton som kan kunnas önskas tillgång till. Utöver VPN och lösenordshanterare finns det även dokumenterat hur hanteringen av data och utrustning skall ske samt en katastrofplan som ska följas vid eventuella dataintrång. Respondent 4 skiljer sig som mest från ovanstående som beskriver ett mer reaktivt tillvägagångssätt där varje incident hanteras efter hand utan några givna riktlinjer på hur det skall hanteras.

Utöver awareness-funktionen som respondent 2 beskriver så menar samtliga respondenter att användning av preventiva medel varit oförändrade sedan flytten till hemarbete och menar att det sedan tidigare redan arbetat med det nämnda typerna som en integrerad del av arbetet. Av att tolka svaren fanns det redan tydliga riktlinjer och preventiva medel från de första tre organisationerna då inställningen till att måna om känslig information för att förebygga dataintrång redan var etablerade sedan innan pandemin och flytten till distansarbete.

5.2.3 ISO-Standarder

För att organisationerna skall nå en bra nivå av informationssäkerhet kan de använda sig av ISO-standarder och mer bestämt ISO-27000 serien som berör en bred aspekt av informationssäkerhet (Nejib et al. 2018). De större organisationerna som vi intervjuade använde sig av just sådana standarder för att nå en bra nivå av informationssäkerhet där till exempel respondent 2 beskriver att de använder sig av ISO-27000 för informationssäkerhets standarder men även av ISO-9000 serien. Respondent 1 beskriver att de använder sig utav ISO-standarder men att det inte preciseras om vilka utan att satta mål för till exempel informationssäkerhet inom ett givet system eller liknande måste nås och att dessa granskas noga för att följa standarderna.

Om organisationerna som respondent 3 och respondent 4 arbetar för använder sig utav några ISO-standarder berörs tyvärr inte under intervjuerna. Av de respondenter som använder sig utav någon form av ISO-standard gällande just informationssäkerhet så har applikationerna av dessa varken tilltagit eller minskat i samband med flytten till distansarbete vilket kan bero på att de redan varit inkorporerade i företagets hantering av informationssäkerhet sedan tidigare.

5.2.4 Utbildningar

För att nå en större medvetenhet om de potentiella hoten som finns inom informationssäkerhet kan organisationerna använda sig utav utbildningar och de olika organisationerna skiljer sig en del visst just denna aspekten.

Respondent 1 beskriver en väletablerad och utbredd utbildning gällande informationssäkerhet med mera. Utbildningarna är återkommande vardera år och ämnar att utbilda de anställda inom vad som anses mest relevant för det givna året. Respondenten beskriver utbildningarna som mycket väl utformade för alla kunskapsnivåer och att mycket resurser går åt just dessa utbildningar. Respondenten beskriver att det inte finns någon skillnad i frekvens eller storlek på utbildningarna utan att de förändringar som skett till följd av flytten till distansarbete endast är kontextuella för att förmedla relevant information gällande just distansarbete och informationssäkerhet.

Respondent 2 beskriver en brett utförande av utbildningar som baseras på din tidigare kunskap genom att ställa frågor om ämnet först och fördela utbildningsmaterial baserat på de svar man fått fel på. Respondent 2 presenterar även resultat av deras simulerade phisingattacker som de skickar ut till de anställda, där de ser en direkt korrelation mellan vilka avdelningar som har tagit del av och följt utbildningarna och vilka som inte har det. Respondenten beskriver ett ökat informationssäkerhetsbeteende och medvatende hos de som faktiskt väl tagit del av utbildningarna vilket styrks av litteraturen (Stefaniuk, 2020). Respondent 2 lyfter även en viktig aspekt av utbildningar när han påpekar att man inte vill ge de anställda för mycket utbildningar om ämnet och skapa ett överflöd vilket direkt stärks som en faktor av de anställdas uppmärksamhet vid utbildningar (Alshaikh, M. et al. 2018). Likt respondent 1, så har inte utbildningarna förändrats i frekvens eller storlek utan endast på det kontextuella planet för att se till att relevant information gällande just distansarbete och informationssäkerhet når de anställda som följd av flytten till distansarbete.

Respondent 3 beskriver en samling dokument och onlinekurser som ligger till grund för deras utbildningar men ingen utbildning i seminarieform eller workshops vilket kan leda till minskad motivation att faktiskt ta in det innehåll som tillhandages (Khan, B. et al. 2011). Respondenten beskriver att det finns ett ökat fokus på utbildningar den senaste tiden men menar att det inte beror på flytten till distansarbete utan skiftet i omvärldsläget de senaste åren och pekar på att medvetenheten av hot har ökat för alla människor. Att medvetenheten av hot har ökat kan bero på att andelen hot faktiskt har ökat, vilket i sig skulle kunna knytas till den ökade användningen av till exempel molntjänster vid distansarbete och attackerna på dessa (Eklund, 2020).

Respondent 4 beskriver en frånvaro av frekventa eller återkommande utbildningar gällande informationssäkerhet och förlitar sig istället på de anställdas medvetenhet och erfarenhet. Respondenten beskriver dock att de inte heller skulle vara emot att bli mer informerade om just informationssäkerhet genom till exempel seminarier eller liknande utan pekar på den logistiska frågan om att samla sina anställda för något sådant istället.

De större organisationerna som vi intervjuat har helt klart ett bredare utförande av utbildningar gällande informationssäkerhet än de resterande organisationerna vilket dels kan bero på just deras storlek. De använder sig även av metoder som styrks av litteraturen vilket pekar mot en mogen informationssäkerhets nivå inom organisationerna.

5.3 Teorier inom IT-Säkerhet och informationssäkerhet

5.3.1 Technology Threat Avoidance Theory (TTAT)

Den mänskliga faktorn står som den huvudsakliga felande faktorn vid lyckade intrång (Kobis, 2021) och när man ser till den mänskliga faktorn är medvetenhet av hot en viktig faktor. Detta eftersom att medvetenhet av IT-riskerna, från till exempel anställda på den givna organisationen, har en direkt relation i motivationen till att undvika dessa (Liang & Xue, 2009). En anställd till exempel utreder inte hanteringen av en potentiell säkerhetsrisk förens denne har informerats, undersökts eller har erfarenhet av det potentiella hotet (Liang & Xue, 2009).

Samtliga korrespondenter beskriver att deras organisation har en bra bild av IT-säkerhet men synen på hur en sådan medvetenhet och erfarenhet skall nås skiljer sig mellan de organisationerna som vi intervjuat.

Respondent 1 och respondent 2 bidrar framförallt medvetenheten till de utbildningar som deras organisationer tillhandahåller. Utbildningarna beskrivs som välutformade och skapade samt underhållna med stora resurser. Detta för att den gemene anställde skall kunna ta del och utnyttja den information som tillhandages och öka den allmänna medvetenheten och beredskapen på potentiella hot.
Respondent 1 beskriver i synnerhet en väldigt djupgående utbildning som senast innehöll en del om segregerade nätverksmiljöer hemma som respondenten menar är så pass välgjord att gemene anställd utan någon datorvana skulle klara av detta, med eller utan existerande extra hjälp. Respondent 2 beskriver en mätning utav deras simulerade phishingattacker som visar på en stor och direkt korrelation mellan vilka avdelningar på organisationen som genomfört och lagt vikt på dessa utbildningar och vilka som inte gjort det.

Organisationerna som Respondent 3 och respondent 4 arbetar för verkar istället peka åt en naturlig medvetenhet av IT-risker i korrelation till branschen dem arbetar i, IT, då ämnet IT-säkerhet ligger naturligt inom medvetenheten för de som just arbetar med IT på en daglig basis. Organisationerna som respondent 3 och respondent 4 arbetar för verkar inte heller vara på samma nivå av breda utbildningar inom deras organisationer som organisationerna som respondent 1 och respondent 2 arbetar för. Respondent 3 beskriver en existerande arkiv av dokument med utbildningar men pekar fortfarande åt att den delen av organisationen som berör IT och känslig information är den mest medvetna, mer så på grund av deras bransch och arbete än nämnda utbildningar. Respondent 3 menar även att den allmänna kunskapen av potentiella hot har ökat de senaste åren. Respondent 4 beskriver en total avsaknad av utbildningar i något formellt upplägg och förlitar sig helt på medvetenheten och erfarenheten på de anställda, också här baserat på deras bransch och arbete.

Skillnaderna på respondenternas fokus angående just medvetenhet och erfarenhet kan bero på ett antal olika faktorer som till exempel branscherna som tidigare nämnts. Båda organisationerna som respondent 1 och respondent 2 arbetar för behandlar en stor mängd känslig information men deras huvudsakliga område inte IT till skillnad från organisationerna som respondent 3 och respondent 4 arbetar för. En annan faktor kan vara den betydande skillnaden i såväl storlek som ålder på organisationerna som respondent 1 och respondent 2 arbetar för i jämförelse med organisationerna som respondent 3 och respondent 4 arbetar vilket kan korrelera med en mindre utveckling av utbildningar och satta riktlinjer.

Respondent 1 pekar på kontextuella förändringar av just deras utbildningar sedan pandemin men att deras upplägg och frekvens förblivit densamma. Respondent 2 däremot beskriver en högre prioritering på just IT-säkerheten sedan flytten till hemarbete och pandemin dock inte budgetmässigt. Vidare beskriver Respondent 2 att vad man faktiskt gjort inte skilt sig utan att fokuset och takten på till exempel projekt har ökat sett till just IT-säkerhet. Respondent 3 och 4 beskriver ingen märkbar skillnad på just fokuset kring medvetenhet, detta kan dock leda tillbaka till tillvägagångssättet dessa organisationer har inte heller baseras på utbildningar eller liknande som främsta medel.

5.3.2 CIA-Triaden

Vidare sett mer till datahantering och informationssäkerhet med utgångspunkt i CIA-tridens tre pelare: *Confidentiality, Integrity & Availability* (Andress, 2014 s.5) beskriver respondenterna väldigt liknande berättelser både innan pandemin och under.

Under till exempel *Confidentiality* beskrev samtliga respondenter någon typ av behörighetskrav på den data som hanteras inom organisationen både inom de givna systemen men också på till exempel organisationernas kontor som i respondent 1 och respondent 2s fall.

Vidare sett på *Integrity* så binder denna samman med ovanstående *Confidentiality* eftersom att samtliga hade en bra grund redan där och kunde på så sätt använda deras behörighetskrav för att uppnå en bra *Integrity* vilket är vanligt (Andress, 2014 s.5). Utöver behörighetskraven använder sig även respondent 4 av en separat miljö och mockad data för att kunna hålla så hög *Integrity* på den givna datan som möjligt.

Availability kan ha varit den punkt som respondenterna beskrev som mest påverkad då trycket på IT-infrastrukturen ökade med flytten till hemarbete. Respondent 3 beskriver till exempel en brist på VPN-licenser och allmänna fel på dessa under den inledande tiden av flytten till distansarbete men att detta sedan med tiden löstes av organisationen. Beskrivningen från respondent 2 låter liknande där respondenter beskriver ett stort ökat tryck på IT-infrastrukturen när mängden distansarbetande personal gick från cirka 10% till 100. Inledande var det även här en brist på VPN-licenser och menar att det kommer att medföra ett behov att byggnad om det interna nätverket.

De två förstnämnda, *Confidentiality* och *Integrity*, verkar ha en starkare anknytning till införandet av GDPR än flytten till distansarbete i samband med pandemin. Respondent 3 beskriver till exempel att förbättringen av datahantering, till exempel kryptering på känslig information och tillgången till denna, har ett större samband med GDPR och dennes införandet än något annat. Denna nivå av *Confidentiality* och *Integrity* på den känsliga datan som de hanterar var alltså redan på en hög nivå sedan innan pandemin och har därför inte varit i fokus under pandemin. Respondent 2 beskriver även att GDPR är det som organisationen

främst ämnar att följa både för att följa lagarna och skydda sina användare. Vidare beskrivs en väldigt låg skillnad på just *Confidentiality* och *Integrity* och, som tidigare nämnt, fokuset var istället främst på *Availability* .

Dessa två pelarna var redan utvecklade och viktiga delar i samtliga organisationen sedan innan pandemin och förblev därför i princip oförändrade vid flytten till hemarbete. Detta medförde att organisationernas fulla fokus kunde gå till den sistnämnde *Availability* vilken kan ha medfört en lättare flytt än kanske väntat. Även denna aspekten kan kopplas tillbaka till just organisationernas branch-områden där känslig information ofta befinner sig och var därför också i större utsträckning påverkade av införandet utav GDPR.

6 Slutsats

Med en uppskalning av distansarbete till följd av Covid-19 pandemin och samtidig en ökning av dataintrång och cyberattacker ställs fokuset på IT-säkerheten och hur denna komma att ha påverkats utav denna plötsliga världshändelse. Med detta som grund formades följande forskningsfråga: *Vilka aspekter av IT-säkerheten har påverkats till följd av distansarbetets uppskalning?*

Vi har undersökt påverkan på en rad olika aspekter av IT-säkerheten, med blandade resultat, enligt nedan:

Distansarbete före Covid-19 pandemin var mer eller mindre obefintligt på organisationer, om det så var större eller mindre företag. Av vad vi kommit fram till så fanns det tekniska möjligheter, men att det inte utnyttjades på någon större skala, och att det ofta inte låg med den generella kulturen hos bolag. De riktlinjer som fanns för distansarbete före pandemin var inte heller något som organisationer följt då man inte fått anledning om deras anställda ändå alltid befann sig på kontoret.

Till en början av pandemin var det många frågetecken och oklarheter då samtliga parter var oförberedda på ett snabbt skifte mellan ena dagen till den andra. Till en början var det svårt för många att anpassa sig då det är många nya faktorer som plötsligt ska spela in som man inte tidigare testat, bara att ha en stabil nätverksuppkoppling skulle kunna ställa till det för många. Längre in i pandemin när anställda börjat komma in i distansarbete förstod vi att det är individuellt om man arbetar bättre hemifrån eller på kontoret, men att det inte bara handlar om individens arbetssätt, utan även vilken tjänst och arbetsuppgifter som kommer förfogat. Att distansarbete är här för att stanna är däremot en självklarhet, och man behöver därför också se över flera rutiner som man kanske tidigare trott endast skulle finnas under pandemin. Här är även IT-säkerheten ett ämne som inte lär få mindre fokus de kommande åren.

Det intressanta gällande hur en organisation kan brista var att man nästan exklusivt talar om Nätfiske och Ransomware, som att andra dataintrång inte längre förekommer. Då dessa två gör upp ungefär 71% av alla intrång så är det inte heller konstigt, och att utbildningar kopplat till IT-säkerhet kontinuerligt behöver ses över är en självklarhet då nya former av intrång kan dyka upp med nya arbetssätt och system. Mindre företag är inte, enligt våra respondenter, måltavlan för dataintrång vilket kan ses som märkligt då de som stora företag har hand om känslig data.

Om vi ser till molntjänster så presenterades en stor ökning i användandet utav dessa enligt litteraturen. Vad respondenterna beskrev var dock att det redan till stor grad var en etablerad aspekt inom samtliga organisationer. Inte heller har man på dessa organisationer märkt av de ökade fallen av dataintrång och cyberattacker på en själva. Dock har det noterats att medvetenheten om dessa finns hos majoriteten av organisationerna och att man i vissa fall sett denna ökning hos sina kunder som blivit utsatta.

De preventiva medel som används inom organisationerna idag är i princip densamma som de som användes innan pandemin. Respondent 2 presenterade en del av deras preventiva medel som de var tvungna att avaktivera till följd av flytten till hemarbete vilket om något pekar på en nedgång i IT-säkerheten under denna period.

Utbildningarna i sin helhet står som oförändrade sett till frekvens eller storlek utan endast kontextuella förändringar av innehållet för att framförhålla relevant information till de anställda. Samtliga organisationer håller samma nivå som innan pandemin på sina utbildningar dock pekar respondent 3 på en allmän ökad medvetenhet om potentiella hot.

Vidare sett till TTAT och medvetenheten inom de olika organisationerna så bidrar de olika organisationerna denna aspekt till olika faktorer men där de två huvudsakliga faktorerna är utbildningar och bransch. Utbildningar i den mån att man anser att utbildningsnivån innan pandemin var så pass hög inom IT-säkerhet att det inte direkt krävdes någon förändring där utöver de kontextuella. Bransch-faktorn kan ha varit den faktorn som spelat mest roll under denna undersökningen då argumentet om en medvetenhet bunden till de informations känsliga och IT relaterade branscherna som organisationerna finns inom beskrevs från samtliga respondenter. De menade att inom de givna branscherna har man en högre standard medvetenhet om IT-säkerhet än andra branscher.

Vidare sett till hur CIA-triadens tre pelare, *Confidentiality, Integrity & Availability* har påverkats utav flytten till distansarbete. Bundet till verksamheten som dessa organisationerna utför beskrevs pelarna *Confidentiality, Integrity* som att dessa redan var på en hög nivå innan skiftet till att distansarbete genomfördes vilket medförde ett mindre behov av att se till dessa under denna period. Utöver detta påverkade även GDPR IT-säkerheten, bland annat *Confidentiality & Integrity,* flera år innan pandemin och flytten till hemarbete.

Den sistnämnda, *Availability,* däremot var det största problemet för samtliga responder som beskrev problem med framförallt VPN-tjänster och licenser till dessa som den största orsaken men att den faktiska strukturen redan fanns där sedan tidigare vilket medförde att när dessa licenser kunde lösas så var *Availability* i princip densamma som innan flytten till distansarbete.

6.1 Förslag på framtida forskning

För framtida forskning kan det vara av intresse att undersöka organisationer som inte har IT och/eller IT-säkerhet, samt samt känslig information, som huvudsektor då detta verkar ha spelat en stor roll gällande medvetenheten, speciellt på de mindre organisationerna. Även medelstora organisationer kan vara av intresse att undersöka under samma forskningsområde då vi endast berör större eller mindre organisationer. Denna forskningen har även en aningen bred utgångspunkt för att försöka fånga de potentiella skillnader som kunnat presenteras vilket öppnar upp för möjligheten att gå in mer på djupen om till exempel medvetenheten inom dessa branscherna och hur den faktiskt ser ut.

Ytterligare en aspekt som nämnts är GDPR som verkar ha förberett företagen på distansarbete i aspekterna om informationssäkerhet. Här tror vi det finns rum att utföra vidare forskning om GDPR:s inverkan på flytten till distansarbete.

7 Appendix

Appendix A - Transkribering intervju 1

Transkriberingsprotokoll
Organisation: PwC Sverige **Intervjuobjekt:** Respondent 1 **Starttid och plats:** 28 April 2022, Klockan 10:00, via Videomöte. **Medverkande:** Respondent: Respondent 1 (R1) Intervjuare: Alexander Nilsson Sump(ANS) och Oliver Ilijason(OI)

Rad	Person	Fråga/Svar	Kod
1	OI	Ja men då börjar vi intervjun här då. Din titel?	
2	R1	Bra fråga. Ja vad ska man säga… kan man ta typ såhär Systemtekniker/Utvecklare?	
3	OI	Yes och vilken organisation arbetar du för?	
4	R1	PWC Sverige.	
5	OI	Tackar. Då går vi väl över till den riktiga intervjun. Då ska vi se. Hade ni på PwC möjlighet till hemarbete före Covid-19 pandemin?	
6	R1	Det fanns möjlighet för det, absolut. PwC har väl ändå varit ganska duktiga på att förkratta möjligheten eftersom att vi har många revisorer som är ute och åker, alla är inte alltid inne på kontoret och jobbar. Så att möjligheten att koppla upp sig remote har alltid funnits sen långt innan pandemin kom… så det har funnits bra möjligheter för det innan också. Kanske inte att det har varit direkt uttalat i samma utsträckning som det varit efter men det fanns möjlighet.	D-FC D-IT
7	OI	Ja. Hur skulle du säga, hur var det för dig, var det att du jobbade hemifrån innan då pandemin några dagar i veckan eller var det	

		bara väldigt sporadiskt?	
8	R1	Nä för oss så kom det som en, det kom ganska, där så fort folkhälsomyndigheten kom ut med rekommendationerna tror jag samma dag. Jag hade inte tittat på nyheterna och hade inte så bra koll på det så när jag kommer in på kontoret så har jag fått ett mail där det står att alla anställda ska jobba hemifrån om det inte är så att man tillhör en viss specifik grupp som måste va på plats så ska alla jobba hemifrån. Så jag kom in på kontoret och så vart jag hemskickad samma dag [skratt].	D-UC
9	OI	Ja precis [skratt]. Det är väl så det var för många kan jag tänka mig. Men innan pandemin, jobbade du hemifrån någonting då?	
10	R1	Aldrig, jag var alltid på plats.	D-FC
11	OI	Yes, super. Så då beslutar sig organisationen för att dem flesta skulle börja jobba hemifrån men vilka var det som inte kunde jobba hemifrån, generellt?	
12	R1	Det vet jag inte. Jag kan tänka mig att, det framgick inte specifikt i mailet men måste väl ha varit någon typ utav personal som hanterar kontorsservicen generellt möjligtvis. Eller folk som håller på med kontorsstädning eller någonting sånt. Posten internt kanske eller någonting sånt.	
13	OI	Ja det låter rimligt. Och när man gick ut med att alla skulle börja hemifrån, har du ett hum om ungefär när detta var i tiden?	
14	R1	Ja det har jag ingen aning om.	
15	OI	Det var väl ungefär i mars 2020, har jag rätt då för mig nu?	
16	R1	Ja, Mars 2020.	
17	OI	Det var väl där vi iallafall från skolan fick veta att nu ska, nu ska vi inte vara i skolan längre.	
18	R1	Det var ju då, det var någonstans där i mars som folkhälsomyndigheten iallafall hade sitt uttalande.	
19	OI	Ja precis. Men så det var strax därefter då?	
20	R1	Jag tror till och med att det var samma dag	D-UC
21	OI	Ja, nä men dåså. Det blir bra. Och du och dina kollegor hur, känns det mest positivt eller mest negativt att jobba hemifrån, både under pandemin men också nu efter?	
22	R1	Jag kan ju säga för min egna del så har jag väldigt svårt att tänka mig en, en arbetsplats där man inte tillåter hybridarbete. Så att, det är… jag vet inte, det är både positivt och negativt att jobba	D-UC

		hemifrån. Man tappar ju mycket av den sociala interaktionen och att hänga med varandra och ha kreativa diskussioner och så. Därför är det skönt att kunna åka in till kontoret någon dag i veckan, eller två, och faktiskt träffas face-to-face och utbyta ideer och prata. Men nu blir det oftast, nu också när dem, när man sitter och jobbar hemifrån så blir det oftast fokusen på det sociala så stort så det vi har gjort, i vårt team, är att när vi träffas så försöker vi ha våra sociala aktiviteter som vi har i teamet, alltså de aktiviteter man alltid gör som ett team, typ gruppmöten och sådana saker, planerar vi in på en dag, så att allting sånt ligger under samma dag under veckan. Så att, för att det var väldigt många i teamet som uppskattar mer, alltså när man åker in till kontoret vill man träffa sina kollegor, man vill inte sitta i möten och jobba, för det kan man lika gärna göra hemifrån.	
23	OI	Jo nä men precis. Nä men det är väl nästan lite kopplat till vår nästa fråga också, att många känner ju ofta kanske att man är lite mer effektiv hemifrån eftersom att man inte blir störd på samma sätt: Känner du att det stämmer också?	
24	R1	Absolut men det kräver ju lite disciplin också. Så jag kan ju säga från början så hade inte jag, jag hade inte den strukturen jag behövde på mitt arbete för att vara, för att kunna koppla av från arbetet och så. Så det vart, det varit en väldigt konstig omställning för mig i början, det varit både, vissa dagar vart alldeles för produktiva, om man kan säga så, och andra dagar vart bara så, man vara bara så trött för att man hade suttit alldeles för länge dagen innan. Så det var, med tiden så vart det bättre, man fick upp lite bättre rutiner kring det.	D-UC
25	OI	Ja, precis. Och har du märkt av att organisationen har förändrats sina säkerhetsåtgärder efter att man då började jobba hemifrån på något sätt? Att till exempel efter att ni fick det där meddelandet att nu ska ni jobba hemifrån, så kanske det sen kom “nu gäller detta också” ur ett it-säkerhetsperspektiv då, lite att…	
26	R1	Här är ju kanske fördelen med att jobba på ett, ett bolag, som ändå sitter och jobbar inom vissa delar av finansmarknaden och har väldigt mycket kundmaterial generellt att säkerheten är redan väldigt hög som det är så att egentligen så var det ingenting nytt som tillkom utan det var mer bara att man fick, man fick möjligheten att applicera det vi redan hade lärt oss innan, fast nu vart det en alldaglig grej. Sen så dyker det ju inte upp några mail längre där det står typ lämna inte papper framme på bordet för att det är ingen som är på kontoret [skratt].	D-UC I-U I-P
27	OI	Nä precis [skratt].	
28	R1	Vissa saker, vissa saker har väl kanske blivit lite annorlunda, nu får man mail där det står istället, lämna inte papper hemma på bordet	

		liksom, utan [hör inte 0:07:42] att alla papper tas hand om och sådana saker. Så det är väl kanske att man har bytt ut orden, vart man är någonstans.	
29	OI	Ja nä men det förstår jag. Nästa fråga kanske inte är något du vet specifikt, men vi kan ju ta på ett ungefär, så PwC har ju då jobbat mycket med till exempel auktoriseringsverktyg och VPN:er och så vidare då som du sa. Har, vet du om organisationen har märkt av något ökat tryck att förövare försöker komma åt data mer än det var tidigare?	
30	R1	Där kan jag nog mer bara svara från en, kanske en extern utblick på vad jag har märkt från PwC kommunicerar ut till sina kunder. Att de kommunicerar ut att det är ju vanligare och det händer mer idag än vad det gjorde förut. Men om vi specifikt är påverkade av det här har jag ingen aning om.	D-IT
31	OI	Nä, men man vet iallafall att det sker mer?	
32	R1	Absolut. Det finns en, det finns en väldigt tydlig awareness av det iallafall.	D-IT
33	OI	Ja precis. Super. Då kan vi gå över lite till molntjänster och annat, är det något som PwC använder sig utav? Då alltså molntjänster?	
34	R1	Ja.	
35	OI	Vilken molntjänst?	
36	R1	Vi har ju sen länge använt Google ganska primärt, för olika samarbetsverktyg och sådana saker. Och sen kanske mer för publicering av kod och sådana saker så använder vi Azure.	I-M
37	OI	Ja, super. Sen ni har använt Google eller Azure, har ni fått reda på från er leverantör att det har skett någon, något försök till dataintrång som kan ha påverkat er?	
38	R1	Inte, inte från, inte på våra saker. Vet inte riktigt hur det där fungerar när Google blir utsatta för någonting. Men jag antar att det borde bli ganska, kommunicerat ganska fort med tanke på att då blir ju hela PwC utsatta i och med att det inte är bara sverige som är med utan det är ju hela nätverket.	I-M
39	OI	Ja precis, nej det är ju rimligt att dem ska få ut det till er iallafall, Att det kan vara någonting som händer.	
40	R1	Exakt.	
41	OI	Det är bra, Alex(ANS) har du något att lägga till där?	
42	ANS	Nej, det är väl ganska tydligt.	

43	OI	Yes då kör vi vidare. Om vi går till lite preventiva medel som till exempel lösenordshanterare, blockering av minneskort och annat, det är ju någonting som du att ni använder.	
44	R1	Ja.	
45	OI	har du några exempel på vad ni använder och vad som kanske egentligen är, som PwC menar på är viktigare och styrker på mer än andra?	
46	R1	Vi har ju alltid så återkommande utbildningar i säkerhet och vi har ju våran interna säkerhetsavdelning, har ju lite roterande tester ibland, där det dyker upp sådana här skumma emails som ser väldigt verklighetstrogna ut. Som mer utbildningsmaterial, som man får hantera i vardagen, så att man får vara med och se vad som händer och se om man agerar rätt eller inte. Så att det pågår alltid kontinuerlig träning utav alla medarbetare hela tiden och sen så finns det alltid en, en återkommande kurs varje år där vi går igenom saker som har förändrats, saker som är nytt, saker man behöver tänka på.	I-U
47	OI	Perfekt, då lägger ni ändå lite vikt i att försöka…	
48	R1	Det är väldigt mycket vikt på utbildning skulle jag säga, kopplat till dem frågorna.	I-U
49	OI	Ja precis, nä men det är väl, det är väl viktigt idag kan jag ju, kan man ju tycka.	
50	R1	Det är ju, jag tror också att det är väldigt viktigt för att vi vill ju också leva som vi själva lär till våra kunder när det kommer till det.	I-U
51	OI	Ja precis.	
52	R1	Det är mycket, mycket fokus på det.	I-U
53	ANS	Jag har en fråga, är det något med utbildningarna i sig som har förändrats sen ni har börjat jobba hemifrån eller är det samma principer.	
54	R1	Nej, dem har förändrats, det är det som jag tycker är så bra med utbildningarna, att det läggs ner väldigt mycket tid, tanke, research och efterforskning på dem, att dem är anpassade till situationen vi befinner oss i idag. Så det vart ett ganska tydligt skift, skifte när det var, när vi kom till Covid. För första året så var säkerhetutbildningarna väldigt mycket fokus på att man ska tänka på vad som händer runt omkring en, nu när man sitter och jobbar hemma. Sen i år så var det väldigt mycket mer fokus på den tekniska delen kring om man jobbar hemma. Jag har ju aldrig varit på ett ställe där man börjar prata om segregering utav nätverk	D-UC I-U

		hemma till exempel, för typ gemensamma personer och typ hur man kan gå tillväga för att hindra saker, så det var, det är väldigt intressant. Dem lägger, det läggs väldigt mycket tid på det och det tillhandahålls material också så att gemene man skulle kunna uppnå en segregerad nätverksmiljö hemma även om man aldrig har gjort det förut så det är lite häftigt.	
55	OI	Så iochmed att du sa gemene man, tänker du då iochmed att du är ganska IT-kunnig, så att du menar på att alla egentligen, även en revisor som kanske aldrig, som knappt vet vad en dator är, skulle kunna, till en gräns iallafall, klara av dessa utbildningarna?	
56	R1	Ja och det finns, det finns supporterande material kring det också. Så efter den sektionen är färdig så finns det, ja men om man inte vet hur man gör så kan man höra av sig hit så kan man få hjälp mer. Så att, väldigt, väldigt bra.	I-U
57	OI	Ja det är väldigt bra att man har den möjligheten. Hade du något Alex (ANS)?	
58	ANS	Nej, det var [hör inte 0:13:32].	
59	OI	Finns det några givna riktlinjer för anställda ifall, för att motverka dataintrång, till exempel ifall… ja	
60	R1	Absolut, vi är ganska hårt indrillade i vilken väg man ska ta och vilken kedja man ska ta, hur man ska rapportera, när man skall rapportera och hur fort man skall rapportera det. Så det finns… och de är återkommande också varje år bara för att så här banka in dem.	I-P
61	OI	Ja en reminder.	
62	R1	Exakt, så det finns det.	
63	OI	Dessa har då kanske förändrats lite efter att man började jobba hemifrån kan jag tänka mig, eller har det egentligen varit samma alltid?	
64	R1	Det har alltid varit ganska högt tryck på hur fort man ska agera och vad man ska hålla utkik efter så jag kan ju inte säga att det har blivit… någon större förändring utan det har det har alltid varit… otroligt seriöst och väldigt välfokuserat på hur man ska hantera sådana incidenter när de uppstår. Så att det är nog inte så stor skillnad från hur det har varit sedan innan vi jobbade hemifrån. För vi har ju ganska många revisorer som ändå är ute hos kund och sitter i andra miljöer så att det är inte ett främmande koncept, det är bara att nu är det lite större skala än vad det var innan kanske.	D-UC I-P
65	OI	Ja precis, du har inte heller känt att det var mer frekvent att man	

		blev påmind mer och mer sen man började jobba hemifrån, utan det har varit ungefär samma	
66	R1	Ja.	D-UC
67	OI	Ja men super. Nu ska vi se om du har någon koll på hur ni använder er utav ISO-standarder. Är det någonting du vet att ni använder inom IT-säkerhet då?	
68	R1	Ja, och vi blir ganska hårt mätta utav våran interna säkerhetsavdelning att vi uppnår dem olika standarderna som finns, det är därför vi har hela den hära… en granskningsprocess för alla applikationer till exempel när dem blir väldigt rigoröst granskade och ser också till att alla standarder som behöver uppnås, uppnås beroende på vilken typ av applikation det är och vilken data som finns i den.	I-I
69	OI	Super. Du kanske inte har koll på vilka ISO-Standarder ni använder eller har någon i huvudet?	
70	R1	Nej, jag har dem inte i huvudet utan man får det inte som, den här har du brutit mot och den här har du gjort fel utan det är mer som det är det här som vi behöver rätta till, så man får mer ett mål om vart man behöver va, inte vad man har gjort fel och enligt vilken paragraf man gjort fel.	I-I
71	OI	Nä precis, det låter väl rimligt att man inte skickar ut det till alla anställda sådär. Vi pratade lite om utbildningar innan men vi kan bara ta lite, ska se om vi har några följdfrågor där… hur ser upplägget ut på era utbildningar, du sa att ni gjorde dem varje år, kan du gissa ungefär hur lång tid man lägger varje år på till exempel IT-säkerhetsutbildningar?	
72	R1	Svårt att säga, jag tror att det finns, det är nog lite olika, det är nog en del som lägger väldigt mycket mer tid på det beroende på kanske hur man är exponerad utåt och vad man jobbar med men det är väldigt mycket mer tid än vad jag har varit med om på tidigare företag jag har jobbat på. Det är väl det jag kan säga om det.	I-U
73	OI	Skulle du säga att det finns dem som ska lägga mer tid än andra, ens chefer till exempel eller om en är mer exponerad än den andra, anses dem bör lägga mer tid då?	
74	R1	Jag tror att dem får nog kompletterande utbildningar just när man sitter och kanske har extern kontakt väldigt mycket mer kanske just när man sitter i en servicedesk där man kan bli uppringd både extern och internt. Som intern personal finns det kanske bara vissa exponeringsytor man har och det är väl dem man blir tränad i.	I-U
75	OI	Ja, låter väldigt bra. Har du märkt nått skifte i utbildningarna från	

		att ni jobbade på kontoret till att ni jobbade hemifrån, du sa innan att dem brukar fokusera på olika saker varje år, det kanske är mest det då?	
76	R1	Det är innehållet som blir väldigt mycket större fokus på och det är baserat till hur verkligen ser ut just nu det året.	D-UC I-U
77	OI	Då kan vi gå in på, när man skriver en kandidatuppsats så har man också lite teorier man behöver gå igenom så vi har lite frågor runt om dessa, du behöver inte kunna teorierna utan nu är det bara lite generella frågor. Skulle du säga att en vanlig anställd på PwC är välinformerad om IT-Säkerheten som ska följas?	
78	R1	Ja.	T-T
79	OI	Om företaget har gett utbildningar inom informationssäkerhet, märker du någon skillnad på dig själv i ditt säkerhetsbeteende, alltså känner du att du lär dig något utav det och att du faktiskt arbetar accordingly?	
80	R1	Absolut, och inte bara kanske när jag tänker och reflekterar själv utan kanske när jag jämför med kollegor som också jobbar i samma bransch… det är en väldig skillnad på fokus så absolut.	T-T
81	OI	Har du märkt någon skillnad på dina kollegor från att ni började jobba hemifrån just på deras säkerhetsbeteende då, att nu börjar man jobba hemma så nu får man antingen kanske man får vara ännu försiktigare, kanske att någon har börjat använda, säga att ni inte hade lösenordshanterare innan, men att någon kanske började använda det nu för att vara lite extra säker?	
82	R1	Det har… jag skulle säga ja på det, sen om det är kopplat till just att jobba hemifrån eller inte eller om det är en ren slump, det kan vara en annan sak.	T-T
83	OI	Absolut, så är det ju… Hur skulle du säga att ni arbetar med konfidentialitet, till exempel använder ni er utav någon behörighetskrav eller liknande vad du vet, just när det är känslig information?	
84	R1	På just IT sidan så absolut och i system absolut, alla har inte rättighet att se allting. Sen så finns det ju också även uppdelning på… inne på kontorsbyggnaden också där vissa områden har en helt annan… alla kommer helt enkelt inte in där.	T-C
85	OI	Nä, det är väldigt bra. Finns det något speciellt sätt ni arbetar för att hålla integriteten på den data ni erhåller, både från er själva och från kunder och annat?	
86	R1	Absolut, men hur i detalj vi gör det har jag inte så jättebra koll på. Jag sitter inte direkt och jobbar med kunddata i den utsträckningen,	T-C

		men det ingår ju i granskningen som görs utav alla applikationer och all data som hanteras.	
87	OI	Om Man säger att ni har ett projekt, har alla möjlighet att kunna göra vad dem vill med till exempel alla system i det projektet och till exempel radera någonting om de vill eller finns det någon typ av hierarki där den här personen får göra detta?	
88	R1	Jag skulle säga, det gör det, men hur vet jag inte eftersom att det är lite mer utav en verksamhetsfråga kopplat till kanske uppdragen och hur det ser ut.	T-C
89	OI	Jag tror inte jag har någonting mer där riktigt, Alex (ANS) är det något du tänker på?	
90	ANS	Nä det är väl om det finns något allmän om IT-säkerheten som du känner har förändrats sen ni har börjat arbeta hemifrån, något som blivit bättre eller sämre?	
91	R1	Nej… inte något konkret. Utbildningarna blir ju generellt sätt bättre varje år eftersom att man får ju lämna feedback på dem också men inte något annat.	D-UC I-U
92	OI	Nej och du har inte känt heller att man lägger för mycket tid på IT-Säkerhet, att man måste hela tiden logga in på 17 olika grejer för att komma åt sina system, du känner inte att det är väldigt tidskrävande att ha en bra IT-Säkerhet?	
93	R1	Nej utan det finns… man kan uppnå smidighet i att ha en väldigt säker miljö också.	T-T
94	ANS	Det verkar ju som att PwC är väldigt långt fram så att ni kanske inte blev så pass påverkade av flytten till hemarbete som kanske andra företag?	
95	R1	Man har ju haft kollegor som jobbat på andra ställen där hela den här grejen varit en jätte-huvudvärk, polare man känt sedan tidigare, där man inte riktigt var förberedd på 2,5 år utav hemarbete så att jag tycker att jag är väldigt lyckligt lottad på stället jag sitter och jobbar för att det har varit otroligt smidigt, det var som att allting var förberett [skratt]. Så att det var skönt.	
96	OI	Super, om inte Alex (ANS) har något mer så tänker jag att vi avslutar inspelningen.	
97	ANS	Nej det avrundade det nog fint.	
98	OI	Då avslutar jag det här.	

Appendix B - Transkribering intervju 2

Transkriberingsprotokoll
Organisation: Företag B **Intervjuobjekt:** Respondent 2 **Starttid och plats:** 3 Maj 2022, Klockan 08:30, via Videomöte. **Medverkande:** Respondent: Respondent 2 (R2) Intervjuare: Alexander Nilsson Sump(ANS) och Oliver Ilijason(OI)

Rad	Person	Fråga/Svar	Kod
1	OI	Så, yes, super då startar vi intervjun … Din titel	
2	R2	Ja min titel kanske, jag är Global Cyber Security… Ja jag är Global Cyber Security Manager på Assa Abloy	
3	OI	Och ja… Vilken organisation arbetar du för, men den kan vi skippa för tillfället	
4	R2	Ja	
5	OI	Så… då börjar vi väl den riktiga intervjun kan man väl säga… hade ni på ert företag möjlighet till hemarbete före Covid-19?	
6	R2	Ja, det hade man	D-FC
7	OI	Hur såg det ut, både hur många, kunde man välja själv hur många dagar i veckan det var eller var man tvungen att, eller kunde man egentligen göra det precis hur man ville?	
8	R2	Om du tänker på den svenska organisationen så är det chefen som godkänner. Sen så kan du ju ha en hel roll som du sköter hemifrån, alltså du jobbar 100% hemifrån i ditt arbete. Men dem som sitter, som kan man säga har en arbetsplatsen är kontoret, Assa Abloy kontoret, där godkänner chefen vilka dagar du kan jobba hemma	D-FC
9	OI	Precis, hade ni några, i och med att man kunde jobba hemifrån då, funderar jag på, fanns det några speciella säkerhetsåtgärder ni hade när man då jobbade hemifrån? Till exempel använde man VPN tjänster eller har ni alltid använt molntjänster eller hur såg det ut? Och detta är alltså då fortfarande i kontexten före Covid-19 tänker jag	

10	R2	Före Covid-19 hade vi allt det, vi har, den stora tjänsten är en VPN-tjänst man har som man kopplar in sig och jobbar via	D-FC I-P
11	OI	Suveränt. Då kan vi enkelt hoppa till lite mer under och efter Covid-19… beslutade sig hela organisationen, då tänker jag egentligen huvudsakligen kanske Assa Abloy Sverige, bestämde man i hela organisationen samtidigt att nu, från och med idag, så jobbar vi hemifrån? Och ifall det var så har du ungefär ett tidsperspektiv på det?	
12	R2	Jag har inte exakt datum när dem gick ut, det har jag inte här men jag kan gräva fram det men det bestämdes av Assa Abloy Group att nu så stänger vi ner. Sen har det varit lite olika i landet när man har öppnat upp och så. Sen har vi fabriker och dem har ju inte stängt, fullt, men de har gått ner i mindre antal med avstånd och hela den biten	D-FC D-UC
13	OI	Det är väl nästa fråga lite jag har, ifall ni har anställda som inte kan jobba hemifrån och då till exempel på fabriker?	
14	R2	Ja det har vi, ja	D-UC
15	OI	Finns det några andra?	
16	R2	Vi har ju säkerhets, jag har ju säkerhetsteam som jag har som måste kunna sitta inlåsta när det är fysiskt säkerhet plus cybersäkerhet så att säga. Vi fick till, vissa av dem fick vi skriva speciella saker så att dem kunde jobba hemma och dem andra teamen fick gå ner på ett minimalt team så att man hade avstånd, väldigt stort avstånd. Så att en avdelning som kanske var 20 personer där satt 2 så att där var fysiskt på plats några	D-UC
17	OI	Ja precis, nä men suveränt… Känner man att dem flesta av, både du och dina kollegor, är positivt eller negativt inställda på hemarbete?	
18	R2	It depends, alltså det berors lite på vilket typ av arbete man gör… det har ju varit ett sug efter att man ska komma tillbaka också för att man vill inte sitta och jobba, alltså, det är trevligt att jobba hemifrån, det är lite frihet och så men faktumet är att produktiviteten går lite neråt. Och sen vissa som är viktiga för teamen, dem har man inte samma tillgång till som man har fysiskt… så vi brukar säga att det blivit lite annorlunda nu när man kommit tillbaka för att vissa som är här inne, dem är så populära så dem hinner inte göra något arbete själva eftersom att det är ett sådant sug efter dem… så då brukar vi säga att när du är på kontoret så är du där för alla andra och sen om du måste göra något speciellt och riktigt liksom, så kan du, men det är jag godkänner, då kan du sätta dig hemma så du får komma ikapp med ditt eget så att säga. Men vi är fortfarande där i det här suget, när vissa, alltså vi är fortfarande, vi är inte tillbaka till den här normala lugna	D-UC

		kontors, för vissa resurser som är väldigt kritiska för alla teamen	
19	OI	Nä precis, nä men det är väl så det ser ut idag kan jag tänka mig på många företag känns det som	
20	R2	Ja	
21	OI	Ja precis, du pratade lite om att ni känner att produktiviteten kanske inte riktigt är densamma, men känner du att, känner du att effektiviteten på vissa arbetsuppgifter har kunnats förbättras eller har allting känts lite sämre? Till exempel…	
22	R2	Nej det är mer saker vi löser tillsammans som blev lite sämre för att där blev ett sådant litet avstånd eller… och sen så gick ju faktiskt, initialt iallafall sen fick man ju sätta regler runt det, det var ju inget, man träffas inte normalt runt kaffet och har korridorssnack och så utan då blev det nästan att man bokade en 15 minuter, 30 minuter, och hade dem har korridorssnacken vilket gjorde att det blev väldigt, väldigt mötes intensivt i början. Så alla hade hela dagen i möte när de satt hemma och det var ju inte riktigt idéen. Så vi… jag införde att dem boka ut, vad ska man säga, man bokade ut tomrum i sin kalender för att jobba själv och implementera det. Och sen så hade vi, på fredagar hade vi en dag efter lunch, alltså en timme efter lunch som vi kallar cyberkafé där vi bara snackar privat och skit rent ut sagt och det var en viktig ventil, och då fick man inte prata jobb	D-UC
23	OI	Precis, som fredagsfika bara	
24	R2	Ja typ så	
25	OI	Ja nä men super… du sa innan att ni har använt VPN-tjänster och annat innan Covid-19	
26	R2	Ja	D-FC
27	OI	Jag tänker mer, har ni några säkerhetsåtgärder som har förändrats på grund av just flytten till hemarbete, att till exempel Assa Abloy har kommit ut och sagt att nu har vi fått ändra på hemarbetet så nu måste vi också jobba så här eller finns det någonting du vet…?	
28	R2	Alltså nä det har man väll inte gjort utan i grund och botten är det reglerna som ligger kvar sen är timingen när man går tillbaka, om man går tillbaka 10%, 20%, 100% till kontoret, det har ju styrts från centralt håll. Men initialt så, du vet, det är ju klassiska grejer som licenser och sånt man har i tjänst som används av kanske 10% av personalstyrkan och så nu ska 100% av personalstyrkan använda den och då får man också titta på tekniken, jag menar om man har klassiskt VPN så kanske, vi gick ju upp mer och mer i molnet med utökningen så att att säga och det kräver ju en annan typ av säkerhet när hela arbetsstyrkan går ut, om några få jackar	D-UC I-P

		upp och connectar på daglig basis så är det väl, det kräver också att man kanske initialt måste bygga om det interna nätverket och sådana bitar också på sikt. Så det har varit, det var en tuff period, tror jag mest för nätverksteamen och så precis när vi switchade över att man hann inte med. Om vi tittar på min avdelning då på Cybersecurity så fick vi ju, ja vi fick, ja vad har vi 30000 till 40000 användare, vi fick ju minst 10000, 20000 hemmakontor som plötsligt dök upp på våra skärmar. För vi har ju produkter i våra datorer som scannar av och känner av okända enheter, så den funktionen fick man nästan mer eller mindre stänga av för att då hade ju ungarna Playstation och grejor som dök upp. Så vi har ju en sådan, vad ska man säga awareness-funktion som plockar upp, det är ju för att vi ska hela tiden hitta okända devicer i våra nätverk. Så att sådana, rent, det fick man ta en paus från sådana funktioner under ett till två år mer eller mindre	
29	OI	Ja det är väldigt intressant faktisk… ja det var väl, då går vi till nästa lilla delkapitel som är, då är det väl egentligen IT-säkerhetsbristerna vid hemarbete som du touchade lite på precis	
30	R2	Ja	
31	OI	Och det första vi, jag tänker är ju att övergången till hemarbete har ju medfört nya potentiella brister för IT-Säkerheten, till exempel att företag har börjat använda, kanske inte Assa Abloy specifikt, men vissa har börjat använda auktoriseringsverktyg, uppkoppling via hemnätverk och annat som de då inte har använt innan som du också touchade på precis, har ni märkt något ökat tryck från förövare att inrikta sig på alltså ju hemarbetet på den enskilde anställde att försöka komma åt genom den mer?	
32	R2	Nej, alltså det är väldigt svårt för att dem, för att pinpointa, dem är kanske… den här klassiska du tar över datorn det finns väll inte så jättemycket längre. Det är fortfarande att du kan få ett malware eller så, man jobbar idag genom att sno konto, credentials, det är det man jobbar på. Du behöver ju inte ha en dator för att logga in, räcker med användarnamnet och människor är människor så det är lätt, din mailadress följer med och kommer med på en föräldralista med fotbollslaget om du är slarvig och sen så har fotbollslaget inte jättestor säkerhet och det är lätt att tanka ner alla mailadresser och så vidare. Sådana här tjänster blir ju breachade rullande. Så det stora är väl mer att man är lite slarvig med sin företagsmail, det är väll en större risk ändå. Sen så, password idag… finns det väldigt sofistikerade att gissa, oftast när du knäcker en databas, om du loggar ju in i sådana här appar, fotbollsappar, alla möjliga privata appar eller restaurangappar eller någonting och oftast är människor människor så du har ju samma password där som du kanske har på jobbet eller liknande password du har där som du har på jobbet. Och sen så finns det ju stora, stora databaser med dem kanske 10000 mest vanliga passworden som man lägger på så det går ju	D-IT

		kan man säga knäckandet mycket, mycket snabbare och då räcker det tyvärr idag med ett konto för att ta sig in och så. I ett stort nätverk hittar du alltid någon… ja någon server som kanske har lite mindre säkerhet och så. Så det är ju det stora, det är ju det vi jobbar med väldigt, väldigt aktivt, det är ju just de här kontona och credentials. Så ett klassiskt då när man tar över datorer och sitter utifrån, de här hackarna vill ju köra sin egen utrustning, de har färdigbyggda scripts och sådana grejer så dem kanske tar sig in och försöker ladda ner dem passworden och dem kontona som varit inne på din dator just för tillfället. Sen kör dem in det i sina verktyg sen pumpar dem på sina brute force attacker mot ett företag.	
33	OI	Ja	
34	R2	Så just det, sen försöker vi alltid att hålla säkra klienter och skydda klienterna för att vi ska ju inte, alltså om du är hemma eller du är på ett kafé eller på flyget eller så som användare så ska du ju inte bry dig var du är utan det är vårt jobb att säkerställa att du är så säker som möjligt.	
35	OI	Ja precis… Det är väl lite det vi touchade på också men har ni märkt någon skillnad på den mängd eller typ av försök till dataintrång sen flytten till distansarbete eller känner du fortfarande att nä det är ändå, som du sa innan att det är samma, ungefär?	
36	R2	Det är samma, ungefär, sen har det ju varit, vad ska man säga… olika kampanjer som har försökt att utnyttja detta men vi har inte sett att vi har blivit targetade med just dem. Så vi har ju följt dem givetvis… det är sådana här fishing attacker blir väldigt, väldigt mycket mer lättare när du har mindre anknytning till arbetet, om du inte är på jobbet varje dag så kan jag skriva en jättefin Assa Abloy logga och fejkad mailadress och skicka till dig, absolut, eftersom att du… kanske lättare när du är på kontoret att fråga någon, är det här någonting som ni känner igen eller inte? Men det är mer av teoretisk art så att säga, det är inget vi har sett, vi har inte sett några trender, vi har inte sett några, vad ska man säga, större säkerhets skillnader mot normalt mot hemma under Corona-tiden	D-IT
37	OI	Nej, det är ändå intressant att det skiljer sig lite där mellan vad man skriver i teorin och hur det funkar på riktigt egentligen och vad företagen märker av. Nä men vi kan väl gå över lite till informationssäkerhet, och då tänker jag att vi kan börja lite med molntjänster. Ni sa innan att ni använder er utav molntjänster?	
38	R2	Ja det gör vi, mycket	I-M
39	OI	Ja precis, får man fråga vilka ni använder i huvudsak? Till exempel Google, Amazon, liknande?	
40	R2	Vi använder i stort sett alla, vi är ju ett globalt, vi har 1400 siter	I-M

		globalt så det är, alla [skratt]. Men om du nämner hyperscalers där så, Google, AWS, Azure använder vi och sedan använder vi Kina-versionerna av dem eftersom… även har vi lite i AliCloud, några miljöer också. Men det stora kan man säga, de främsta miljöerna är AWS och Azure som vi använder	
41	OI	Precis, ja men super, och detta var då globalt?	
42	R2	Globalt	
43	OI	Ja precis super. När… ja det var längesen ni implementerade molntjänster då antar jag?	
44	R2	Ja, men vi flyttar mer och mer upp till moln och SaaS	I-M
45	OI	Ja precis. I din erfarenhet, vet du om någon av era leverantörer av molntjänster har utsatts för dataintrång som kan ha påverkat er? Så till exempel oj nu är det någon som har kommit åt vårt som, där ert ligger, eller liknande?	
46	R2	Nä det vet jag inte, det kommer mig, men vi ser att en del av våra kunder har blivit träffade så att säga men vi har ju, ja, vi har ju väldigt stor kundbas så att säga. Så det har vi ju sett, allt från ransomware till credential steal så att säga	I-M
47	OI	Precis, nä men det är bra…	
48	R2	Det är tyvärr den världen idag	
49	OI	Ja men precis, nä det är ju det. Det är väll att, man märker också mycket att man måste få ut det till alla så att alla förstår lite vad det innebär också, så oftast kan det vara lite det känns det som…	
50	R2	Jo men en sån attack går väldigt, väldigt snabbt idag, så det räcker med en 5-10 minuter	
51	OI	Ja, har ni några speciella policys, riktlinjer för det, när till exempel, shit nu kanske jag har gjort något fel här, en anställd till exempel, har ni något… jag vet ju till exempel att EU har väl en lag som säger att ni måste, att företaget i sig måste rapportera inom… nu kan jag inte tiden	
52	R2	Inom 72 timmar	
53	OI	Precis, har ni också något, på dem anställda att om det är någonting som är lite fishy här då måste ni rapportera det?	
54	R2	Ja, anställda har, vi har gjort så, att de anställda har flera olika möjligheter att kontakta oss, lite beroende på var dem är, via intranätet eller våra supportsystem och så. Och det är okej bara om man misstänker att kontakta oss om man inte, det är väldigt viktigt att bygga en coachande miljö så att även om du inte har något som	I-M

		absolut, som du inte förstått, som absolut inte, att man inte klankar ner på det utan att man är coachande för det är ju de anställda som är första indikatorn och det är viktigt att dem är med på banan i alla led. Som sagt det går så snabbt idag, speciellt om du möter nationer, det går väldig, väldigt snabbt	
55	OI	Visst är det så. Använder ni er utav några preventiva medel som till exempel lösenordshanterare eller att man inte får använda sitt eget USB-minne på jobbdatorn eller liknande?	
56	R2	Ja [skratt], jo det gör vi men vi är lite mer sofistikerade än så. Vi övervakar allting som stoppas in i datorerna via USB, så det är okej att ha ett USB-minne utan vi har full koll när det sticks in. Det är ju så ibland att… dem är smittade, antingen från företaget det kommer ifrån och så men det ser vi ju och hanterar och då isolerar den datorn inom någon sekund så att det inte sprider sig. Lösenordshanterare… har vi väl inte centralt till dem anställda, från grupps sida, sen vad varje division har det kan jag inte berätta och vet inte riktigt vad dem har. Men vi har, vad ska man säga, vi har, vi bygger permlösningar som är centrala password-lösningar och det är egentligen på kontot, så kontona byter password varje timme och roterar själv passworden, speciellt när du har systemkonton och så. Så även om du kommer över ett password på ett systemkonto så, en timme senare så är det passwordet, kan du kasta det typ, för att det roterar hela tiden. Så vi försöker att bygga sådana lösningar, speciellt på då, vad ska man säga, system till system kommunikation.	I-P
57	ANS	Jag har en liten fråga, är det någonting av detta som har blivit annorlunda efter pandemin eller har det alltid varit den standarden?	
58	R2	Det har inte med pandemin, utan det har med att, man kan inte hålla på med, det blir för mycket passwords att hålla reda på. Ska du hålla reda på just ditt, du har oftast ett standard användarkonto och sen om du har någon sorts adminrättigheter så att du har ett admin konto så separerar man accessen på då. Så jag menar om jag äger mitt användarkonto som jag använder varje dag så äger du inte ditt adminkonto så att man bygger, vad ska man säga, en tierad modell av olika konto. Sen finns det servicekonto då som är system till system, ska du då som applikationsägare ha koll på dem passworden till dina system så är det oftast 20-30 konton per system, och vad gör en människa då, jo dem skriver ju ner dem någonstans eller hur?	I-P
59	ANS	Ja precis	
60	R2	Det är ju helt omöjligt att hålla koll på i hjärnan. Sen kan du ha en passwordhanterare absolut, men oftast är det ju, stoppar du ju in privat passwordhanterare, det är ju inte jättebra heller, där du har dina bankkonto och sådana grejer så om du blir [hör inte 0:20:25]	I-P

		privat så blir du [hör inte 0:20:26] på företaget också. Så vad vi försöker nu är ju att ta bort hela det så att servicekontona är något maskinellt som bara sköts och roteras. Och sen så, det finns ju nya tekniker här med Windows 11 och så, att istället för att ha password så har du pin-kod istället och det sparas, allting sitter lokalt så den pinkoden är ju bara din, vi kanske inte ska det här i denna, hur det funkar men det är väldigt, väldigt säkert för att då kommer du ifrån password, lite på användarnivå. Så att där är massa ny teknik som hjälper till	
61	ANS	Och det är samma då för det här med USB som ni nämnde, det var samma innan pandemin, att ni kontrollera det?	
62	R2	Det är samma nu. Det är ju klassiskt, vad har vi… snart 55000 anställda, där är alltid någon som har en smutsig USB-sticka i världen eller, det är inte så att dem har det själva utan dem får ju från leverantörer, dem ska byta ritningar och allting, men oftast kommer inte stora grejer in där utan oftast stora grejer måste det sitta en fysiskt person bakom och hacka. Sen kan du ju få en, vad ska man säga, en väg in med ett script som ligger på en USB-sticka. Idag med den säkerhet som finns så är det väldigt, väldigt svårt, det är coolt i filmer och så men, det går absolut, du vet den här klassiska man går och kastar ut en massa USB-stickor utanför företaget, sen tar dem upp det och hittar, en blänkande fin USB-sticka och stoppar in den i datorn, det finns attacker som gått till så absolut, det är klassiskt. Men det använder man mer för att försöka testa användarnas utbildning, man trycker på användaren ganska mycket för cyberutbildning idag, allt från phishingattacker till, ja som ni sa innan med GDPR och nu kommer också Schrems 2 här från EU. Så idag får, vad ska man säga, IT användare väldigt, väldigt mycket utbildning. Sen så gör vi också fejkade phishingattacker internt, så vi skickar ut en phishingmail och sen ser vi vem som klickar på dessa och när dem då klickar på dessa och åker fast så att säga, så är där en länk till en utbildning och sen så flaggas den upp och så får dem ta phishingutbildningen en gång till. Man försöker att inte sätta dit dem, man försöker bara testa dem och coacha dem, det är viktigt	I-P I-U
63	OI	Ja men precis. Nä men det är jättebra.. tänker bara, ISO-Standarder är ju någonting jag antar att ni använder er utav också, är det några on the top of your head som du känner att ni använder som är mer relevanta än andra?	
64	R2	Det ligger ju närmare businessen, det ligger ju närmare kan man säga, fabrik och businessen så jag menar, ISO-9000, ISO-27000 och alla dem bitarna absolut finns det. Sen så, oftast så har vi inte direktförsäljning till kunder, vi säljer ju till kunder som sen säljer våra produkter men vi har säkert PCI DSS standarden någonstans och så vidare. Sen finns det rena, det är ju inte standarder på så sätt, men det finns SOC 2 regelverket som vi försöker att följa och	I-I

		andra, men det är mer kan man säga av kvalitetsskäl, så att vi säkerställer att vi fyllt i alla, vi har bockat alla rutor och sådana bitar. Men sen är det ju, GDPR är stort, data protection, skydda våra användare så att vi följer lagar och sådana grejer för att vi samlar ju, jag ser ju allt som händer i bolaget rent krasst, för vi samlar in all den datan, idag kan du ju spåra allt en användare gör och därför är det viktigt att följa de lagarna och skydda våra användare också. Det finns ju alltid chefer som vill övervaka sin personal och se, när öppnade han Outlook, öppnade han den 08:01 eller 08:30, när var han på jobbet, där finns tyvärr människor med sådana kontrollbehov och då får man säkerställa att dem inte har någon access så att vi håller dem… så är det ju, människor är olika och det är olika kulturer också.	
65	OI	Precis, jo men visst är det så. Vi kan hoppa lite till utbildningar då som du också touchade på innan… och då specifikt om informationssäkerhet då ju tänker vi väl, hur ser upplägget ut på dem, är det att ni har, är det till exempel att en utbildning när man börjar och sen så är det inget eller har ni… återgående utbildningar till exempel en gång om året eller liknande?	
66	R2	Våra utbildningar är så, det styrs utav ett HR-system så vi har implementerat ett nytt HR-system här nu för två års sedan och nu ligger kan man säga all utbildning, så jag som chef kan också se vilken av min personal som inte har gjort utbildning, så det får jag rapporter på det och går igenom det, så det är jättebra. Och sedan så finns allting integrerat, så vi… och sen så finns det extra utbildning. Men det funkar i stort sett såhär, om du klarar en phishingutbilning eller vi har, alltså utbilning runt vad är en muta, vad är inte en muta, sådana grejer, klarar du då de utbildningarna så är du clearad för 3 år, sen efter nästa 3 år så får du en uppdaterad version av den utbildningen. Och dem är rätt så sofistikerade för att du svarar först på frågor, så när du svarar fel på en fråga, då läggs det utbildningskapitlet till som du svarade fel på, så det är rätt skönt om du skall ta om någonting att du kan svara på några enkla frågor så slipper du sitta en timme och köra utbildningen eller två, så det är rätt trevliga saker. Sen så jag, jag sitter ju och testar en massa utbildningar så jag har ju en hel hög, men jag sitter med i vårt Global Security Council så vi testar ju en hel del utbildningar också	I-U
67	OI	Testar och godkänner att de känns som att de är relevanta?	
68	R2	Ja och sen, vi vill ju hela tiden, man vill ju hela tiden ge användarna mer men man får vara försiktig så att dem inte sitter i bara utbildningar och kan jobba också lite. Sen så Cyber Security avdelningen har ju dessutom ytterligare utbildningar som vi kör, vi har ju utbildningsprogram där, för att idag gäller det ju att vara ajour hela tiden. Så vi har ju ytterligare… vi har djupare utbildningar än, vad ska man säga, användar gänget	I-U

69	OI	Precis, men det låter väldigt bra. Så ungefär, ja vad var det du sa, 3 år håller en licens och sen så	
70	R2	Nä 3 år håller en utbildning som då går som phishingutbildningen, sedan får du ta om den. Men har inte utbildningen förändrats så mycket så och beroende hur du svarar på frågorna så, man gör ju provet först lite, det är det som är lite roligt med dessa utbildningarna	I-U
71	OI	Ja men det är ju ändå väldigt smidigt, ifall de ändå har rätt bra koll så kanske man inte ska	
72	R2	Tänk om man hade haft det på, så mycket studietid ni hade sparat [skratt]	
73	OI	Gud ja, det hade varit otroligt [skratt]	
74	R2	Bara slippa plugga de veckorna [skratt]	
75	OI	Vi får hoppas på att det kommer kanske [skratt] … Har ni utvecklat några av era utbildningar till, förändrat dem lite på just att man har börjat jobba hemifrån och att hemarbetet har ökat?	
76	R2	Ja absolut, absolut har vi det	I-U
77	OI	Har du något konkret exempel på ungefär hur det har ändrats? Ifall ni har lagt fokuset på något annat eller om det är helt	
78	R2	Nä men det är bara att man säkerställer, ja och nej, man säkerställer att de kapitel är med, bara för att det är ditt hem så kan du inte lämna din dator på, man tänker att man är hemma, det blir ju klassiskt, man står och lagar mat samtidigt som man halvt jobbar, speciellt om man har ungar, så försöker man…	I-U
79	OI	Kanske trycka lite på att, bara för att ni är hemma så ska man kanske inte vara helt hemma kanske	
80	R2	Nä exakt, men inte mer än så, bara ta upp det som ett exempel på arbetsplats mer	I-U
81	OI	Ja men precis.	
82	R2	Men mindsetet har ju, att jobba hemma, har ju, vad ska man säga, det här tråkiga som har hänt har nog lärt en hel del i management att det funkar ganska okej att jobba hemifrån. Det är många som har lite kontrollbehov att vilja ha alla på kontoret så mindsetet har ju definitivt ändrats	
83	OI	Ja, det var en fråga jag glömde att fråga innan som vi kanske kan ta nu, du sa innan att ni har haft möjlighet att jobba hemifrån tidigare också, hur skulle du säga, hur många ungefär var det, procentuellt från företaget som jobbade hemma? Eller om du säger din, i ditt	

		team kanske så kan vi ta det därifrån?	
84	R2	Ja men det är ju…	
85	OI	Testade alla på det?	
86	R2	Ja men vi har ju många, det är ju livet, ni är ju unga och pluggar sen så när man kommer in 25-30 så blir det ju oftast några barn och det är svårt i början när de ska på dagis och är sjuka hela tiden och så vidare. Så de beror lite på vart man är i livet, men jag brukar godkänna alltid när någon frågar av en giltig anledning så är det bara att köra. Så jag skulle säga att på en vecka så, ja… om vi inte tar Covid då, så är det kanske 10-20% som jobbar någon dag hemma, det beror lite på. Jag har en kille, han har 12 hästar och dem ska föla och så, då får han köra hemma den veckan [skratt]	D-FC
87	OI	Ja det är förståeligt [skratt]	
88	R2	Ja men det är viktigt att kunna kombinera privatliv och arbete så, det är viktigt för mig iallafall. Men som sagt 10-20% över en vecka och av då, kan man säga, normala kontorspersonalen då, inte dem som jobbar i en 24/7 leverans eller något sådant	D-FC
89	OI	Nä precis… och om man går till idag, nu har man börjar kunna jobba på kontoret också ju	
90	R2	Det är samma, vi har samma procent ungefär	D-UC
91	OI	Ja men suveränt. Super super, jag tänker, vi har ju även haft några, vi har några teorier i vår uppsats också så nu är det väl lite frågor som är lite mer, lite enkel svarade kanske, som	
92	R2	Är det ja eller nej frågor eller?	
93	OI	Ja nä inte riktigt men nästintill, men ja det är bara så att du vet. Så då kommer dem, hur välinformerade skulle du säga säga att anställda på företaget är gällande IT-Säkerhet? Och då tar man väl moget, mindre moget och inte moget, brukar man väl ta då som en liten skala	
94	R2	Kan väl säga att vi är moget där sen är där säkert anställda som jobbar i en fabrik som, vi köper ju mycket bolag, vi köper 1-2 bolag i månaden, det tar lite tid att få in dem i rutinerna och få ut centrala system. Så där är absolut någon som aldrig har fått någon utbildning också, men sen är där ju många som är experter så vi är nog moget och de utbildningar som finns är väldigt, väldigt mogna	T-T
95	OI	Ja nä men det låter, från intervjun låter det som att ni är väldigt mogna skulle jag säga, helt klart. När ni har gett utbildningar inom informationssäkerhet, har ni märkt någon skillnad i säkerhetsbeteendet från arbetaren som kanske gjort just den	

		utbildningen då? Ifall ni har… ni har koll på vad dem gör	
96	R2	Absolut, absolut, vi mäter ju phishing eftersom att vi skickar ut fejkade phishing, vi mäter alla divisioner individuellt och de som har utbildat och promotat dem har ju mycket, mycket bättre resultat än övriga, så det är ganska tydligt vem som har gjort ett gott jobb och vem som gjort ett mindre gott jobb på dem bitarna, så det syns.	T-T
97	OI	Ja men det är bra, annars hade man kanske inte gjort det. har ni märkt någon skillnad i medarbetarnas säkerhetsbeteende i samband med flytten till hemarbetet? Till exempel att nu helt plötsligt så står deras dator igång utan att de gör någonting ett tag eller någonting annat liknande?	
98	R2	Initialt var det ju det, eftersom att många var ovana vid att jobba hemma och sen så hade vi problem initialt eftersom att det gick över en dag, över en vecka från att jobba till att vara hemma, så initialt kom det säkert en massa felkoder och sådana grejer för vissa användare som dem trodde att, du vet. Men förutom inkörningproblemen där i början som var relativt smidiga med den här storleken på företaget, så nä det kan jag inte säga att det har varit något	T-T
99	OI	Nä, det är ju väldigt skönt… Hur arbetar ni med konfidentialitet, använder ni er utav behörighetskrav för känslig information eller är det något annat sätt ni arbetar på, just på det sättet?	
100	R2	Det är många olika, vi klassificerar data enligt, vad ska man säga, en skala, så alla dokumenten och allting blir klassificerade. Sen har vi ju rena röda nätverk som vi säger, röda nätverk är ju att dem har ingen access in eller ut utan dem finns bara	T-C
101	OI	Så ingen alls?	
102	R2	Ingen alls, utan det nätverket finns bara på den siten, den har ingen internetaccess, ingenting, och de jobbar ju där. Sen är det ju, vad ska man säga, sen har vi ju, det är också vilken chef du är, vilken information du får tillgång till och så vidare. Så vi har många olika sätt vi skyddar känslig information	T-C
103	OI	Men det är ändå lite sådär teambaserat, att vissa teams kanske har lite annorlunda riktlinjer än andra? Sen har man kanske några andra som alla supportar	
104	R2	Ja, vad ska man säga, vi har våra utvecklarteam, de jobbar med en produkt så dem kanske inte är samma linje, men där finns ett produkt IT-Council som driver Cybersäkerhetsarbete också och informationssäkerhet. Men utvecklare är ju glada att göra det på sitt sätt [skratt] … det är därför man vill ha dem också, det är tyvärr så att min vill ha dem för att dem är dem, så kommer dem	T-C

		och, nä ni ska köra Windows nu annars så eldar dem upp huset typ och så vill dem köra sin Linux version, nä vi ska inte köra Ubuntu vi ska köra Mint och vi ska köra, du vet. Men det är härligt också, de är ju oftast hjärnorna så man får vara snälla mot dem	
105	OI	Precis, dem har väll väldigt ofta bra koll… Nä men det är bra, hur arbetar ni för att behålla den här integriteten på datan då, är det så att, ja som du sa innan att vissa grejer kommer ju ingen åt, men är det då att chefen på en avdelning bestämmer vem som har behörighet för vad? Till exempel den här personen kan korrigera eller?	
106	R2	Inte, nä det har inte med linjeägande att göra utan det har med rollen i sig själv. Så till exempel, jag kan vara chef över Cybersäkerheten men jag kan kanske inte ha access till all data. Jag vill också inte oftast ha allt på min access som chef för att jag står på LinkedIn som ansvarig för Cybersäkerhet på Assa Abloy	T-C I-P
107	OI	Ja det är en prime target	
108	R2	Ja där är jag en target och eftersom att jag är chef så är jag mindre teknisk än min personal så det gör mig därför också till en target. Men det är rollen som avgör vilken access du har till vilken data och känslig information	I-P T-C
109	OI	Ja så specifikt du då har till exempel, inom Cybersäkerhet, ganska hög generellt, sen om du inte vill ha det för att du inte behöver	
110	R2	Ja, men jag kan absolut få den men jag har valt att inte access till många saker	I-P
111	OI	Ja precis… Hur ser tillgängligheten ut, har ni till exempel allt sparat på ett, är allt tillgängligt på ett och samma ställe när det handlar om kanske ett system eller är det uppdelat lite så att man inte kan komma åt allt på ett och samma ställe, om du förstår vad min fråga var där?	
112	R2	Ja men då får man ju tänka vilket system det är, vi klassificerar ju olika system med olika klassificeringar, vi har något som vi kallar kronjuveler, crown jewels, det är dem viktigaste applikationerna för varje division och då definierar dem det, kan vara interna affärssystem, det kan vara produkter. Så man börjar att jobba så och sen så skyddar man, säkerställer man att där finns ett skydd som är till klassen av, jag menar skulle det här bli infekterat det här, så stannar alla våra fabriker till exempel. Det är kanske inte hela världen men att starta upp alla fabriker igen så kan det kosta x-antal 100 miljoner så det är det som är problematiken och då gör man en riskbedömning efter systemet. Något som vi har som mål är att om alla de här systemen då, som är crown jewels då, alltså vi har ju flera, flera tusen applikation, men dem som kritiska för vårt levebröd så att säga, då har vi ett mål att om dem blir träffade av	T-C I-P

		någonting, av någon anledning, att dem ska vara uppe och rulla inom 24 timmar och det kräver ju då att man har till exempel om vi utgår från säkerhets perspektivet, det kräver ju då att man har sin backup offline. Så att om en hackare kommer in att dem inte kan vara där i 6 månader och komma in i backupen så att sen när du lägger tillbaka backupen så lägger du tillbaka hackaren också. Så vi massa olika sådana saker där runt om systemen. AD är ju ett klassiskt sånt här där alla rättigheter finns, då har man en offline backup av AD. Oftast när man blir [hör inte 0:39:31] stor då så vill man ju reseta alla konto i hela företaget och hela AD:t, det är viktigt att träna också på sådana saker	
113	OI	Ja det är intressant	
114	R2	Det är väl det som gör att nere så länge, att folk som, jag vet inte, ni såg väl Coop här som blev [hör inte 0:39:49] för något år sedan	
115	OI	Ja precis	
116	R2	Dem tappade ju alla kassasystem och så, det kan hända vilket företag som helst, det är bara otur och det är ju hur man tränar, är hela AD ägt och har man aldrig byggt för det så att säga så blir man nere väldigt, väldigt länge. Har man byggt för det, det är ju inget kul, men man kan ju hantera situationen och komma upp snabbare.	I-P
117	OI	Ja men precis. Super… har, om det här med konfidentialitet, integritet och tillgänglighet, är det någonting som ni har skiftat hur ni arbetar på det på grund av flytten till hemarbete eller från att Covid-19 släpptes eller det har alltid varit samma där också?	
118	R2	Jag tror att det har hjälpt att Covid-19 hände för att det har gått snabbare och man har, vad ska man säga, exekverat snabbare för att det har varit mer fokus på det. Sen tror jag inte det har skilt sig något nämnvärt i vad man har gjort i jämfört, det känns bara som att det har gått snabbare, en känsla bara, det är svårt att mäta men det känn som om det har fått fokus och i med Covid-19 så stannade världen upp och tänkte på lite säkerhet i två år. Jag tror att det är mer att, vad ska man säga, världen förändrades och det kom upp på agendan högt uppe, vilket gjorde att det fick mer mandat och drogs igenom snabbare, sådana här projekt	T-C
119	OI	Det är intressant men… har företaget du jobbar på då, lagt mer resurser eller en högre budget de senaste åren på IT-säkerheten?	
120	R2	Nä det tror jag inte utan det har bara kommit längre upp, där är ju alltid så 200 grejer du vill göra och sen så har man bara flyttat upp det i den kategorien. Det är inte så att det inte fanns något innan, det är bara att man har jobbat mer med det, man har blivit bättre på det	D-IT

121	OI	Ja men det är intressant, så ur det perspektivet så var ju Covid en bra grej	
122	R2	Om man ska säga att Covid var en bra grej överhuvudtaget, men ja, det ger ju ett fokus på annat	
123	OI	Jo men precis så är det ju. Ja, nä jag har nog inga fler frågor faktiskt, tycker vi har tagit det mesta, Alex (ANS) har du någonting du vill flika in på eller?	
124	ANS	Nä det var väl mer av en observation, det verkar ju som att ni redan var ganska adapterade till remote work innan, så den här flytten till hemarbete kanske inte var så stor påverkan på er som andra företag	
125	R2	Nä kanske inte men vi är ju ett stort globalt företag så vi har ju, vad kan man säga, vi har ju dem här systemen redan så att säga. Det var bara att vi var tvingade till att expandera dem väldigt, väldigt snabbt	D-FC D-UC
126	OI	Jag tror nog att dem flesta som blivit mest påverkade är nog dem medelstora företagen som ändå har tillräckligt många anställda där man måste, verkar det som… men det är väldigt intressant	
127	R2	Men samtidigt om du skall slå på att 30000 går hem, det blir ju ändå liksom från fredag till måndag, så okej, okej grabbar hur gör vi detta [skratt]. Det är ju inte bara så att dem ska ha någonstans att logga in i världen, dem ska ha snabb access också, om du sitter i Mallorca eller du sitter i Sydamerika, det är inte så att de kan logga in till Lund precis utan du måste ju leverera det globalt snabbt. Det är ju därför man väljer då cloud som bärare	D-UC I-M
128	OI	Jo men precis och det kommer väll mer och mer har man märkt, känns som att alla vi har intervjuat har, använder sig utav molntjänster idag faktiskt	
129	R2	Ja absolut, sen får man ju vara försiktig för att det kan, har man glömt någonting så sticker kostnaden iväg, lika snabbt som det blir billigt, lika snabbt blir det jävligt dyrt [skratt]	I-M
130	OI	Jo precis [skratt]. Det är ingenting du heller vill lägga till R2? Någonting du funderar på?	
131	R2	Nä jag har bara frågor till er	
131	OI	Nä men då skall vi inte ta upp mer av din tid	

Appendix C - Transkribering intervju 3

Transkriberingsprotokoll
Organisation: Grade AB **Intervjuobjekt:** Respondent 3 **Starttid och plats:** 5 Maj 2022, Klockan 09:30, via Videomöte. **Medverkande:** Respondent: Respondent 3 (R3) Intervjuare: Alexander Nilsson Sump(ANS) och Oliver Ilijason(OI)

Rad	Person	Fråga/Svar	Kod
1	ANS	Då kör vi igång. Vi kan börja med lite före Covid-19 pandemin, det var någon möjlighet till hemarbete då?	
2	R3	Det hade vi, Samma tekniska möjligheter före pandemin som under pandemin men att möjligtvis dem sociala delarna gjorde att det inte var lika accepterat att jobba hemifrån innan pandemin kanske utan man förväntades att finnas på kontoret.	D-FC D-UC
3	ANS	Okej, men möjligheterna som sagt låg där redan?	
4	R3	Absolut.	
5	ANS	Mm, okej! Hur såg säkerhetsåtgärderna ut då innan Corona om man skulle jobba hemma?	
6	R3	Säkerhetsåtgärderna är ju, Vi har VPN för att komma åt de tekniska miljöerna och sen är allt lösenordsskyddat såklart där vi använder en lösenordshanterare, 1Password, där vi har egna inlogg. Sen har vi väl, vad ska man mer säga, det var säkerhetsrutinerna innan om man ser till hur vi hanterar våra utvecklingsmiljöer och tillgång till våra kunders databaser och installationer.	D-FC
7	ANS	Mm.	
8	OI	Och det var då innan pandemins start tog jag det som?	
9	R3	Ja precis.	

10	ANS	Då har vi pratat lite om före pandemin precis, och nu ska vi gå till under pandemin. Var det så att samtliga skulle börja jobba hemifrån när organisationen beslutade sig för att gå över till hemarbete?	
11	R3	Ja det resonerades från början som så att alla som, i alla situationer där vi inte behövde vara på jobbet så skulle vi arbeta hemifrån, och på vårt företag behöver i princip ingen vara på jobbet då det tekniska möjligheterna redan fanns, och vi har inga kunder som kommer till oss om det inte är planerat sen tidigare.	D-UC
12	OI	Jag tänker bara flika in där, fanns det något som gjorde att ni ibland tog er in till kontoret ändå, du sa innan att om man inte var tvungen att vara på kontoret, men fanns det någon gång ni behövde åka in, och av vilken anledning isåfall?	
13	R3	Jag kan nog bara svara för mig själv isåfall men för min del åkte jag in till kontoret när det var tråkigt att sitta hemma eller om jag hade ett möte med en kollega som jag tyckte var bättre att ha i verkligheten än på nätet.	D-UC
14	OI	Ja, perfekt.	
15	ANS	Fanns det, du sa att ert arbete i princip kan skötas på distans, var det någon anställd över huvud taget som var tvungen att stanna på kontoret under denna perioden?	
16	R3	Om det var någon så var det nog beroende på att de inte haft möjlighet eller kunskap att använda VPN, tror jag.	D-UC
17	ANS	Alright, var det någonting som fortsatte under pandemins gång eller det fasades ut så folk lärde sig använda VPN tillslut?	
18	R3	Ja, jag tror det iallafall, jag jobbar inte med att hjälpa medarbetare med det, men jag tror att alla kunde jobba hemifrån, det är möjligt att det finns vissa system som kräver att man sitter på kontoret, men jag tror inte det Jag hoppas alla fick möjlighet att köra VPN och jobba hemifrån iallafall.	D-UC
19	OI	Så i stor grad jobbade de flesta hemifrån!	
20	ANS	Hur känns det generellt, är de flesta positivt eller negativt inställda till hemarbete?	
21	R3	Jag tror att till stor andel är man positivt inställda på hemarbete, i vår organisation.	D-UC
22	ANS	Mm, tror du det kan ha någonting med effektivitet att göra?	

23	R3	Det tror jag att det kan ha med effektivitet att göra, du kanske kommer till det, men jag tror det har och göra med vad man jobbar med också. Om man jobbar med programmering till exempel så tror jag att en lugnare miljö med mindre störande objekt kan vara med effektiv än en delad kontorsmiljö. Medans för min del där jag jobbar mycket med kontakt med mina kollegor så blir det inte mer effektivt.	D-UC
24	ANS	Okej, jag förstår.	
25	OI	Jag kan bara flika in där också, i och med att du sitter mycket med kollegor, har du haft svårt att hitta tider att kunna boka in tider med en kollega typ sista minuten grejer eller har du känt att det har man löst? Just av anledning att man varit hemma.	
26	R3	Det har nog alltid löst sig i princip, det är lättare att veta vem som jobbade när alla var på kontoret, medans man numera i och med att det är flexibelt att jobba hemifrån så blir också tiderna man jobbar mer flexibla så ibland vet man inte om de jobbar eller hämtar ungarna på skolan eller är hos tandläkaren osv. Men jag känner att för min del har det inte varit några stora problem med det.	D-UC
27	OI	Nä men bra, det är ju skönt.	
28	ANS	Alright, och säkerhetsåtgärderna gick vi över lite, de har, de ändrades i princip inte från att ni var på kontoret till att ni jobbade hemma?	
29	R3	Nä, vi har i princip haft samma säkerhetsrutiner sen innan pandemin och även efter, alltså samma rutiner hela tiden.	D-IT
30	ANS	Ska vi se, om ni då har använt samma säkerhetsåtgärder, har ni känt något ökat tryck på liksom försök till dataintrång eller liknande på den enskilde anställda i jämförelse med kontoret?	
31	R3	Nej, vi har egentligen inte uppmärksammat något direkt försök till några sådana attacker, men än att, jag kan inte minnas om detta var innan eller under pandemin, men det är vissa som fått något mail som var adresserat han som är VD på företaget med någon länk. Men det är nog den enda attacken jag fått nys om från organisationen.	D-IT
32	ANS	Great, men det, i det fallet då är det samma säkerhetsrutiner hur man hanterar sådana mail?	

33	R3	Ja men precis, det är ju klart svårt att ha rutiner för allt, men i det fallet så kontaktade den drabbade personen VDn och frågade om det verkligen var han som skickade den länken till honom, och när det då inte var det så meddelade VDn via mail eller Teams att det kommit ett sånt mail och att man ska vara uppmärksam, men det är ju, som jag sa innan att det är svårt att vara förberedd på allt.	D-IT
34	ANS	Ja klart.	
35	OI	Kan bara flika in där också, är det så att ni har någon person eller liknande som har hand om sådana situationer hur man ska hantera, nu kom det in ett mail där någon sa att hen var VDn, finns det någon kontaktperson för det eller det är något man löser internt mellan drabbade parter istället?	
36	R3	Jag tror faktiskt snarare att man sköter det mellan varandra, det finns ju personer som jobbar mer med IT-miljön som datorer och våra servers som man kanske skulle kunna ta hjälp av, men det finns ingen uttalad som jobbar med den typen av arbete på vårt företag.	D-IT
37	OI	Nä, super.	
38	ANS	Perfekt, då går vi vidare lite och kikar lite på molntjänster, är det något ni använder er utav?	
39	R3	Vi använder oss utav flera molntjänster, vi använder oss av till exempel Jira, det är ett ärendehanteringssystem, och de ägs av Atlassian, och där använder vi även Confluence som är ett intranätsystem. Sen använder vi oss av Trello som också ägs av Atlassian, det är en sån här board där man kan flytta lappar mellan olika kolumner. Vi använder Zendesk för ärendehantering, det är ju en molntjänst. Office 365, Microsoft, Teams för kommunikation. Så flera.	I-M
40	OI	Har ni era egna servers för data eller sker det också via en molntjänst eller liknande?	
41	R3	Ja det är också en typ av molntjänst, det är ett företag i Malmö som har våra servers i en serverhall.	I-M
42	ANS	Alright, och då får ni access till molntjänsten på något sätt kanske?	
43	R3	Precis, det är ju då den VPN-tjänsten.	I-M
44	ANS	Okej, ska vi se…	

45	OI	Vet du med dig ifall ni har blivit kontaktade någon av era molntjänster som berättat att nu är det någon som kommit åt vår data, och er data skulle kunna finnas där också. Eller det har alltid skötts sig bra och aldrig varit någon sån kontakt?	
46	R3	Inte vad jag vet, jag har inte hört talas om något sånt.	I-M
47	OI	Nä, super.	
48	ANS	Perfekt, då täckte vi det och går vidare, du nämnde ett par stycken innan, lite preventiva medel som VPN och du sa att ni hade lösenordsskydd också?	
49	R3	Lösenordshanterare ja, där alla konton för att komma åt lösenord man behöver ha tillgång till.	I-P
50	ANS	Är det så att datorer ni använder har någon speciell blockering av minneskort eller liknande?	
51	R3	Det vet jag inte om jag vet, nä det vet inte jag. Inget jag hört talas om iallafall. Vi beställer ju våra datorer från samma ställen där vi har servrarna och det är möjligt, men jag kan inte svara på det faktiskt. Känner inte till det.	I-P
52	ANS	Då ska vi se, vi har pratat lite om riktlinjer, finns det några satta riktlinjer för att just motverka dataintrång?	
53	R3	Ja, vi har dokument för IT-säkerhet och katastrofplaner och sånt, där finns det ju instruktioner för hur man ska hantera sin data och sin hårdvara och så.	I-I
54	ANS	Är detta något som har förändrats eller det har lagts till något sen ni flyttade till hemarbete?	
55	R3	Det har nog lagts till saker i dem dokumenten, säkert både pga hemarbete men även mer kunskap om de här hoten osv.	I-I
56	ANS	Och det är då något som alla på företaget har tillgång till? De här dokumenten.	
57	R3	Ja	I-I
58	ANS	Perfekt, vi går vidare. Kommer väl in lite på det då, indirekt. Utbildningar då, hur hanterar ni utbildningar angående IT-säkerhet utöver då de skrivna dokumenten?	
59	R3	Jag tror inte vi har några utbildningar alls kring det. Så som vi uppmanas att ta del av dokumenten är via en online-utbildning eller flera onlineutbildningar. Och via den så får man först ladda ner dokumentet, och efter det får man tre till fyra frågor som baseras på vad som står i dokumentet.	I-U

60	ANS	Okej!	
61	R3	Men det är väl en typ av utbildning, men ingen annan sådär, det är ingen som kommit till oss och presenterat något för oss.	I-U
62	ANS	Nä precis, är detta då att man gör detta en gång eller återkommande?	
63	R3	Tanken är att man ska göra detta varje år, så man får ett certifikat som gäller ett år, sen vid nästa medarbetarsamtal så ska man helst ha gått utbildningen igen.	
64	OI	Ja det låter ju bra.	
65	ANS	Vet du om det är något, okej så utbildningen är baserad på dokumenten, så någon skillnad där är ju då det du redan nämnt på flytten till hemarbetet då tänker jag. Vi ska se, märks det att det har lagts mer eller mindre tid på detta i och med flytten jämfört med andra utbildningar?	
66	R3	Ja det har det nog faktiskt, men jag vet inte om motivationen till det är just hemarbete eller om det är omvärldsläget som förändrats senaste åren. Som jag sa tidigare så tror jag att kunskapen om vad det finns för olika hot har ökat för alla människor. Men det kan vara lite blandat kanske, i och med att alla tar med sin hårdvara och sitter hemifrån så måste man ju ännu mer göra folk, att de förstår vad de har ansvar för när man tar hem det.	I-U
67	ANS	Precis, har du något att tillägga, Oliver?	
68	OI	Nä, det låter rimligt. Det är svårt att säga att bara pga man jobbar hemma så lägger man mer tid på IT-säkerhetsutbildningar och liknande. Det kan nog vara många faktorer. Till exempel nu med Ryssland osv kan man tänka sig att det blir ännu mer tryck.	
69	R3	Jag tror det beror mycket på vad man har för typ av arbete också, och liknande branscher som den jag jobbar i eller andra mjukvaruföretag så kan den mjukvaran vara mycket mer känslig än vår är. En utvecklare i vårt företag sitter ofta inte med kunders känsliga data, det är möjligtvis deras mailadresser och liknande. Medans andra företag kan ha väldigt mycket känsligare data.	I-U
70	OI	Ja men så är det säkerligen, förövarna går för de som man vet om har känslig data.	

71	ANS	Vad bra, ska vi går vidare. Nu har vi pratat lite om utbildningar och säkerhetsåtgärder och så, jag tänker ifall du har en bild av hur medveten och kunnig en gemene anställd på ditt företag är inom just IT-säkerhet?	
72	R3	Gud det är svårt att svara på, I och med att hälften är mjukvaruutvecklare är hälften väldigt informerade och andra hälften kanske begränsat informerade. Så om man kan svara lite både och på det?	T-T
73	ANS	Såklart, men de har alla samma säkerhetsförutsättningar och utbildningar?	
74	R3	Aa, alla får samma typ av dokument och utbildning att läsa igenom samt att alla använder samma verktyg för att hantera lösenord och koppla upp sig till servers och sånt.	T-T
75	ANS	Super. Ska vi kika, är det så att ni har märkt någon skillnad på medarbetarnas säkerhetsbeteende då i samband med flytten till hemarbete?	
76	OI	Kan det vara att till exempel i början när man inte stängde ner sin dator vilket gjorde att vem som helst kunde komma och kolla på den?	
77	R3	Ja kanske, men det är svårt att svara för någon annan när det går hemma.	
78	OI	Det förstår jag, men om du svarar mer för dig själv?	
79	R3	Ja alltså jag låser min dator, men det är mest för att mina barn inte ska göra något. Vi gick igenom innan pandemin inom utvecklingsavdelningen att alla också alltid skulle låsa sin dator innan man gick därifrån och för min del fick man mer rutin på det då och att det hänger med en hem. Jag trycker alltid på WIN-L när jag reser mig upp.	T-T
80	OI	Ja precis, då känns det ändå som att ni haft riktlinjer sen tidigare hur ni ska hantera detta.	
81	ANS	Vi kikar vidare lite på Konfidentialitet, använder ni er utav behörighetskrav för känslig information? Att alla inte har access till all information	
82	R3	I den mån vi gör det så gör vi det med kunder servers, databaser. Där har de utvecklare åtkomst fullständigt. Jag kommer inte åt detta då jag inte har de lösenorden. Varje utvecklare har individuella konton som man kommer åt servrarna så det inte finns något gemensamt konto.	T-C
83	OI	Så man kan alltid se vem som gjort vad osv?	

84	R3	Ja precis, och till dem när man loggar in hos kundernas installationer, alltså i gränssnittet i vårt system så ska man använda ett eget konto. I den mån det finns gemensamma konton så hanteras det genom vår lösenordshanterare men använder man det så får man inte samma log på vem som använt kontot.	T-C
85	ANS	Men detta är något ni alltid använt er av och inte ändrats på grund av flytten till hemarbete?	
86	R3	Det har inte ändrats på grund av flytten hem, utan det ändrades innan det. Det har blivit säkrare under de senaste åren, men sen finns det andra system som behandlas liknande där jag inte kommer åt, exempelvis löner och anställningsavtal.	T-C
87	ANS	Precis, och det knyter an lite till nästkommande som är integriteten till datan ni erhåller. Vi pratade om behörighetskraven, men finns det något annat sätt ni skyddar den datan ni använder?	
88	R3	Den datan som bedöms vara känslig i våra system är krypterad. Så att vi inte kan läsa utan att göra ett mindre intrång vilket isåfall skulle loggas om vi skulle få för oss att göra något sådant. Så datan är krypterad med en nyckel.	T-C
89	ANS	Alright, och detta återigen, är det något som förändrats?	
90	R3	Nej, det har mer med GDPR att göra än något annat.	T-C
91	OI	Var det något ni fick lägga mer tid på under när GDPR tog över 2018?	
92	R3	Ja, då fick man på ett helt annat allvar se över rutinerna man har.	T-C
93	ANS	Har du något mer att inflika med, Oliver?	
94	OI	Nä har jag det? Tror faktiskt inte det. Du sa att tillgängligheten att jobba hemifrån har varit lika bra innan som efter. Det enda jag funderar på är hur det ser ut idag, sitter ni och jobbar mest hemifrån fortfarande eller sitter ni hellre på kontoret?	
95	R3	Det är ju helt frivilligt numera, eller det kanske jag inte ska säga. Man önskar nog att vi är tre dagar i veckan på kontoret, men jag tror de flesta på min avdelning jobbar en eller två dagar på kontoret och resten hemma.	T-C
96	OI	Ja, försöker ni komma överens om vissa dagar ni jobbar på kontoret tillsammans, eller man åker dit när man vill utan att egentligen behöva synka det med någon annan?	

97	R3	Vi har nyligen kommit överens om en dag där alla som kan ska vara där. Och det lutar med att det blir mer vanligt att vi gör så, att man kan komma överens om någon dag till.	T-C
98	OI	Ja men precis, Jag har nog inte något mer att tillägga nu faktiskt.	
99	ANS	Jag har en liten sista fråga, Är det så att ni har haft problem med tillgängligheten, exempelvis att VPN-tjänsten strulat eller att ni inte haft access till den data ni behövt när ni jobbat hemma?	
100	R3	Nä det kan jag inte minnas att det varit några tekniska bekymmer. Vissa har haft lite problem med att få fel på sin VPN klienten men det har också löst sig ganska snabbt. Ett problem vi hade precis i början var att vi hade för lite licenser till VPN-klienten. Som jag sa innan så förväntades man vara på kontoret och antalet som behövde använda VPN var ju kanske max en eller två, men när plötsligt alla skulle använda VPN-tjänsten så hade vi endast cirka 5 licenser för hela organisationen. Så under någon dag kunde vi inte arbeta så enkelt då vi behövde köpa in fler licenser.	T-C
101	OI	Ja. Nej men det är ju bra, vi har täckt allt vi vill ha nu tror jag.	
102	ANS	En sista generell fråga, är det något gällande IT-säkerhet som du känner förändrats åt det bättre eller sämre sen du började jobba hemma?	
103	R3	Nej det har jag faktiskt inget bra svar på.	
104	OI	Då så, då säger vi så och jag stänger av inspelningen.	

Appendix D - Transkribering intervju 4

Transkriberingsprotokoll
Organisation: Företag D **Intervjuobjekt:** Respondent 4 **Starttid och plats:** 10 Maj 2022, Klockan 15:00, via Videomöte. **Medverkande:** Respondent: Respondent 4 Intervjuare: Alexander Nilsson Sump(ANS) och Oliver Ilijason(OI)

Rad	Person	Fråga/Svar	Kod
1	OI	Då tänker jag att vi börjar fråga om vilket företag du arbetar på?	
2	R4	Mm, Know e AB heter det.	
3	OI	Snyggt, och hur lång erfarenhet har du inom IT-branschen?	
4	R4	Då ska vi se här, 25 år.	
5	OI	Aa, snyggt. Det var allt vi behövde därifrån, lite innan vi börjar igång på riktigt. Därför gör vi det nu också! Angående före Covid-19 pandemin kommer vi börja med, och då tänkte jag fråga om ni på Know e hade möjlighet till hemarbete före Covid 19?	
6	R4	Alltid, yes.	
7	OI	Mm. Hur såg de möjligheterna ut, var det så att de anställda satt mycket hemifrån eller var det bara ibland eller sporadiskt?	
8	R4	Men vi har ju alltid haft väldigt fria arbetstider att jobba när man är som mest kreativ och det har gjort att förutsättningarna sett ut att man har arbetsplatsen någonstans mobilt med sig. Så det var riggat för det.	D-FC
9	OI	Mm, precis. Säkerhetsåtgärderna, hade ni några riktlinjer för det till exempel att låt oss säga att man har en jobbdator och att man bör se till att man stänger ner den när man går därifrån? Eller det har kanske inte funnits några direkta riktlinjer sen innan?	
10	R4	Nej alltså vi har alltid haft en bra hygien i det. Alltså med inloggning och utloggning, sen har vi alltid haft separata kontorsmiljöer som vi kan vara hur dumma i som helst egentligen	D-FC

		utan att något skulle kunna ske. Sen att ta sig upp i våra miljöer vi jobbar i är VPN-bundna.	
11	OI	Ja, det är grymt. Vad skulle du säga generellt hur de anställda jobbade, var det generellt att vissa jobbar 2 dagar i veckan, 3 dagar i veckan eller helt och hållet 5 dagar i veckan? Alltså både då hemifrån och kontoret.	
12	R4	Vi höll kontoret öppet under hela pandemin, men däremot var det under perioden som samhället var som mest utsatt, då var vi mer eller mindre nedstängda även om vi faktiskt inte officiellt var det. Nästan alla jobbade konstant hemifrån under den perioden.	D-UC
13	OI	Ja, och hur såg det ut innan Covid? Såg det ut på liknande sätt?	
14	R4	Nej, alltså innan Covid så, vi är ett socialt gäng och arbetade också på det sättet. Inte för att det var något krav på kontorsarbete, men utan att det var så man ville jobba och man tyckte det var kul att träffas.	D-FC
15	OI	Förstår, man ville det helt enkelt! Då går vi över till under Covid-19 pandemin. Du sa att ni hade kontoret öppet, men beslutades någon form av att man bör jobba hemifrån, eller var det helt och hållet att man fick ta sitt egna initiativ till det?	
16	R4	Nej men vi rekommenderade hemarbete.	D-UC
17	OI	Ja, och det var då ungefär när folkhälsomyndigheten gick ut med det?	
18	R4	Yes.	D-UC
19	OI	Snyggt, har ni på Know e några medarbetare som inte har möjlighet att jobba hemifrån? Antingen om det är av tekniska skäl eller om det är för att deras arbetsuppgifter inte kan göras hemifrån?	
20	R4	Nope.	D-UC
21	OI	Grymt, kände du att de flesta var positivt eller negativt inställda till att jobba hemifrån?	
22	R4	Det är väldigt individuellt faktiskt, det är en spännande analys nu efteråt. Att vissa anammar detta och ser denna friheten som en fantastisk sak medans andra tycker detta varit rent smärtsamt.	D-UC
23	OI	Ja, är det någon skillnad i arbetsuppgifter mellan de som tycker det är smidigt och de som inte tycker det?	
24	R4	Nej egentligen inte arbetsuppgifter. Det är väldigt likt här på så sätt, men däremot tror jag i hur man bedriver eller genomför sina arbetsuppgifter, vissa gör det ju helt isolerat med ett par hörlurar i	D-UC

		öronen och andra gör det gärna genom att rådfråga och bolla idéer och sådär. Sistnämnda har då tyckt det varit mycket jobbigare att sitta hemma och de andra har tyckt det var dö skönt att sitta hemma på en torsdag i sitt hemlandskap och köra på liksom.	
25	OI	Precis, och det är ändå som så att dessa har samma typ av arbetsuppgifter?	
26	R4	Jajamen.	D-UC
27	OI	Super, har du känt både själv och om du vet dina kollegor, jag antar att vissa tycker att effektiviteten för förbättrats, men då har nog även vissa känt att den försämras antar jag. Känner du att effektiviteten har förbättrats eller försämrats vid följd av hemarbete?	
28	R4	Nej, alltså i och med att vi varit så inträngade och haft den friheten sedan tidigare så har vi inte känt eller upplevt någon skillnad. Sen är det som alltid när man är ett stort gäng att frihet och ansvar inte alltid faller väl ut, men det har inte med pandemin att göra.	D-UC
29	—	Samtalet avbröts kort.	—
30	OI	Såklart, har ni ändrat några av era säkerhetsåtgärder på grund av flytten till hemarbete? Nu har ni kunnat jobba hemma innan men har ni haft några anledningar till att ändra era säkerhetsåtgärder när man började jobba hemifrån?	
31	R4	Nej.	D-IT
32	OI	Hur ser era säkerhetsåtgärder ut, har ni några speciella sätt att göra någon bästa praxis om ni har några dokument eller utbildning eller liknande för detta?	
33	R4	Nej man alltså, det borde man kanske ha. Men det har vi inte, man hackar upp sig på VPN:et om man ska komma åt kontoret och det är ett annat VPN om man ska komma åt vår serverpark och sådär så att. Vi har också att genom datorerna har vi dubbel inloggning men det har vi ju alltid haft.	D-IT
34	OI	Det kopplar väl ihop till nästa fråga också, i och med att man kopplar upp sig till sitt hemnätverk och liknande så kan man ju tänka sig att det har blivit lite ökat tryck. Att förövare går på individen, har ni märkt av någon typ av tryck eller förövare som försökt komma åt era grejor?	
35	R4	Nej men det har vi faktiskt inte, vi har inte blivit hårdare ansatta än tidigare men som sagt vårt känsliga material är inlåsta i serverhallar i vilket fall som helst.	D-IT
36	OI	Är det serverhallar ni själva har hand om eller det är någon tjänst?	

37	R4	Ja men vissa utav dem har vi fysisk access till, men det är inget som vi har, eller som vi driftar själva utan det är, vi köper utrymmet helt enkelt.	D-IT
38	OI	Mm, då går jag till molntjänster. Är det något ni använder er utav?	
39	R4	Svar ja.	I-M
40	OI	Bra, har du några exempel på vilka, eller när ni använder molntjänster?	
41	R4	Ja men vi kör Microsoft rätt mycket så det är ju Azure för våran del. Vi har varit lite med Amazon osv men det är Azure huvudsakligen. Det gäller både eller egentligen alla typer av tjänster, men primärt är det virtuella servermiljöer egentligen. Vi använder ganska lite deras tjänsteinfrastruktur.	I-M
42	OI	Mm precis Azure. Har ni någon, behandlar ni er data via serverhallarna genom någon molntjänst också?	
43	R4	Jodå men det gör vi absolut. Vi jobbar ju mycket inom sjukvård osv. mycket och då är det höga krav på på avanalysering för GDPR men också patientsäkerhet just därför kör vi Sverigebaserade serverhallarna på de bitarna.	I-M
44	OI	Ja precis, du sa GDPR, Know e fanns ju innan GDPR också ju vilket kom 2018. Var det mycket arbete med att fixa till exempel molntjänster och kryptera och annan konfidentialitet när just GDPR kom fram? För er del.	
45	R4	Aa men det har det varit. Men som tur är så har vi haft väldigt bra datakontroll under hela vår resegång, så det har inte varit av det skälet. Utan det är mer att vara tvungna att bygga in lösningar där vi fortfarande kan arbeta. För det är väldigt tunga analys-funktioner vi bygger och att kunna analysera data på krypterat material är inte helt lätt. Så det är mest det som tagit tid.	I-M
46	OI	Grymt, har ni fått veta från någon av era molntjänstleverantörer att de haft något typ av dataintrång som kan ha påverkat er?	
47	R4	Nej faktiskt inte.	I-M
48	OI	Nä, det är ju tur det, då har de skött sig!	
49	R4	Nä det vet vi ju inte om de gjort, men de har åtminstone inte hört av sig!	I-M
50	OI	Nä precis, men det hoppas vi inte iallafall. Då ska vi se, då använder ni VPN-tjänster helt och hållet för att komma åt era system tar jag det som. Använder ni några andra typer av preventiva medel som till exempel lösenordshanterare?	

51	R4	Nej men alltså vi har ju brandväggar och alla dessa bitarna då, men inte något mer avancerat. Utan då är det VPN.	I-P
52	OI	Ja, ifall någon skulle säga att ett dataintrång skett, har ni några givna riktlinjer som ni skulle följa då, eller hade ni tagit det lite som det kommer?	
53	R4	Nej det skulle nog ha tagits som det kommer.	I-P
54	OI	Ja precis. Då har vi inte så mycket inom utbildning på den nivån, men än att ni mest har IT-folk som förmodligen har ganska bra koll på det.	
55	R4	Ja precis men det handlar lite om hygien igen, jo men det tycker jag handlar om allt om dessa frågor att det är just hygien. Det finns alltid utrymme för förbättring men i ett snabbt växande bolag blir det lätt fokus på något annat.	T-T
56	OI	Såklart, det är nog ingen chock! Men om vi säger såhär då, hur välinformerade skulle du säga att anställda är på ert företag? Inom då IT-säkerhet?	
57	R4	Ja men det här är ju en ständig frågeställning, så jag skulle vilja säga att den är tillräckligt god för att vi ska känna oss trygga i det.	T-T
58	OI	Det är ju bra. Har du själv märkt i dig själv eller hos kollegor hur man har ändrat sitt säkerhetsbeteende just med flytten till hemarbete till exempel att man stänger av datorn varje gång man lämnar eller ska göra något annat? Finns det någonting som gör, som du känner är skillnad från när du jobbade på kontoret?	
59	R4	Det är ju så att vi har haft en datapolicy, de flesta sitter på gamingutrustning yrkesmässigt också. Så liksom hybriden mellan när det är en arbetsstation och när det är en nöjesstation är inte helt klar. Och det har varit ett medvetet val från våran sida, så att vi har ju valt att separera näten, vi har liksom inte… man skulle egentligen kunna sätta upp ett snöre mellan våra kontorsnät och våra miljöer osv men vi har ju valt att smäller en dator eller liknande ska inte det heller påverka någonting annat egentligen. Så det vore synd att säga att vi har den typen av styrning, nej.	T-T
60	OI	Använder ni någon typ av BYOD då att man har sin egen utrustning eller det är företagets utrustning?	
61	R4	Nejdå det är företagets utrustning.	T-T
62	OI	Jag förstår. Då ska vi se, i och med att ni arbetar mycket med sjukhuset. Konfidentialitet, när det handlar exempelvis om behörighetskrav och liknande, jag antar att alla kanske inte kommer åt all data inom företaget, utan kanske bara de som sitter i projekten?	

63	R4	Nej verkligen inte. Vi har kolossalt mycket sekretessavtal som är personlighetsbundna och inte bara på företagsnivå utan så är det ju.	T-C
64	OI	Hur ser det ut i praktiken, är det som så att en person har tillgång till datan eller är det alla i ett projekt?	
65	R4	Ja, men det beror på. Vi sätter ofta ihop teams som jobbar med specifika klienter, och då genomgår de ju allt från poliskontroller tänkte jag säga, men myndighetskontroller till sekretessavtal osv. Det beror helt på vad det är för typ av uppdrag	T-C
66	OI	Och säg att det är flera på ett uppdrag, hur…	
67	R4	Då är det personliga konton, så alltid spårbart på det som görs.	T-C
68	OI	Super, och när det handlar om integriteten på datan, har ni behörighetskrav på när man till exempel korrigerar eller raderar så man alltid kan tracka hur och vem som gjort vad?	
69	R4	Ja du tänker kodmässigt då?	T-C
70	OI	Nej inte bara, jag tänker allt egentligen. Jag tänker att man skulle kunna gå in i ett system och jag vet inte, radera en del av en databas exempelvis, det behöver man ju inte göra med kod exempelvis.	
71	R4	Nänä men vi har ju, såklart om jag lånar ut mina konton till någon annan så utsätter jag mig för fara om någon annan gör något dumt så att säga, men det är ju personlighetsstyrt.	T-C
72	OI	Ja precis, har du något att lägga till Alex?	
73	ANS	Nej.	
74	OI	Alright, sen ja, nästa fråga binder ihop det lite med det andra. tillgängligheten av datan. har ni då tillgängligheten på samma ställe eller är det uppdelat i olika system, till exempel när man kommer åt datan från ett projekt och data från ett annat projekt. Är det ganska kopplat till samma system eller är det helt olika?	
75	R4	Vi jobbar ju alltså med utvecklingsmiljöer och då är det mockat data och där arbetar vi med en mycket mer kompakt miljö, men när man direkt går över till QA eller produktion så är det helt separerat.	T-C
76	OI	Jag antar att detta varit ganska likt från innan flytten också, och även under?	
77	R4	Absolut. Återigen hygien. Det är ju hygienfrågor, det är samma sak som att vi alltid arbetar med byggservrar så att stegen är alltid kontrollerad utav både enhetstester och byggserver så det inte är manuella handpåläggningar. Där är ju också spårbarhet på vem	T-C

		som gör vad och vem som accepterar, vilken typ av publicering som sker osv.	
78	OI	Nä men precis, är detta något som ändrats sen GDPR?	
79	R4	Hm nej det skulle jag nog inte säga. Märkligt nog har vi nog alltid haft en väldigt sund bild på det så vi har nog aldrig byggt lösningar som har varit på ett sånt sätt och man ska inte heller glömma det att GDPR är väldigt inriktat på där bolag med många datakällor använder för korsbefruktningar av användning av data för andra skäl än det de ämnas för. Det är för att skydda individen där, och där har vi inte varit, så vi är ganska förskonade av det.	T-C
80	OI	Men det är ju snyggt, något att tillägga Alex?	
81	ANS	Hm nej det var egentligen lite mer, jag är intresserad av hur ni tänker med utbildningarna och så, att ni inte riktigt kör någonting på IT-säkerhet utan att det låter mer som någon del av företagskulturen verkar det som lite.	
82	R4	Ja om någon skulle ringt mig och sagt att vi skulle behöva ha en endagsseminarium på den så handlar det väl mer om praktikaliteten om när vi ska få till det då alla är upptagna men det är klart att det är av intresse att lyssna till. Men då får man se vad det är för område också, för oss är ju säkerhet egentligen hur kan vi säkerställa att vi, eller att alla sitter på en lagom hög nivå att inte klicka på mail liksom med bilagor i onödan.	I-U
83	ANS	Mm okej! Är det någonting som sållas ut när ni anställer folk eller testar ni det på något sätt?	
84	R4	Det är inte en enskilt fråga, det är det inte, men det är klart att i anställningsprocessen handlar det väldigt mycket om datakunnigt folk. Så någonstans där, men det är inte enskilda frågor runt det.	I-U
85	ANS	Nä men precis, men nej jag tror inte jag har något utöver det. Väldigt effektivt!	
86	OI	Då så, inget du heller känner för R4 som du vill få in eller flika in på?	
87	R4	Just genom att det handlar mycket om access och liksom distansdelar och det är något som vi inte är nya med på något sätt så är det liksom, nä.	
88	OI	Ja är med, det känns ganska självklart förstår jag det som. Vi har väl märkt det att när vi intervjuat både de mindre företagen och de större företagen, att de mindre tenderar på att distansarbete känns mer som en självklarhet och att de större inte haft det som en självklarhet även om möjligheten funnits. Men sen när de testat på att jobba hemifrån så har det också känts bättre och fått en bild av	

		att det går. Lite intressant. Nä men då har jag inget mer så jag tänker att jag stänger av intervjun.	

8 Referenser

Alshaikh, M., Maynard, S., Ahmad, A. & Chang, S., (2018). An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations. 10.24251/HICSS.2018.635. <https://www.researchgate.net/publication/322634101_An_Exploratory_Study_of_Current_Information_Security_Training_and_Awareness_Practices_in_Organizations> (Hämtad 2022-04-26).

Amis, J. & Greenwood, R., (2020). Organisational Change in a (Post‐) Pandemic World: Rediscovering Interests and Values. Journal of Management Studies, [online] 58(2), pp.582-586. <https://www.researchgate.net/publication/346932850_Organisational_Change_in_a_Post-_Pandemic_World_Rediscovering_Interests_and_Values> (Hämtad 2022-05-01).

Andress, J., (2014). Chapter 1 - What is Information Security? The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice: Second Edition. 1-22. DOI 10.1016/B978-0-12-800744-0.00001-4. <https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid&db=edselp&AN=B9780128007440000014&site=eds-live&scope=site> (Hämtad 2022-04-14).

Assa Abloy, (u. å.). About us. <https://www.assaabloy.com/se/sv/about-us> (Hämtad 2022-05-11).

Bryant, S., (2000). At home on the electronic frontier: work, gender and the information highway. New Technology, Work and Employment, 15(1), pp.19-33. <https://onlinelibrary.wiley.com/doi/epdf/10.1111/1468-005X.00062> (Hämtad 10 April 2022).

Dubey, A. & Tripathi, S., (2020). Analysing the Sentiments towards Work-From-Home Experience during COVID-19 Pandemic. Journal of Innovation Management, [online] 8(1). <https://www.researchgate.net/publication/341059331_Analysing_the_Sentiments_towards_Work-From-Home_Experience_during_COVID-19_Pandemic> (Hämtad 2022-05-15).

Eklund, H., (2020). Svenska notan för cyberangrepp i år: 20 miljarder. [online] Ny Teknik. <https://www.nyteknik.se/sakerhet/svenska-notan-for-cyberangrepp-i-ar-20-miljarder-6997884> (Hämtad 2022-05-02).

Felstead, A., Jewson, N., Phizacklea, A. & Walters, S., (2002). Opportunities to work at home in the context of work-life balance. Human Resource Management Journal, 12(1), s. 54-76. <https://onlinelibrary.wiley.com/doi/epdf/10.1111/j.1748-8583.2002.tb00057.x> (Hämtad 2022-04-10).

Golden, T. & Gajendran, R., (2018). Unpacking the Role of a Telecommuter's Job in Their Performance: Examining Job Complexity, Problem Solving, Interdependence, and Social Support. Journal of Business and Psychology, [online] 34(1), pp.55-69. <https://www.researchgate.net/publication/323120977_Unpacking_the_Role_of_a_Telecommuter's_Job_in_Their_Performance_Examining_Job_Complexity_Problem_Solving_Interdependence_and_Social_Support> (Hämtad 2022-04-10).

Grade, (u. å.). Om oss. <https://www.grade.com/om-oss/> (Hämtad 2022-05-11).

Imperva, (u. å.). What is MITM (Man in the Middle) Attack. [online] Learning Center. <https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/> (Hämtad 2022-04-14).

ITC Secure, (2020). COVID-19 RELATED CYBER ATTACKS - ITC Secure | Cyber Advisory & Managed Security Services. [online] ITC Secure | Cyber Advisory & Managed Security Services. <https://itcsecure.com/people-technology-and-governance/covid-19-related-cyber-attacks/> (Hämtad 2022-04-08).

IT-Finans, (2017). Kostnader för cyberattacker för svenska företag. [online] IT-Finans. <https://it-finans.se/kostnader-for-cyberattacker-for-svenska-foretag/> (Hämtad 2022-05-02).

Jacobsen, DI & Hellström, C., (2002), *Vad, hur och varför: Om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen.* Översatt av Gunnar Sandin, Studentlitteratur AB, Lund.

Khan, B., Alghathbar, K.S., Nabi, S.I. & Khan, M.K., (2011). Effectiveness of information security awareness methods based on psychological theories, African Journal of Business Management 5(26), 10862-10868. <https://academicjournals.org/articles/search?q=Effectiveness+of+information+security+awareness+methods> (2022-04-26).

Kirsten, S., (u. å.). Cross Site Scripting (XSS). [online] Owasp.org. <https://owasp.org/www-community/attacks/xss/> (Hämtad 2022-04-14).

Knowe, (u. å.). Om oss. <https://www.knowe.se/index.php/om-oss/> (Hämtad 2022-05-11).

Kobis, P., (2021) 'Human Factor Aspects in Information Security Management in the Traditional it and Cloud Computing Models', Operations Research and Decisions, . 31(1), pp. 61–76. <https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid&db=edsdoj&AN=edsdoj.012517a24cc04cb084e1a2dcb64eb071&site=eds-live&scope=site> (Hämtad 2022-04-25).

Liang, H. & Xue, Y., (2009) 'Avoidance of Information Technology Threats: A Theoretical Perspective', MIS Quarterly, 33(1), pp. 71–90. doi: 10.2307/20650279. <https://eds.p.ebscohost.com/eds/pdfviewer/pdfviewer?vid=6&sid=44126a8c-9854-4a0f-970f-d65e75458738%40redis> (Hämtad 2022-04-12).

Makarius, E. & Larson, B., (2017). Changing the Perspective of Virtual Work: Building Virtual Intelligence at the Individual Level. Academy of Management Perspectives, [online] 31(2), pp.159-178.

<https://www.researchgate.net/publication/317051625_Changing_the_Perspective_of_Virtual_Work_Building_Virtual_Intelligence_at_the_Individual_Level> (Hämtad 2022-04-10).

Mandal, S. & Khan, D. A., (2020). A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic. 2020 International Conference on Smart Electronics and Communication (ICOSEC), [online] Available at: <https://ieeexplore.ieee.org/document/9215374> (Hämtad 2022-04-16).

McAfee, (2020). Cloud Adaption and Risk Report. [online] Mcafee.com. <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-cloud-adoption-and-risk-report-work-from-home-edition.pdf> (Hämtad 2022-04-16).

Monev, V., (2020) 'Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002', 2020 International Conference on Information Technologies (InfoTech), Information Technologies (InfoTech), 2020 International Conference on, pp. 1–5. doi: 10.1109/InfoTech49733.2020.9211066. <https://ieeexplore-ieee-org.ludwig.lub.lu.se/document/9211066?arnumber=9211066> (Hämtad 2022-04-25).

Najib, W., Sumaryono, S., Nugroho, L.E., & Putra, G.D. (2018). Development of Enterprise Security Framework in SKK Migas Based on Integration of ISO 27000 and SABSA Model. 2018 10th International Conference on Information Technology and Electrical Engineering (ICITEE), 382-387. <https://ieeexplore-ieee-org.ludwig.lub.lu.se/document/8534747?arnumber=8534747> (Hämtad 2022-04-25).

Oates, B.J., Griffiths, M. & McLean, R. (2022). *Researching Information Systems And Computing.* 2nd ed. London: SAGE Publications Ltd.

PwC, (u.å. a). Fakta om PwC. https://www.pwc.se/sv/om-pwc/fakta-om-pwc.html (Hämtad 2022-05-11).

PwC, (u.å. b). About us. https://www.pwc.com/gx/en/about.html (Hämtad 2022-05-11).

Razmerita, L., Peroznejad, A., Pantelli, N. & Kärreman, D., (2021). Adapting to the Enforced Remote Work in the Covid 19 Pandemic. [online] Researchgate. <https://www.researchgate.net/publication/353122164_Adapting_to_the_Enforced_Remote_Work_in_the_Covid_19_Pandemic> (Hämtad 2022-04-15).

Richter, A., (2020). Locked-down digital work. International Journal of Information Management, [online] 55, pp.102-157. <https://www.researchgate.net/publication/341804463_Locked-down_digital_work> (Hämtad 2022-05-01).

Rupietta, K. & Beckmann, M., (2017). Working from Home. Schmalenbach Business Review, [online] 70(1), pp.25-55. <https://www.researchgate.net/publication/321694287_Working_from_Home_What_is_the_Effect_on_Employees'_Effort> (Hämtad 2022-04-10).

Saxena, S., (2020). Replay Attack. [online] GeeksforGeeks. <https://www.geeksforgeeks.org/replay-attack/> (Hämtad 2022-04-14).

Titcomb, B., Millard, B., Warrington, B., Wallace, B., Wallace, B., Titcomb, B. & Rees, B., 2022. Apple exec quits over working from home row. [online] The Telegraph. <https://www.telegraph.co.uk/business/2022/05/09/apple-exec-quits-working-home-row/> (Hämtad 2022-05-16).

Stefaniuk, T., (2020) 'Training in shaping employee information security awareness', Entrepreneurship and Sustainability Issues, 7(3), pp. 1832–1846. doi: 10.9770/jesi.2020.7.3(26). <https://doaj.org/article/f4c00f5d8fc641af95cee684de1fe471> (Hämtad 2022-04-26).

Verizon, (2020). Analysing the COVID-19 data breach landscape. [online] Verizon.com. <https://www.verizon.com/business/resources/articles/analyzing-covid-19-data-breach-landscape/> (Hämtad 2022-04-18).

W3schools, (u. å.). SQL Injection. [online] W3schools.com. <https://www.w3schools.com/sql/sql_injection.asp> (Hämtad 2022-04-14).