LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Social Engineering: Kampen att stärka den svagaste länken

En kvalitativ studie om informationssäkerhetsutmaningar i förebyggande och mitigering av social engineering-attacker hos distansarbetande verksamheter

Kandidatuppsats 15 hp, kurs SYSK16 i Informationssystem.

Författare: Tarek Bermalm
Albin Olsson

Handledare: Björn Svensson

Rättande lärare: Odd Steen
Magnus Wärja

Social Engineering: Kampen att stärka den svagaste länken - En kvalitativ studie om informationssäkerhetsutmaningar i förebyggande och mitigering av social engineering-attacker hos distansarbetande verksamheter

ENGELSK TITEL: Social Engineering: The struggle to strengthen the weakest link

FÖRFATTARE: Tarek Bermalm, Albin Olsson

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Osama Mansour, PhD

FRAMLAGD: Maj, 2022

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 137

NYCKELORD: informationssäkerhet, social engineering, mänskliga faktorn, informationsäkerhetspolicy, utbildning, medvetenhet, informationssäkerhetskultur, distansarbete

SAMMANFATTNING (MAX. 200 ORD):
I samband med COVID-19-pandemin blev distansarbete vardagen för många verksamheter. Detta ser ut att bli bestående för många verksamheter. Distansarbete utgör stora risker för informationssäkerhetsarbetet i och med ändrat beteende hos anställda och dålig anpassning av verksamheter. Det kan även konstateras att den mänskliga faktorn är bristpunkten inom informationssäkerhet. Därmed är intrång genom social engineering-attacker, det vill säga de attacker som utnyttjar den mänskliga faktorn, ett aktuellt problemområde. Därför ämnades att beskriva de informationssäkerhetsmässiga utmaningar som distansarbetande verksamheter ställs mot i arbetet mot social engineering samt hur dessa hanteras. För att besvara detta genomfördes kvalitativa intervjuer med CISOs (Chief Information Security Officer) och säkerhetsexperter inom olika verksamheter. Dessa verksamheter varierade i storlek och var verksamma i den privata eller offentliga sektorn. Det framkom av studien att phishing, säkerhetskultur, ISP och SETA är områden där utmaningar och förbättringsmöjligheter är närvarande hos distansarbetande verksamheter.

Innehåll

Förkortningar

Följande är en tabell över förkortningar som förekommer samt dess betydelse, i slumpmässig ordningsföljd.

Tabell 1: Förkortningar och dess betydelse

Förkortning	**Betydelse**
IT	Informationsteknik
SETA	Security Education, Training and Awareness
CIA	Confidentiality, Integrity, Availability
ISP	Informationsssäkerhetspolicy

1 Introduktion

1.1 Bakgrund

Distansarbete har blivit vardag för många anställda (Eurofound, 2020). Enligt Eurofound (2020) jobbar 40% av alla anställda på distans. En ökning från 5%, vilket 2019 var antalet distansarbetande i EU (Eurostat, 2020). Vilket i sin tur är ett direkt resultat av viruset COVID-19 som år 2020 tvingade länder till stränga restriktioner (Europakommissionen, 2020). När pandemin börjar nå sitt slut år 2022 är det många företag som kommer att välja fortsätta med distansarbete, i någon utsträckning (Eurofound, 2020). Enligt McKinsey & Company (2021) kommer det att ske en stor ökning i antalet distansarbetare. McKinsey & Company (2021) beskriver även i en rapport att 9 av 10 företag kommer att tillämpa hybridmodellen efter pandemin. Enligt Barrero, Bloom & Davis (2021) kommer ungefär 70% av företagen oavsett storlek nyttja distansarbete. I och med att pandemin i början av 2020 drabbade samhällen världen över, tvingades verksamheter att anpassa sig till nya omständigheter (Europakommissionen, 2020).

Förändringar som dessa kan ha som konsekvens att verksamheter ignorerar eller nedprioriterar arbetet med informationssäkerhet (Trzupek, 2020). Informationssäkerhet kan definieras på olika sätt, men i en generell bemärkelse handlar ämnet om att skydda information (von Solms och van Niekerk, 2013). I takt med att omvärlden förändras måste också säkerhetsarbetet utvecklas kontinuerligt (Whitman & Mattord, 2011). Nya omständigheter skapar hot för informationssäkerheten när anställda jobbar på distans (Borkovich & Skovira, 2020; Trzupek, 2020). Ett av problemområdena är att människan ofta är den svagaste länken inom informationssäkerhet (Clarke, Furnell & Talib, 2010; Hughes-Lartey, Li, Botchey & Qin, 2021; Chapman, 2021). Detta är av betydande vikt då säkerhet bara är så starkt som dess svagaste länk (Clarke, Furnell & Talib, 2010). Innebörden av social engineering är att manipulera människor till att bryta rutiner som säkerhetsprotokoll, bästa praxis och normala procedurer, med målet att få åtkomst till ett system såsom nätverk eller datorer (Borkovich & Skovira, 2020). FBI (2020) påvisar att antalet phishing-attacker i samband med pandemin har fördubblats. Phishing är en typ av social engineering-attack där den mänskliga faktorn utgör en kritiskt aspekt (Krombholz, Hobel, Huber & Weippl, 2015). Social engineering utgör i och med dessa aspekter ett aktuellt problemområde (Trzupek, 2020; Borkovich & Skoivra, 2020).

Tidigare forskning har förts gällande denna uppsats behandlingsområde till viss mån. Det har skrivits rikligt med litteratur om informationssäkerhet. Inom detta område har Principles of Information Security (Whitman & Mattord, 2011) och Working From Home: Cybersecurity in the Age of Covid-19 (Borkovich & Skovira, 2020) varit centrala för uppsatsen. Social engineering och den mänsklig faktorn har det även skrivit förhållandevis mycket om, varav de verk som varit mest relevanta inom social engineering för denna uppsats är Advanced social engineering attacks (Krombholz et al., 2015), Social Engineering Attacks: A Survey (Salahdine & Kaabouch 2019), samt Social Engineering: The Neglected Human Factor for Information Security Management (Brody, Burd, Luo & Seazzu, 2011). Däremot finns det

betydligt färre moderna verk som skrivits om kombinationen utav dessa ämnen. Det vill säga, social engineering, distansarbete och de nya omständigheter som verksamheter enligt tidigare redogörelse har ställts mot. Gällande tidigare forskning bör det även tilläggas att en modern uppsats, skriven av Andersson, Berg & Holmqvist (2021), publicerats med fokus på ett snarlikt område. Denna studie syftar till att undersöka utmaningar gällande informationssäkerhet som uppstår vid distansarbete i en större skala (Andersson, Berg & Holmqvist, 2021). Därmed skiljer sig dessa uppsatser huvudsakligen åt på två punkter. Den första är att deras uppsats begränsar sig till storskaligt distansarbete något denna uppsats inte tar i beaktande. Den andra är att deras uppsats, varken i form av syfte, empiri, diskussion eller slutsats, behandlar social engineering, medan detta är ett huvudfokus i denna uppsats.

1.2 Problemformulering

Antalet cyberattacker mot verksamheter ökar kontinuerligt (Borkovich & Skovira, 2020; Sharton, 2020; Williams, Chaturvedi & Chakravarthy, 2020). Endast under året 2020, under trycket av COVID-19-pandemin, har en 3- till 5-faldig ökning av cyberattacker observerats (Borkovich & Skovira, 2020; Sharton, 2020; Williams, Chaturvedi & Chakravarthy, 2020).

Det kan även konstateras att säkerheten blir bristande i distansarbetande miljöer (Borkovich & Skovira, 2020; Furnell & Shah, 2020). I en studie av Georgiadou, Mouzakitis och Askounis (2021) visar de att 53% av alla distansarbete inte mottagit nya säkerhetspolicys när de började arbeta på distans. Borkovich & Skovira (2020) beskriver i deras artikel att säkerhetspolicys överges när arbetet sker hemifrån. I Tessians (2021) rapport skriver de att 30% av distansarbetande anställda upplever att de kan komma undan med ett mer riskbenäget arbetssätt samt att 39% anger att de arbetar annorlunda med informationssäkerhet hemifrån. Vidare visar en ytterligare rapport från Tessian (2020) att för 48% av distansarbetande medarbetare är det mindre sannolikt att de kommer följa goda säkerhetsrutiner, varav anledningen är att de inte känner sig övervakade av IT-avdelningen på samma sätt som på kontoret. Samma rapport (Tessian, 2020) beskriver även att 47% av anställda är mindre troliga att följa goda säkerhetshetsrutiner hemifrån p.g.a. att de upplever distraktion. Till sist nämner även rapporten (Tessian, 2020) att 50% av anställda anser att det är mindre sannolikt att de följer goda säkerhetsrutiner när de jobbar hemifrån p.g.a. att de inte använder sina vanliga enheter. Ett bristande säkerhetsbeteende hos anställda försvårar för organisationer då policys och utbildning samt hur väl dessa följs är grunden till en god säkerhet samt det primära sättet att motverka den mänskliga faktorn (Puhakainen & Siponen, 2010).

Vidare är människan för informationssäkerheten den svagaste länken (Clarke, Furnell & Talib, 2010; Hughes-Lartey, Li, Botchey & Qin, 2021; Chapman, 2021), och ett system kan inte vara starkare än sin svagaste länk (Clarke, Furnell & Talib, 2010). Enligt CybSafe (2020) kan 90% av intrång eller säkerhetsincidenter tillskrivas mänskliga misstag eller mänskligt beteende. Social engineering är utnyttjandet av den mänskliga faktorn (Borkovich & Skovira, 2020). Det har visats att anställda är mer troliga att utsättas för social engineering-attacker när de arbetar på distans (Borkovich & Skovira, 2020). Litteraturen visar också att den mänskliga faktorn behöver prioriteras högre (Borkovich & Skovira, 2019; Brody et al., 2011). Trots detta får den mänskliga faktorn mindre uppmärksamheten än andra aspekter av informationssäkerhet (Rahman, Rohan, Pal & Kanthamanon, 2021; Hughes-Lartey, Li, Botchey & Qin, 2021).

1.3 Syfte

Som grund för det problemområde som redogjorts för avser denna uppsats att beskriva de informationssäkerhetsutmaningar som verksamheter ställs inför i förebyggandet av att deras distansarbetande anställda utsätts för social engineering-attacker. Uppsatsen avser även att beskriva hur dessa hanteras.

1.4 Forskningsfråga

I enlighet med syftet av uppsatsen lyder forskningsfrågan:

Vid förebyggande åtgärder och mitigering av social engineering-attacker, vilka informationssäkerhetsutmaningar ställs distansarbetande verksamheter inför och hur hanteras dessa?

1.5 Avgränsningar

Att kombinera arbete både hemifrån och på kontoret kan beskrivas som en hybridmodell (Yang, Holtz, Jaffe, Suri, Sinha, Weston, Joyce, Shah, Sherman, Hecht & Teevan, 2022), 2022; McKinsey & Company, 2021). Vid denna uppsats behandling av konceptet distansarbete har det inte tagits i beaktande ifall verksamhetens anställda arbetar enbart på distans eller ifall de tillämpar hybridmodellen.

2 Litteraturgenomgång

2.1 Distansarbete och hybrid arbetsmodell

Distansarbete är inte något nytt fenomen utan myntades redan 1970 (Baruch, 2001). Baruch, (2001) definierar distansarbete som att verksamhetens kontor inte är den enda platsen arbete utförs. Det som möjliggör distansarbete är teknologiska framsteg som tillåter anställda att jobba från en annan plats (Baruch, 2001). Det finns flera fördelar med att jobba på distans, som till exempel ökad produktivitet (Popovici & Popovici, 2020). En annan fördel är att anställda kan jobba i en lugnare miljö vilket kan leda till bättre fokus (Popovici & Popovici, 2020). En nackdel kan vara att det är svårare för verksamheter att bygga en bra kultur (Popovici & Popovici, 2020).

I samband med COVID-19-pandemin skedde ett stort skifte för verksamheter att gå över till distansarbete (Yang et al., 2022). Enligt Yang et al. (2022) är det många verksamheter som inte kommer att gå tillbaka till att endast arbeta på kontoret. De kommer istället antingen jobba helt på distans, eller byta till en hybrid arbetsmodell (Yang et al., 2022).

2.2 CIA-triaden och informationssäkerhet

Grunden till informationssäkerhet lades till en början i datorsäkerhet under andra världskriget då behovet att skydda fysiska platser och hårdvara uppstod (Whitman & Mattord, 2011). Det var primärt för att skydda mot fysisk stöld av utrustning (Whitman & Mattord 2011). Under 2000-talet är landskapet däremot förändrat (Whitman & Mattord, 2011). I och med internets uppkomst och popularitet tillåts möjligheten för miljontals osäkrade nätverk att kommunicera med varandra (Whitman & Mattord, 2011).

Det finns flera definitioner av informationssäkerhet (von Solms & van Niekerk, 2013). Enligt Whitman och Mattord (2011) är definitionen att informationssäkerhet är till för att skydda tillgångar som lagrar, använder och överför information från risker genom policys, utbildning och teknologi. Den vanligaste modellen för att beskriva informationssäkerhet är CIA-triaden (Andress, 2014; Lundgren & Möller, 2019) Denna modell består av tre egenskaper; *Confidentiality* (kommer benämnas som konfidentialitet), *Integrity* (kommer benämnas som integritet) och *Availability* (kommer benämnas som tillgänglighet) (Whitman & Mattord, 2011; Lundgren & Möller, 2019, Andress, 2014). Denna modell är också den som kommer att ligga till grund för denna uppsats.

2.2.1 Konfidentialitet

Konfidentialitet är en nödvändighet för att möjliggöra skyddet av data genom att enbart de med korrekta rättigheter och privilegier får tillgång till informationen (Andress, 2014, Whitman & Mattord, 2011; Lundgren & Möller, 2019). Denna information som behandlas under konfidentialitet betraktas som hemlig eller känslig (Nayak & Rao, 2014). Nayak & Rao

(2014) säger att information som är konfidentiell bör skyddas rigoröst av autentisering och restriktioner.

2.2.2 Integritet

När information har *integritet* är den komplett och inte skadad eller korrupt (Whitman & Mattord 2011; Lundgren & Möller, 2019; Nayak & Rao, 2014). Korruption kan ske när informationen lagras eller skickas (Whitman & Mattord, 2011). Detta kan ske av virus designade för att korrumpera informationen (Whitman & Mattord, 2011). Denna egenskap är alltså att förhindra information från att ändras av obehöriga eller förändras på annat sätt, som att en behörig tar bort viktig information av misstag (Andress, 2014). För att skydda informationen krävs det huvudsakligen att två aspekter tillgodoses, den ena är att skydda från obehöriga och den andra är möjligheten att återställa förlorad information (Andress, 2014). Integriteten är av extra vikt när det handlar om information som berör beslutsfattande (Andress, 2014)

2.2.3 Tillgänglighet

Tillgänglighet innebär att informationen ska vara åtkomlig när den behövs (Andress, 2014). Detta för att underlätta för verksamheter att snabbt kunna agera (Nayak & Rao, 2014). Det blir då nödvändigt att tillåta användare eller system att få åtkomst till information utan förhinder (Whitman & Mattord, 2011; Nayak & Rao, 2014).

2.3 Social Engineering

Social engineering är nyttjandet av den mänskliga faktorn för att få åtkomst till information, ett system eller liknande (Krombholz et al., 2015; Mann, 2008). Tillämpningen av social engineering går ut på att manipulera en eller flera människor och på så vis uppnå sina mål (Krombholz et al., 2015; Ian Mann, 2008). Efter ett framgångsrikt utfall vid användningen av social engineering kan man nyttja denna position för att utföra flera olika typer av handlingar (Krombholz et al., 2015). Exempelvis kan man med den nyvunna systemåtkomsten extrahera känslig information (Krombholz et al., 2015). Alternativt kan man även nyttja sin position för att låta användaren plantera skadliga filer i systemet (Krombholz et al., 2015).

2.3.1 Den mänskliga faktorn och dess betydelse för social engineering

Enligt CybSafe (2020) kan 90% av dessa intrång tillskrivas mänskliga misstag eller beteenden. Eminağaoğlu, Uçar & Eren (2009) beskriver människan som den huvudsakliga faktorn till att lyckas eller misslyckas med informationssäkerhet. Människan är den svagaste länken i informationssäkerhet (Clarke, Furnell & Talib, 2010; Hughes-Lartey, Li, Botchey & Qin, 2021; Chapman, 2021).

I social engineering-attacker utnyttjas generellt människors kognitiva bias (Brody et al., 2011). Kognitiv bias kan beskrivas som bristfällig logik, varav denna logik kan härledas till medfödda personlighetsdrag (Brody et al., 2011). Det är dessa kognitiva bias som möjliggör att den mänskliga faktorn kan utnyttjas genom social engineering-attacker (Brody et al., 2011). Enligt Brody et al. (2011) bör därför den mänskliga faktorn för arbetet med informationssäkerhet tas i samma beaktande som avancerade teknologiska lösningar. Trots

den betydelse mänskliga faktorn har samt det faktum att litteraturen säger att den mänskliga faktorn behöver prioriteras (Borkovich & Skovira, 2019; Brody et al., 2011) är den mänskliga faktorn ofta förbisedd och får mindre uppmärksamhet än andra aspekter av informationssäkerhet (Rahman, Rohan, Pal & Kanthamanon, 2021; Hughes-Lartey, Li, Botchey & Qin, 2021).

För att mitigera brister hos den mänskliga faktorn och därmed förebygga social engineering-attacker finns ett flertal tillvägagångssätt. En viktigt sådant är nyttjandet av policys (Puhakainen & Siponen, 2010). Ett annat är att utbilda anställda i informationssäkerhet (Whitman & Mattord, 2011). Även efterlevnad av policys, att säkerställa att de följs, är ett huvudsakligt moment i denna aspekt (Hove, 2020). Dessa tillvägagångssätt kommer att redogöras för i mer detalj senare.

Samtliga ovannämnda tillvägagångssätt för att förebygga social engineering-attacker utgår ifrån att adekvat *konfidentialitet* i CIA-triaden (Whitman & Mattord, 2011) är tillgodosedd (Krombholz et al., 2015). Med andra ord kan detta uttryckas som robusta och strikta rättigheter för systemåtkomst (Krombholz et al., 2015). Utnyttjandet av den mänskliga faktorn för systemåtkomst går ut på att obehöriga kringgår rättigheter (Krombholz et al., 2015). Detta görs genom att utnyttja en behörig användare som har dessa rättigheter och därmed få tillgång till ett system (Krombholz et al., 2015). Vid detta skede kan intrånget utgöra ett riskmoment för både *integritet* och *tillgänglighet* i CIA-triaden då ett intrång kan korrumpera, förstöra data och/eller kryptera data (Whitman & Mattord, 2011).

2.3.2 Den mänskliga faktorn i samband med distansarbete

Ett bristande säkerhetsbeteende hos anställda försvårar för organisationer då policys och utbildning, samt hur väl dessa följs är grunden till en god säkerhet som utgör det primära sättet att motverka den mänskliga faktorn (Puhakainen & Siponen, 2010). Informationssäkerheten är bristande vid distansarbete (Borkovich & Skovira, 2020; Furnell & Shah, 2020). Enligt Tessian (2020), Tessian (2021) samt Wang, Liu, Qian och Parker (2021) menar att anställdas informationssäkerhetsmässiga beteenden försämrats under distansarbete. Dessutom kan det konstateras att 53% av alla anställda i samband med övergång till distansarbete inte har fått några nya säkerhetspolicys (Georgiadou, Mouzakitis och Askounis, 2021).

2.3.3 Social engineering-attacker

För att behandla social engineering och skyddet mot detta är det nödvändigt att känna till några huvudsakliga attacker och deras kategorisering. Gällande kategoriseringen delar Krombholz et al. (2015) upp attacker i fyra huvudsakliga kategorier: fysiska, sociala, tekniska och sociotekniska. Fysiska attacker kan utföras på flera olika sätt, men alla har gemensamt att de utförs fysiskt snarare än digitalt (Krombholz et al., 2015). Ett exempel på detta är shoulder surfing (Salahdine & Kaabouch, 2019). Shoulder surfing är en attack som går ut på att utan en individs vetskap se på när denne anger lösenord eller användarnamn i ett digitalt system (Salahdine & Kaabouch, 2019). Pretexting är ytterligare en attack (Ivaturi & Janczewski, 2011; Salahdine & Kaabouch, 2019). Här nyttjas ett påhittad scenario för att utvinna känslig information (Ivaturi & Janczewski, 2011; Salahdine & Kaabouch, 2019). Ofta läggs mycket tid på att söka bland offentlig information, som sedan används för att iscensätta ett scenario som verkar pålitligt (Ivaturi & Janczewski, 2011). Exempelvis kan pretexting utföras i form

av ett riktat jobberbjudande, som i själva verket är en fälla för att utvinna känslig information från en viss individ (Salahdine & Kaabouch, 2019). Sociala attacker involverar ofta övertalning, manipulation eller påhittad auktoritet (Krombholz et al., 2015). Här är den mänskliga faktorn en central aspekt av utförandet (Krombholz et al., 2015).Tekniska attacker utförs huvudsakligen över internet (Krombholz et al., 2015). Exempelvis kan sociala medier användas för att samla information om en eller flera användare i ett system (Krombholz et al., 2015). Detta är även del av metoden OSINT, Open Source Intelligence (Ball, Ewan & Coull, 2012). Informationen kan sedan användas för att utföra riktade attacker med ett annat medium (Krombholz et al., 2015). Sociotekniska attacker utnyttjar fler eller samtliga av ovanstående metoder för att få åtkomst till ett system (Krombholz et al., 2015). Phishing är ett exempel på en vanligt förekommande socioteknisk attack (Ivaturi & Janczewski, 2011; Krombholz et al., 2015). Detta går ut på att få tag på känslig information genom att utgöra sig för att vara någon annan, som dessutom är mer pålitlig eller auktoritär (Ivaturi & Janczewski, 2011). I dessa attacker är den mänskliga faktorn även här en kritiskt aspekt (Krombholz et al., 2015).

De fyra attacktyper som beskrivits utgör samtliga negativa konsekvenser för CIA-triaden. Vad varje typ har gemensamt är att man i någon utsträckning utnyttjar bristfällig logik i mänskligt beteende och dess användarmönster, det vill säga just den mänskliga faktorn (Krombholz et al., 2015). Detta för att kringgå rättighetsbegränsningar (Borkovich & Skoivra, 2020), som täcks av *konfidentialitet* (Whitman & Mattord, 2011). Det kan även leda till att data korrumperas, vilket medför att *integritet* i CIA-triaden har korrumperats (Whitman & Mattord, 2011).

2.4 Informationssäkerhetskultur

För att förstå vad informationssäkerhetskultur är måste först begreppet verksamhetskultur förklaras (Wiley, McCormac & Calic 2020). Detta definieras som hur en grupp individer uppfattar att världen fungerar, vilket formar deras uppfattning, känslor, tankar och beteende (Wiley, McCormac & Calic 2020). Enligt Thomson, von Solms & Louw (2006) påverkar kulturen hos en verksamhet anställdas beteende. Informationssäkerhetskultur kan ses som en del av verksamhetskulturen och är en bidragande faktor till en organisations informationssäkerhet (Wiley, McCormac & Calic 2020). Detta kan då definieras som en grupps delade åsikt om hur information ska skyddas (Da Veiga and Eloff, 2010).

Att arbeta med kultur stärker informationssäkerhetsarbetet hos en verksamhets, i och med att de åtgärder som redan implementerats också upprätthålls (Da Veiga and Eloff, 2010). Louw, Thomson & von Solms (2006) beskriver att verksamhetskultur bör användas för att forma och ändra anställdas beteende kring informationssäkerhet. Kulturen hos en verksamhet och dess effekt på informationssäkerhet är en betydande faktor i säkerhetsarbetet (Siponen, Pahnila, & Mahmood, 2010; Van Niekerk & von Solms, 2010). En stark informationssäkerhetskultur är när de anställda tar ansvar och är medvetna om risker samt hur de hanteras (Wiley, McCormac & Calic 2020).

Vidare har det tidigare nämnts att den mänskliga faktorn ofta är den svagaste länken i informationssäkerhet (Clarke, Furnell & Talib, 2010; Hughes-Lartey, Li, Botchey & Qin, 2021; Chapman, 2021). För att motarbeta detta är etablerandet av en informationssäkerhetskultur i verksamheten en nödvändighet (Eloff & Von Solms, 2000; Von Solms, 2000).

2.5 Informationssäkerhetspolicys och dess efterlevnad

En informationssäkerhetspolicy (kommer hädanefter benämnas som ISP) kan beskrivas som instruktioner från en verksamhets högsta ledning till dess medarbetare som utför handlingar, tar beslut eller dylikt (Whitman & Mattord, 2011). Enligt Höne & Eloff (2002) är ISPs en essentiell aspekt för att förebygga intrång. Det är också viktigt att implementera och nyttja ISPs på rätt sätt (Bulgurcu, Cavusoglu & Benbasat, 2010). Ett exempel på detta är att genom ISPs förenkla medarbetarens möjlighet att arbeta säkert, istället för att komplicera processen (Bulgurcu, Cavusoglu & Benbasat, 2010). Dessutom bör ISPs vara utformade med utförbarhet i åtanke då det finns risk att de inte följs ifall de inte passar medarbetarens arbetsflöde (Samonas & Coss, 2014; Borkovich & Skovira, 2020). Hur ISPs utförs och implementeras är av betydelse då det finns en risk att dessa missuppfattas, tillämpas fel eller rent av inte följs (Ceraolo, 1996; Goodhue and Straub, 1989; Hoffer and Straub, 1989; Straub, 1990; Straub and Welke, 1998)

Att skapa ISPs för att arbeta med informationssäkerhet är en bra start, detta är dock inte tillräckligt för att få en verksamhets anställda att följa dem (Bulgurcu, Cavusoglu & Benbasat, 2010). Om det inte säkerställs att ISPs följs är risken att verksamheten påverkas negativt (Koohang, Anderson, Nord & Paliszkiewicz, 2020). Det är därför viktigt att etablera efterlevnad av ISPs (Koohang et al., 2020). Bulgurcu, Cavusoglu & Benbasat (2010) skriver i sin artikel att efterlevnad av ISPs har blivit en värdefull tillgång för verksamheter. Ledningen har en påverkan på efterlevnad i verksamheten då anställda ser upp till dem, därför krävs det att ledningen följer ISPs (Amankwa, Loock & Kritzinger, 2017). Detta styrker Koohang et al., (2020) i deras artikel, varav författarna beskriver att det måste finnas tillit mellan ledningen och anställda. Ett sätt att få efterlevnad i verksamheten är att göra det till en del av kulturen (Amankwa, Loock & Kritzinger, 2017).

2.6 Security Education, Training and Awareness

Security Education, Training and Awareness (kommer hädanefter benämnas som SETA) kan beskrivas som informationssäkerhetsmässig utbildning och träning med syfte att minska antalet intrång som sker där anställdas medvetenhet kring säkerhet utgör bristpunkten (Hight, 2005). Detta verktyg har visats påverka anställda till att i större grad följa ISPs (Eminağaoğlu, Uçar & Eren, 2009). SETA har även beskrivits som ett av de mest effektiva sätten att mitigera risker med informationssäkerhet (Eminağaoğlu, Uçar & Eren, 2009). Kruger & Kearney (2006) beskriver utbildning och träning i medvetenhet som en kritisk aspekt av informationssäkerhet. Det är dock essentiellt att SETA inte utförs vid endast ett tillfälle med enstaka utbildningar utan bör inkludera uppföljningsmoment (Eminağaoğlu, Eren & Uçar, 2009). Detta för att anställda med tiden ofta glömmer de koncept som har lärts ut under utbildning (Eminağaoğlu, Eren & Uçar, 2009).

Enligt Hight (2005) berör SETA medvetenhet. Medvetenhet kan beskrivas som ett tillstånd då användare i en verksamhet känner till och är medvetna om verksamhetens säkerhetsarbete (Siponen, 2000). Medvetenhet kring säkerhet i en verksamhet kan ofta innebära medvetenhet för ISPs (Siponen, 2000). Medvetenhet och kännedom om ISP är av vikt då det finns en risk att ISPs missuppfattas, tillämpas fel eller inte följs (Ceraolo, 1996; Goodhue & Straub, 1989; Hoffer & Straub, 1989; Straub, 1990; Straub & Welke, 1998). I den aspekten kan syftet med medvetenhet beskrivas som en strävan att minimera effekten av den mänskliga faktorn, i teorin helt och hållet oskadliggöra dem, samt maximera effektiviteten av säkerhetsarbetet

(Siponen, 2000). Verksamhetsledningen har dessutom en effekt på anställdas medvetenhet kring informationssäkerhet (Koohang, Anderson, Nord & Paliszkiewicz, 2020).

2.7 Informationssäkerhetsarbetet mot social engineering-attacker vid distansarbete

Den mänskliga faktorns svagheter gör att arbetet mot social engineering kräver mer än bara tekniska skyddsåtgärder (Brody et al., 2011). Istället behövs ett multidimensionellt tillvägagångssätt som bl.a. inkluderar ISPs, SETA och mitigering (Brody et al., 2011; Salahdine & Kaabouch, 2019). Verksamheter bör även arbeta med säkerhetskultur för att motarbeta social engineering (Salahdine & Kaabouch, 2019).

2.7.1 Den mänskliga faktorn i samband med distansarbete

Ett bristande säkerhetsbeteende hos anställda försvårar för organisationer då ISPs och informationsäkerhetsutbildning samt hur väl dessa följs är grunden till en god säkerhet samt det primära sättet att motverka den mänskliga faktorn (Puhakainen & Siponen, 2010). Informationssäkerheten är bristande vid distansarbete (Borkovich & Skovira, 2020; Furnell & Shah, 2020). Enligt Tessian (2020), Tessian (2021) samt Wang, et al. (2021) är anställdas informationssäkerhetsmässiga beteenden försämrade under distansarbete. Dessutom kan det konstateras att 53% av alla anställda i samband med övergång till distansarbete inte har fått tillgång till några nya ISPs (Georgiadou, Mouzakitis och Askounis, 2021).

2.7.2 Förebyggande åtgärder av social engineering-attacker

För att skydda verksamheten mot social engineering-attacker bör verksamheter arbeta på ett förebyggande sätt (Salahdine & Kaabouch, 2019). En av dessa är genom ISPs (Brody et al., 2011). ISP för social engineering innebär, ifall de förstås och efterlevs, att anställda bättre hanterar social engineering-attacker (Brody et al., 2011). Användning av ISPs kan även leda till att anställda värderar information högre, vilket stärker förmågan att motstå social engineering-attacker (Brody et al., 2011). SETA hjälper även anställda att upptäcka och urskilja social engineering-attacker (Brody et al., 2011; Gragg, 2003; Peltier, 2006; Whitman & Mattord, 2008). En av dessa är att anställda värderar informationen högre och att detta är stärkande i motståndet av social engineering-attackerna (Brody et al., 2011). Det är därför viktigt att verksamheter vidtar vissa åtgärder för att öka medvetenheten om social engineering (Brody et al., 2011; Salahdine & Kaabouch, 2019).

2.7.3 Mitigering av intrång genom social engineering-attacker

Attacker mot människor är svåra att detektera, verksamheter bör därför arbeta med dess mitigering (Salahdine & Kaabouch, 2019). Mitigering innebär att minimera skadan av en attack eller ett intrång i så stor utsträckning som möjligt (Salahdine & Kaabouch, 2019). Detta görs när en attack eller intrång i verksamheten har skett (Salahdine & Kaabouch, 2019). Verksamheten måste vidta åtgärder för att minska attackens påföljder (Salahdine & Kaabouch, 2019). Det finns två tillvägagångssätt att arbeta med mitigering av den mänskliga faktorn, den första är granskning och ISPs (Zulkurnain et al. 2015; Salahdine & Kaabouch, 2019). Detta

utgörs av säkerhetsregler och processer för att motverka social engineering-attacker mot anställda i verksamheten (Salahdine & Kaabouch, 2019; Zulkurnain et al. 2015). Detta tillvägagångssätt är en försvarsstrategi vars ändamål är att kontrollera den anställdas reaktion vid attack (Salahdine & Kaabouch, 2019). Granskning är till för att komplettera ISPs genom att testa medvetenheten eller utsattheten av social engineering (Zulkurnain et al. 2015). Den andra är utbildning, träning och medvetenhet (Zulkurnain et al. 2015; Salahdine & Kaabouch, 2019). Detta tillvägagångssätt syftar till att tillämpa och applicera ISPs och granskning i verksamheten (Salahdine & Kaabouch, 2019; Zulkurnain et al. 2015). Denna mitigeringsmetod kan även för verksamheter bidra till att anställda vet vart de bör rapportera överträdelse av en ISP, bl.a. (Whitman & Mattord, 2008). Mänskliga mitigationstekniker är viktiga för att en verksamhet ska kunna minimera effekten av svagheter hos de anställda (Whitman & Mattord, 2008; Salahdine & Kaabouch, 2019).

Man kan dessutom arbeta med säkerhetskultur som en mitigeringsmetod (Salahdine & Kaabouch, 2019; Puhakainen & Siponen, 2010; Siponen, Pahnila, & Mahmood, 2010). Detta bidrar till sannolikheten att anställda rapporterar suspekta aktiviteter (Salahdine & Kaabouch, 2019). Ett sätt att arbeta med mitigering är genom säkerhetskultur (Salahdine & Kaabouch, 2019; Puhakainen & Siponen, 2010; Siponen, Pahnila, & Mahmood, 2010). En positiv säkerhetskultur hjälper den som blev utsatt för attacken att inte känna skam över att ha blivit lurad (Salahdine & Kaabouch, 2019). Detta kan även medföra att de anställda vågar rapportera attacker direkt och på så sätt kan skadan minimeras (Salahdine & Kaabouch, 2019). I samband med tekniska verktyg möjliggör detta att upptäcka och undvika attacker (Salahdine & Kaabouch, 2019).

3 Metod

3.1 Forskningsmetod

Denna uppsats har tillämpat kvalitativa intervjuer som insamlingsmetod. Detta beslut har tagits i och med några huvudsakliga faktorer. En av dessa är att en kvalitativ metod är som mest lämplig ifall avsikten är att skapa större klarhet och en nyanserad beskrivning (Jacobsen, 2002). Detta ansågs som relevant för utförandet av denna studie då syftet är att beskriva informationssäkerhetsutmaningar och dess hantering. Vidare uttrycker Jacobsen (2002) att en kvalitativ metod är lämplig för de fall då fokus läggs på sambandet mellan individ och kontext. Den mänskliga faktorn och hur verksamheter hanterar denna är centralt för verksamheten, vilket ligger i linje med författarens resonemang för kvalitativa metoder.

Angående en kvantitativ metod beskriver Jacobsen (2002) detta som bäst lämpad för de studier som intresserar sig för ett fenomens frekvens eller omfattning. Syftet med denna uppsats berör inget av dessa två aspekter, vilket stödjer valet av en kvalitativ metod.

3.2 Urval av respondenter

I urvalet av respondenter har vi riktat oss till CISOs (Chief Information Security Officer) samt chefer eller experter inom IT, informationssäkerhet och cybersäkerhet. Vilket ökade möjligheten att få informativa och kvalitativa svar. Utöver detta har det inte tagits hänsyn till storleken eller branschen för respondenternas verksamhet. Som tillvägagångssätt för att hitta potentiella respondenter har plattformen LinkedIn använts. Det söktes på anställda med yrkestitel CISO och individen kontaktades därefter antingen genom plattformens meddelandefunktion eller genom e-post. Vi fick även tillgång till en respondent via personliga kontakter. Alla meddelanden som skickades till potentiella respondenter återfinns i bilaga 7.3.1.

Vi har valt att anonymisera samtliga respondenternas namn och verksamhet.

Tabell 2: Respondenter

Respondent	Verksamhet	Roll	Återfinns i kapitel
R1	Bank	CISO	7.2.1
R2	Detaljhandel	Senior Security Engineer	7.2.2
R3	Patentskydd	CISO	7.2.3
R4	Patentskydd	Säkerhetskonsult	7.2.4

3.3 Intervjuer

3.3.1 Utförande av intervjuer

För utförande av den kvalitativa metoden har öppna individuella intervjuer tillämpats. En öppen individuell intervju innebär att informationen som insamlas utgörs av ord, meningar och berättelser (Jacobsen, 2002). Detta är mest lämpligt bl.a. när få deltagare undersöks (Jacobsen, 2002). Detta är av vikt för uppsatsen då tillgängligheten på respondenter är begränsad i och med den yrkestitel eller erfarenhet som krävs. Dessutom fanns en tidsmässig begränsning på studiens utförande vilket även påverkade antalet intervjuer som kunde genomföras. Jacobsen (2002) beskriver även att personer tycks ha lättare att tala om känsliga ämnen ansikte mot ansikte, i jämförelse med per telefon. Eftersom att säkerhetsfrågor kan utgöra känslig information (Dandurrand & Serrano, 2013) är detta relevant för utförandet av intervjuerna. Dagens teknologi möjliggör ett möte med video och ljud, därför ansågs detta vara den bästa möjliga lösningen med hänsyn till känslighet och utförbarhet, i och med att det geografiska avstånd mellan oss och respondenterna var betydande. Därmed utfördes samtliga intervjuer online. Vi valde att använda oss utav mjukvarutjänsten Zoom för våra intervjuer. Detta då tjänsten har en gedigen funktionalitet för inspelning av ljud samt att det finns vana att använda mjukvaran hos oss.

3.3.2 Bearbetning av intervjuer

Bearbetning av intervjuerna påbörjades genom transkribering, varav Word Onlines transkriberingsverktyg användes. Detta för att generera en grundtext, varav denna sedan redigerats och bearbetats för att framställa den slutliga transkriberingen. Viss korrigering gjordes även för att undvika störande av läsbarhet. Detta rör sig huvudsakligen om upprepningar såsom “vi vi vi”, detta har då ändrats till “vi”. Även förekomsten av orden

"liksom" och "så" togs bort, vid de fall det stör läsbarheten. Extra noggrannhet har lagts på att endast redigera bort de störningsmoment som inte påverkar innebörden av texten.

Följande symboler har använts i transkriberingen.

Tabell 3: Symboler och dess betydelse i transkriberingen

Symbol	Betydelse
[***]	anonymisering av namn, verksamhet, eller känslig data.
[xxx]	Ord som är svåra att höra under inspelning

3.3.3 Irrelevant data

Uppföljningsintervjuer utfördes med samtliga deltagare. Detta gjordes då mycket innehåll i första intervjun inte upplevdes tillräckligt relevant för forskningsfrågan. Det är uppföljningsintervjuerna som har utgjort det huvudsakliga innehållet till denna studie.

3.4 Kvalitetssäkring av studie

3.4.1 Etik

Jacobsen (2002) redogör för tre grundläggande krav inom etiskt utförande av en undersökning. Dessa är informerat samtycke, krav på privatliv och krav att bli korrekt återgiven (Jacobsen, 2002). Det förstnämnda kravet, informerat samtycke, innebär att deltagandet i undersökningen ska vara frivilligt (Jacobsen, 2002). Jacobsen (2002) beskriver detta som att valet att delta ska ske utan påtryckningar från andra. För att tillgodose detta har varje respondent, vid varje intervjutillfälle, informerats om att deltagandet är frivilligt och att samtycke till deltagande kan återkallas när som helst. Det andra kravet, krav på privatliv, behandlar aspekter såsom hur känslig den informationen som samlas in är samt möjligheten att identifiera individer utifrån denna information (Jacobsen, 2002). I och med att säkerhetsfrågor kan utgöra känslig information (Dandurrand & Serrano, 2013) har extra vikt lagts på att bibehålla respondenternas privatliv. Dessutom beskriver Jacobsen (2002) att de som utför undersökningen måste kunna garantera att det vidtas åtgärder för att hindra att andra ska kunna identifiera en respondent. Ett exempel på hur detta har efterföljts är anonymisering av en respondents verksamhet, trots att denne gav samtycke till att inkludera verksamhetens namn. För samma respondent har även vissa ord exkluderats ur transkriberingen. Detta gjordes på grund av möjligheten att härleda informationen i respondentens svar, yrkesroll och verksamhetsnamn till dennes fulla identitet. Det tredje och sista kravet, krav att bli korrekt återgiven, innebär att eftersträva öppenhet i forskningsprocessen och återgivning av resultat i helhet (Jacobsen, 2002). För att tillgodose detta återfinns samtliga transkriberingar av intervjuer samt kommunikationen mellan författarna och respondenterna som bilagor.

3.4.2 Validitet

Med validitet menas att empirin ska vara giltig och relevant alltså att mäta det som studien ämnar att mäta (Jacobsen, 2002). Jacobsen delar in giltighet i två delar, varav den första är intern giltighet och den andra är extern giltighet (Jacobsen, 2002). Intern giltighet handlar om att faktiskt mäta det som studien har ämnat att mäta (Jacobsen, 2002). Jacobsen (2002) ger som exempel på detta en studie då organisationskultur mäts. Ifall en organisation hade både en viss kultur, och stor framgång, kan inte slutsatsen dras att kulturen skapade framgången, då det är oklart ifall det faktiskt är kulturen som lett till framgång (Jacobsen, 2002). I detta avseende väcks frågan ifall det faktiskt är just kultur som mätts, eller något annat (Jacobsen, 2002). Denna studie avser att beskriva informationssäkerhetsmässiga utmaningar och dess hantering. Detta är inte i korrelation med andra faktorer, utan det som ämnats att beskriva är även det som redogjorts för i det empiriska resultatet, diskussion samt slutsats. Därför bör denna uppsats ha intern giltighet. Extern giltighet och relevans innebär att resultatet är giltigt i andra sammanhang också, som till exempel en annan organisation (Jacobsen, 2002). Det handlar alltså om hur väl det går att generalisera till andra sammanhang (Jacobsen, 2002). För att stärka den externa giltigheten valdes våra respondenter helt utan beaktande av deras verksamhets bransch eller storlek. Avsikten var att få med en bredare blandning av verksamheter, där det resultat som nås inte är beroende av verksamhetens egenskaper. Därmed fick vi in en god variation av verksamheter i både privata och offentliga sektorn samt storlek. Det som försvagar den externa giltigheten av studien är att samtliga personer som intervjuades jobbar på något sätt med informationssäkerhet.

3.4.3 Reliabilitet

Reliabilitet innebär att studien är tillförlitlig och trovärdig (Jacobsen, 2002). För att uppnå detta krävs det att studien utförs korrekt (Jacobsen, 2002). Jacobsen (2002) säger att studien ska kunna få samma resultat om den utfördes igen. Detta är något som är svårt med en kvalitativ studie med semistrukturerade intervjuer då följdfrågorna kan skapa en skillnad i resultaten. Kvale (1996) skriver i sin bok att intervjufrågor inte ska vara ledande för att stärka reliabiliteten. I de intervjufrågor som ställdes undveks att de på något sätt skulle vara ledande, följdfrågorna kunde däremot ha en viss ledning. Till exempel kunde detta ske ifall svarens relevans till forskningsfrågan var för låg inte var riktade mot forskningsfrågan om respondenten gick utanför ämnet.

.

4 Empiriska resultat

Vid citat ur intervjutranskriberingen har vissa avsnitt innan eller efter citatet exkluderats ifall de inte bidrog till innehållet. Detta har markerats med symbolen [...]. Vid referens till intervjutranskriberingen har radnummer angetts inom parentes. Vidare har vilken av de två intervjuerna som refereras till anvisats genom förkortningarna I1 och I2 (Intervju 1 och Intervju 2).

4.1 Social engineering-attacker

R1 (66:I1) beskriver att verksamhetens fysiska säkerhet mot intrång gällande dess kontor och byggnader är väldigt hög. Däremot beskriver R1 (66:I1) även att vid distansarbete är detta helt utanför verksamhetens kontroll. R1 (66:I1) uttrycker här att det är svårt att veta om anställda utsätts för shoulder surfing, t.ex. i samband med läsning av e-post på pendeltåget. R1 (67:I1) får som följdfråga till detta ifall de kunnat följa upp huruvida intrång sker i denna situation. R1 (68:I1) uttrycker då att det är en risk, att det kan hända, och att denne inte riktigt löst problemet. R1 (68:I1) beskriver det som att den enda möjligheten är att utbilda, men vidare uppföljning är svårt. Respondenten säger att denne vill tro att de människor som sysslar med riktigt känslig information agerar som man bör agera (R1, 68:I1).

> *"Jag vill tro att människor som sysslar med riktigt känslig information här, alltså, de agerar så som man bör agera. Jag upplever att människor är ganska mogna, men risken är absolut inte. Ja, den är nog inte ens minimal. Det kan hända, så är det." - R1 (68*:I1*)*

Gällande att skydda mot sociotekniska attacker uttryckte R3 (90, I1) att just phishing är speciellt utmanande och att attackerna blir alltmer sofistikerade. Ett exempel på detta är BEC-attacker, vilket står för Business Email Compromise-attacker, som även beskrivs som en form av Impersonation attack (R3, 81:I1). R3 (81:I1) uttrycker att dessa BEC-attacker används för att utge sig för att vara en annan verksamhet. Vidare beskriver respondenten att detta sedan används för att t.ex. skriva vidare på en e-posttråd, med samma språkstil och signatur (R3, 81:I1). På denna punkt säger R3 (81:I1) till sist att e-post och phishing har blivit ett av det absolut största hoten mot deras verksamhet.

> *"Jag skulle säga att email och phishing och så har blivit ett av de största, absolut största hoten som vi har." - R3 (81*:I1*)*

R2 (41:I2) beskrev även att ledningens medvetenhet kring risken att medarbetare kan utsättas för social engineering vid distansarbete också är beroende av andra hot som uppstår i samband med det nuvarande generella säkerhetsläget. R3 (47:I2) uttryckte även problematik i samband med tidspressen vid hantering av intrång, i och med att virus kan sprida sig till många andra system på bara 10-15 minuter. Att identifiera och bemöta hotet på kort tid upplever respondenten som speciellt svårt, då det dessutom ofta är flera simultana händelser på en gång att uppmärksamma vid intrång (R3, 47:I2). R4 (12:I2) beskrev svårigheter vid

attacker social engineering-attacker då de utger sig för att vara en kollega man jobbat med i under lång tid och därefter skickar meddelanden av samma karaktär som kollegan skulle ha gjort.

R4 (16:I2) angav att de inte utför någon aktiv handling för att skydda verksamheten mot social engineering-attacker vid just distansarbete och att de inte skiljer på detta. Respondenten angav även att de inte haft några incidenter i samband med social engineering vid distansarbete och därför inte har detta på agendan (R4, 22:I2). Till frågan hur de skyddar sig mot phishing vid distansarbete särskilde respondenten heller inte på detta från arbetet på kontoret (27, R4:I2). Respondenten angav också att de inte har kommit i kontakt med någon som drabbats av social engineering-attacker, men att de kunnat se att det fungerar när de utfört egna testar (R4, 29:I2). Vidare beskriver respondenten att phishing-incidenter har förekommit, men att denne inte ser detta som social engineering (R4, 29:I2). Gällande phishing-attacker vid distansarbete anger respondenten att det finns svårigheter i hur sofistikerade attackerna har blivit (R1, 20:I2). Dessutom beskriver respondenten att den utvecklingen fortsätter och att avancerade phishing-attacker med AI-element som fejkade videos, förr eller senare kommer att nå oss (R1, 20:I2). För att motarbeta phishing-attacker köper respondentens verksamhet extern intelligens, varav respondenten ger ett exempel på intelligens som Security Operations Centre-tjänster (SOC) (R1, 24:I2). Dessa tjänster kan övervaka och meddela händelser som aktivitet på dolda delar av internet samt ändra kanaler (R1, 24:I2). Respondenten uttrycker även att de i samband med detta får rapporter som är skräddarsydda för deras verksamhet (R1, 29:I2). Detta beskriver respondenten som omvärldsbevakning (R1, 22:I2).

4.2 Informationssäkerhetskultur

Gällande säkerhetskultur i samband med distansarbete svarade R1 (49:I1) att det påverkas av deras personalomsättning. Respondenten nämnde även att de har startat ett projekt om hur man blir en kulturbärare (R1, 49:I1). Detta projekt är dock inte bara inriktat på informationssäkerhet utan innehåller flera andra aspekter (R1, 49:I1). R1 (83:I1) nämner också att de outsourcar till en tredje part. Det framkommer då att det är svårare att få en samhörighetskänsla till verksamheten vilket blir en risk (R1, 83:I1). I intervjun med R2 (50:I1) var svaret att det hålls awareness-veckor. R2 (50:I1) nämner dock att i det stora hela är det upp till varje individ och att det viktiga är att ändra tankesättet snarare än att skapa fler policys och verktyg vilket är något de satsat på under pandemin. R3 (57:I1) beskrev å andra sidan att det inte har skett någon ändring med säkerhetskulturen utan beskriver istället att det är en extern hotbild som härstammar från internet istället. R3 (67:I1) nämner dock att med distansarbete försvinner den informella diskussion om IT-säkerhet. R3 (67:I1) ger som exempel på detta att man annars behöver ringa någon via en mötestjänst, vilket respondenten beskriver som mer formellt. Fortsättningsvis så har R3 arbetat för att skapa en kultur genom en policy som säger att man inte lägger skulden på någon om de råkat göra något (R3, 69:I1). Detta för att undvika att anställda tar dåliga beslut själva (R3, 69:I1). Eftersom det är enligt R3 farligt att ha en kultur där anställda inte vågar berätta saker (R3, 71:I1).

R4 (31:I1) uttryckte att trots att säkerhetsincidenter sker har dessa inte effekt nog att få påverkan på verksamheternas säkerhetsarbete. Respondenten beskriver även att en faktor i denna aspekt är att säkerhetsincidenter inträffar förhållandevis sällan (R4, 31:I1). Vidare angav R4 (31:I1) att branschen som verksamheten tillhör har en effekt på deras vilja, eller ovilja, att arbeta med informationssäkerhet.

> *"Det är svårt att få gehör för det här av den enkla anledningen att det händer inte tillräckligt mycket grejer som får de konsekvenserna så att du faktiskt skulle börja jobba med det här"* - R4 (31:I1)

R3 (22:I2) nämnde att respondenten, med sin roll som CISO, inte sitter i ledningsgruppen. Vidare uttryckte respondenten att ifall denne vore i ledningsgruppen skulle det ha en positiv effekt på medvetenheten i verksamheten (R3, 22:I2). R3 (22:I2) beskrev också att om en säkerhetskultur finns i bolaget lär de även vilja ha CISOn i ledningsgruppen, men om inte denna kultur finns anses det oviktigt. R3 (22:I2) uttrycker det som en mognadsfråga och att detta avgörs av hur viktigt organisationen anser att detta är för dess kärnverksamhet.

R3 (40:I2) beskrev även att arbetet med säkerhetskultur är svårare under distansarbete p.g.a avsaknad av informell diskussion efter ett utbildningsmoment. Respondenten uttryckte att när denne har haft utbildningar eller föredrag med fysiskt deltagande har det funnits en möjlighet att föra en informell diskussion, ställa frågor och engagera sig (R3, 40:I2). Detta beskrev respondenten som mycket fördelaktigt i avseendet att få ut ett budskap samt det faktum att detta inte finns har en påverkan på säkerhetskulturen (R3, 40:I2). R3 (42:I2) beskrev även att engagemang kan bidra till att en chef som deltagit på föredrag kan sprida vidare budskapet till sin organisation och på så vis skapa effekt. R1 (75:I2) angav att säkerhetskulturen har till viss del gått förlorad under distansförhållanden, speciellt för de anställda som påbörjat anställning när verksamheten redan arbetar på distans, som under COVID-19-pandemin.

4.3 ISP för social engineering och dess efterlevnad

Vid frågan om verksamheten har några policys speciellt utformade för social engineering i distansarbete så svarade R2 (6:I2) att de finns i andra policys och att de är väldigt väl utarbetade kring vad man får och inte göra. R3 (6:I2) säger att det är svårt att få anställda att läsa policys. Vidare säger R3 (8:I2) att de försöker skriva lättläsliga policys men att det förekommer långa policydokument. Vidare uttrycker R2 (6:I2) att det är svårt att göra policy för social engineering. R4 (2:I1) säger att de inte har några som är specifikt för distansarbete. Det finns en introduktion med "end user guideline" där det finns information om hur anställda ska agera med "mobile devices" och även social engineering (R4, 4:I2). Vidare berättar R4 (4:I2) att de inte haft några utökade policys i samband med det allt mer förekommande distansarbetet under pandemin. R1 (3:I2) angav att de har specifika policys för distansarbete, samt att det även finns policys som berör social engineering men att dessa företrädesvis är punkter på detaljnivå i en mer generell policy. Respondenten angav också att det görs mätning av distansarbete, men respondenten uttryckte inget samband till social engineering i denna aspekt (R1, 9:I2). För social engineering görs tester för phishing och liknande angrepp (R1, 9:I2).

Vidare anger R2 (88:I1) att de restriktioner och policys du behöver beaktat beror på vilken del av organisationen man tillhör och att detta utgör ett förbättringsområde för verksamheten. Respondenten ger som exempel på detta att för anställda som arbetar inom säkerhet finns det angivelser med syfte att skydda mot säkerhetsintrång (R2, 88:I1). T.ex. finns det begränsningar för vilka typer av Wi-Fi man får ansluta till eller krav på privacyfilter på datorer (R2, 88). Däremot finns det andra medarbetare som dessa policys inte appliceras på och detta faktum kan enligt respondenten därmed utgöra en risk för läckage av känslig data genom att t.ex. arbeta på offentliga platser, eller via ett publikt Wi-Fi (R2, 88).

4.4 SETA

I frågan om hur respondenterna skyddar sin verksamhet mot social engineering i distansarbete svarade R2 (12) att det handlar mycket om medvetenhet. R2 (12:I2) beskrev också att verksamheten arbetar mycket med träning genom olika tester, och när det har skett intrång förklarar de hur man ska arbete i framtiden. Fortsättningsvis säger R2 (12:I2) att medvetenhet är ett effektivt skydd mot att förhindra social engineering-attacker. R3 (14:I2) säger att de utbildar sina anställda men beaktar inte distansarbete, det är snarare en generell utbildning. Vidare nämner R3 (14:I2) att det kan vara viss skillnad i att distansarbete är mer mottagligt för attacker då medarbetare är mer isolerade hemma och att de kanske inte är lika noggranna eftersom det kan vara svårare att kommunicera med kollegor. R4 (16:I2) svarade också att denne inte skiljer på det. R1 (14:I2) angav att de arbetar mycket med generell utbildning, introduktionsutbildning, information och även specifika läromoment utformade enligt specifika behov. Till exempel angav respondenten att de utfört utbildning i källkritik i och med en förväntan på ökad mängd påverkanskampanjer i samband med kriget i Ukraina (R1, 14:I2). Respondenten uttrycker i den aspekten att de inte alltid utför utbildningar själva utan att de istället köper in det som en tjänst (R1, 14:I2). R1 (40:I2) angav även att de utför utbildningarna ca två till tre gånger per år, exkluderat specialfall som kriget i Ukraina eller i det fall då medvetenheten har upplevts vara ovanligt låg.

När det ställdes en fråga kring medvetenheten gällande social engineering svarade R4 (12:I2) att det finns en medvetenhet när de anställda gör något de inte borde göra. Kring frågan angående genomförandet av utbildningar då man förklarar de större riskerna med distansarbete svarade R2 (25:I2) att det inte har gjorts, utan att befintliga medvetenhetsutbildningar används samt att det inte har behandlats annorlunda. R1 (26:I2) uttryckte kring medvetenhet att anställda har en relativt hög mognadsgrad för risker med social engineering, i och med den mängden utbildning som genomförts, samt att tester har stärkt detta. I den aspekten uttrycker R1 (29:I2) trots en hög mognadsgrad hos en stor andel av anställda kan det finnas ett antal anställda som inte har samma insikt i risker för social engineering. I detta beskriver respondenten att de behöver jobba med lager av tekniska skydd som överlappar varandra, varav respondenten beskriver detta som lökprincipen (R1, 29:I2). Respondenten anger en svårighet i utförandet av utbildningar, att det inte räcker att bara säga det som behöver sägas och förvänta sig att utbildningsdeltagarna har lärt sig innehållet (R1, 36:I2). Istället säger respondenten att man behöver på ett långsiktigt plan arbeta pedagogiskt och verkligen arbeta in materialet med flera moment, och att hur detta görs eller kan göras beror på utbildningens innehåll (R1, 38:I2). Som exempel ges ifall ett phishing-angrepp har skett, då behöver informationen komma ut snabbt (R1, 38:I2). I annat fall, på ett mer långsiktigt plan, kan man arbeta med utvecklandet av kritiskt tänkande samt att föra en dialog istället för en monolog (R1, 38:I2). Gällande medvetenhet för social engineering-attacker hos deras ledningsgrupp angav respondenten att deras medvetenhet är hög, samt att medvetenheten för distansarbete är extra hög hos ledningen då de ofta jobbar på distans i samband med tjänsteresor (R1, 56:I2).

Respondenterna fick även frågan ifall de har gjort någon speciell anpassning av deras utbildning för distansarbete. På detta svarade R1 (28:I1) att när de påbörjade distansarbete utfördes en utbildning i vad man får och inte får göra samt risker med distansarbete. R2 (33:I1) angav att de har en utbildning för distansarbete men denna täcker inte säkerhetsfrågor utan berör innehåll som arbetsmiljö, ergonomi och dylikt. R3 (40:I1) sa att detta inte görs. R3 (40:I1) uttryckte att eftersom att distansarbete även har förekommit innan pandemin är det ingen större ändring, utan den enda ändringen är volymen av anställda som arbetar hemifrån.

R3 fick gällande detta en följdfråga, huruvida de särskiljer distansarbete eller inte. R3 (42:11) bekräftade att de inte särskiljs. R4 (24:I1) uttryckte att utbildningar för distansarbete inte existerar i deras verksamhet. Istället säger R4 (24:I1) att distansarbete är något som verksamheten "vuxit in i", och att det inte funnits några angivelser om att det ska gå till på ett visst sätt.

R4 (17:I1) tillfrågades i vilken utsträckning de utbildar personal i social engineering. Som svar angav respondenten att nyanställda går igenom olika utbildningspaket där IT och informationssäkerhet täcks (R4, 18:I1). Vidare uttrycker R4 (18:I1) att det utförs tester några gånger per år i form av phishing-attacker och fejkat e-postutskick. Däremot anger respondenten att utöver detta är det är upp till var och en att leta bland informationen som finns i verksamhetens allmänna informationsflöde för att hålla sig uppdaterad (R4, 18:I1). Till detta bör tilläggas att R4 (18:I1) uttrycker att anställda har eget intresse (p.g.a. att deras bransch involverar säkerhet) vilket enligt R4 (18:I1) minimerar behovet för verksamheten att utföra utbildning.

> *"Men annars är det ganska mycket upp till var och en alltså. Det finns information att hitta, men då måste man ju själv leta upp det, så det är ingen som sitter och naggar oss anställda för att hålla oss uppdaterade i vad som händer och sker. Utan det är i det allmänna informationsflödet på bolaget."* - R4 (18:I1)

R2 (16:I2) angav att anställda kan utsättas för ett överflöd av information vid distansarbete, på annat sätt än ifall denne befinner sig på kontoret. Respondenten uttryckte att i och med att man hanterar flera kanaler på en gång är det mer sannolikt att man missar identifiering av riskfaktorer för något man i annat fall skulle ifrågasatt (R2, 16:I2). Respondenten sa även att vid en social engineering-attack framkallas ofta ett inslag av stress och tidspress, för att skapa denna effekt. Till sist nämnde även R2 (16:I2) att trots att en anställd kan ha genomgått utbildning i social engineering kan man glömma dessa riskfaktorer, speciellt under stress och tidspress R2 (16:I2).

4.5 Mitigering

I frågan gällande verksamhetens mitigering av social engineering-attacker svarar R4 (49:I2) att de rapporterar och övervakar. Vidare nämner R4 (49:I2) att de har eskaleringsrutiner där de klassificerar en incident och i efterhand analyserar händelsen. Vid misstanke om stora ekonomiska konsekvenser tar man in den kompetens som eftersöks. R2 (45:I2) gav ett exempel på en phishing attack där en anställd råkar skicka sina inloggningsuppgifter. Då finns det funktioner som detekterar detta vilket sätter igång en automatisk process som resulterar i att kontot blir låst och lösenordet byts ut (R2, 45:I2). Vidare beskriver R2 (45:I2) att detta kanske orsakar en förlust på en halv dags arbete, vilket är bättre än att det får sprida sig. Fortsättningsvis beskriver R2 att verksamhetens detekionsavdelning använder en funktionalitet som är väldigt stark. Detta i samband med att verksamheten har "playbooks" för att hantera olika social engineering-scenarion via färdiga processer (45:I2). Vid följdfrågan om huruvida detta blir svårare vid distansarbete svarade R2 (47:I2) att det antagligen inte spelar någon roll. Respondenten fortsatte med att säga en viss del av hur de detekterade hade försvunnit i och med att anställda inte alltid använder företagets nätverk vilket resulterat i att de fått hitta andra sätt att få till detektionsfunktionaliteten. R3 (34:I2) berättar att de arbetar mycket med säkerhetslager.

> *"Det är inte ett system som ska detektera eller förhindra angrepp, utan du ska ha olika typer av system på olika lager som hjälper till att detektera angrepp och förhindra det." - R3 (34:I2)*

R1 (58:I2) anger kring mitigering att även de jobbar mycket med lager, att de behöver jobba med skydd och hantering via olika tjänster och lösningar (R1, 58:I2). Respondenten angav att vad de gör vid en incident beror på vad det är för incident (R1, 60:I2). Till detta gavs exemplet att en anställds inloggningsuppgifter läckt ut. Som svar uttryckte respondenten att de inte har några färdiga recept på det, utan att de arbetar mer proaktivt genom att skydda känslig information bättre än okänslig information (R1, 62:I2). Respondenten angav även att de använder SOC-tjänster för mitigering, vilket möjliggör snabb respons på intrång dygnet runt (R1, 64:I2). I detta uttryckte respondenten att distansarbete inte har någon större påverkan, att de är ungefär lika snabba oavsett plats (R1, 66:I2). Respondenten uttryckte att medarbetarna ur ett säkerhetskulturellt perspektiv är ganska handfallna, men att de samtidigt vet att man t.ex. bör koppla loss från nätverk (R1, 71:I2), samt att rapportera intrånget (R1, 73:I2). Dessutom angavs det att dessa procedurer är något medarbetarna bör känna till men att många säkert inte efterlever dem på grund av lathet, stress, eller brist på tid eller ork (R1, 73:I2). Respondenten uttryckte även att de försöker etablera en accepterande säkerhetskultur vid intrång, snarare än en skuldbeläggande sådan (R1, 73:I2). Respondenten uttryckte även svårigheter i tidsaspekten vid mitigering av social engineering-attacker (R1, 83:I2). I detta beskrev respondenten att de förväntas tillgodose marknaden med finansiella tjänster och att intrång kan hota detta (R1, 83:I2; R1, 85:I2).

5 Diskussion

5.1 Förebyggande åtgärder mot social engineering-attacker

5.1.1 Social engineering-attacker

En utmaning som uppstod i samband med social engineering-attacker är risken att utsättas för shoulder surfing-attacker vid distansarbete. Enligt (Salahdine & Kaabouch, 2019) är shoulder surfing en attack som går ut på att utan en individs vetskap se på när denne anger lösenord eller användarnamn i ett digitalt system. Det nämndes att vid distansarbete är social engineering-attacker som denna svåra att kontrollera då de är utanför verksamhetens uppsyn. Gällande hantering av denna utmaning nämndes tre olika aspekter som kan nyttjas. Dessa var ett tekniska medel som ett skärmskydd som begränsningar vilka vinklar skärmen kan ses från, begränsning på var anställda får jobba ifrån, samt bättre utbildning och medvetenhet.

Phishing som social engineering-attacker uppkom väldigt mycket i empirin. Det uttrycktes flera olika problematiska aspekter. och detta beskrevs även som ett av de absolut största hoten mot deras verksamhet. Det faktum att phishing-attackerna blivit så pass sofistikerade är en utmaning som beskrivs som svårhanterlig. Detta stämmer överens med litteraturen, då Krombholz et al. (2015) och Ivaturi & Janczewski (2011) har beskrivit phishing som väldigt vanligt förekommande.

5.1.2 Informationssäkerhetskultur

Det var flera respondenter som beskrev säkerhetskulturella utmaningar i arbetet mot social engineering-attacker, samt aspekter då den säkerhetskulturen uteblir eller brister. En aspekt av detta var möjligheterna till informell diskussion i samband med utbildning, då dessa blir sämre, vilket angavs påverka säkerhetskulturen negativt. Det finns underlag från empirin som visar att i säkerhetsarbetet spelar kultur i form av utbildning och informell diskussion en stor roll, men att dessa moment under distansarbete är mer utmanande och tappar viss effekt. En aspekt av detta är anställda som börjat under COVID-19-pandemin. Kultur i säkerhetsarbetet beskrivs som positivt bidragande till informationssäkerhet (Siponen, Pahnila, & Mahmood, 2010; Van Niekerk & von Solms, 2010; Eloff & Von Solms, 2000; Von Solms, 2000; Louw, Thomson & von Solms, 2006, Salahdine & Kaabouch, 2019). Dessa utmaningar vid distansarbete utgör därför en bristfällighet. I empirin framkom ett sätt att hantera detta, vilket var att försöka skapa effekt genom att utbilda chefer inom organisation, varefter dessa sedan kan sprida budskapet vidare till fler chefer och deras organisationer.

Det uttrycktes vid flertal tillfällen att säkerhetskulturen och resursallokeringen till säkerhetsarbetet är beroende av den skadliga effekten av intrång, samt att denna effekt i vissa fall inte är tillräcklig för att faktiskt motivera verksamheter till att prioritera säkerhetsarbetet högre. I vissa fall, enligt empirin, har denna utmaning att göra med att det överhuvudtaget inte skett något intrång. Samtidigt angavs det att genom tester har det kunnats bekräftas att social

engineering-attacker mot deras verksamheter fungerar. I empirin framkommer också att i vissa fall är verksamheten medveten om dess effektivitet och risker, men att de trots det ger arbetet mot social engineering en låg prioritering. I andra sammanhang beskrevs hur det generella säkerhetsläget i samband med kriget i Ukraina haft en påverkan på säkerhetsarbetet och prioriteringen av social engineering-aspekter. Litteraturen beskriver att den mänskliga faktorn behöver prioriteras högre (Borkovich & Skovira, 2019; Brody et al., 2011). Faktumet att respondenternas verksamheter nedprioriterar arbetet utgör därför ett problem, men det finns visst stöd i empirin för att arbetet mot social engineering kommer prioriteras högre i takt med det generella säkerhetsläget.

5.1.3 ISP och dess efterlevnad

Eloff & Höne (2002) beskriver i litteraturen att ISPs är en essentiell aspekt för att förebygga intrång. Det framgår av empirin att de tillfrågade verksamheterna inte har specifika ISPs för social engineering vid distansarbete utan att de finns beskrivet i andra policys. Till exempel beskrevs det att de inte har specifika policys för distansarbete utan i deras “end user guide lines” finns det policys om hur anställda ska agera med “mobile devices” och social engineering. En respondent uttryckte att social engineering är svårt att göra policys för. Litteraturen säger att användningen av ISP kan leda till att information värderas högre (Brody et al., 2011). Vidare framkom det att ISPs varierar beroende på vilken del av verksamheten du tillhör. Det kan också orsaka risken att konfidentiell information läcker ut då det enligt respondenten inte finns ISPs på vissa avdelningar för distansarbete och vilka nätverk som får användas. Vidare skriver Samonas & Coss (2014) att ISPs ska vara utformade med utförbarhet i tanke då de annars riskerar att inte följas. Empirin visade på att detta är något som avses att följa, men att dock fortfarande förekommer långa policydokument. Detta kan påverka efterlevandet av ISPs då anställda är mindre benägna att läsa dem.

5.1.4 SETA

I litteraturgenomgången beskrevs vikten av SETA i arbetet mot social engineering-attacker. Det har även beskrivits hur distansarbete påverkar medarbetares förhållningssätt till säkerhetsrisker, säkerhetsrutiner, riskbenägenhet, m.fl. Empirin visade underlag för att även verksamheter placerar stor vikt i nyttjandet av SETA. Gällande distansarbete och dess konsekvenser för informationssäkerhet var det däremot ingen verksamhet som svarade att de utför utbildningar gällande social engineering-attacker vid just distansarbete. I ett fall hade till och med risken för att distansarbetande anställda skulle utsätts för social engineering-attacker uppmärksammats, men att det ändå inte behandlas annorlunda. En aspekt som framkom i empirin var även att det finns andra hot just nu som är högre prioriterat än arbetet mot social engineering vid distansarbete.

Kring medvetenhet har empirin gett underlag för att medvetenhet anses vara av hög vikt. Detta stärker resonemanget som förs av Ceraolo (1996), Goodhue & Straub (1989), Hoffer & Straub (1989), Straub (1990), Straub & Welke (1998). En utmaning som nämndes i detta var att trots hög generell medvetenheten hos anställda kring social engineering-attacker, kan en liten andel anställda med lägre medvetenhet utgöra ett problem. Enligt empirin hanteras bäst utmaning genom att arbeta med flera lager av skydd i olika skikt, vissa tekniska och vissa riktade mot människan. Detta multidimensionella arbetssätt är dessutom i linje med den information som redogörs för av Brody et al. (2011) samt Salahdine & Kaabouch (2019).

Det framgick även av empirin att stor vikt lämpligen bör läggas vid att befästa utbildningsinnehåll via flera olika metoder. Detta då det är osannolikt att deltagarna på ett långsiktigt plan skulle ha lärt sig innehållet på endast ett tillfälle. En aspekt som beskrevs som utmanande i arbetet mot social engineering vid distansarbete är att man i hemmet ofta hanterar flera en stor mängd information på en gång. Det lyftes att en svårighet är att social engineering-attacker kan avse att skapa tidspress och stress, vilket gör att trots utbildning kan en anställd missa eller glömma signalement för en social engineering-attack. Detta stärker resonemanget som läggs fram av Eminağaoğlu, Eren & Uçar (2009), att utbildning måste göras vid flera tillfällen under en längre period, för att anställda kan glömma innehållet.

5.2 Mitigering av social engineering-attacker

Litteraturen säger att det finns två sätt att arbeta för att mitigera effekten av attacker (Salahdine & Kaabouch, 2019; Zulkurnain et al. 2015). Den första är att verksamheter bör använda sig utav säkerhetsregler och processer för att motverka social engineering (Salahdine & Kaabouch, 2019; Zulkurnain et al. 2015). Detta använder sig respondenterna av genom att de har ISPs och rutiner för att hantera incidenter. Via olika förutbestämda processer som aktiveras när ett intrång har skett. Vissa respondenter nämner även att de har speciella avdelningar för detektion av attacker. Detta går då i linje med vad litteraturen säger angående hur man ska arbeta med mitigering. Vidare är det andra sättet att mitigera genom utbildning, träning och medvetenhet, vilket är ett sätt för verksamheten att verkställa de processer och rutiner som verksamheten etablerat (Salahdine & Kaabouch, 2019). Empirin visar att de tillfrågade verksamheterna utför träning genom tester av social engineering-attacker. Angående mitigering vid distansarbete uppkom det att respondenterna i viss utsträckning anser att mitigering inte påverkas av distansarbete. Det är inte i linje med litteraturen. Detta i och med Tessian (2020), Tessian (2021) samt Wang et al. (2021) redogör för att informationssäkerhetsmässiga beteenden blir sämre vid distansarbete.

En säkerhetskulturell aspekt gällande mitigering som har förekommit i empirin är att flera respondenter uttryckte en avsikt att etablera och nyttja en kultur av förståelse istället för en skuldbeläggande sådan. Gällande informationssäkerhetskultur beskrev Salahdine & Kaabouch (2008) att en positiv säkerhetskultur hjälper den som blev utsatt för attacken att inte känna skam över att ha blivit lurad (Salahdine & Kaabouch, 2019). Dessa två resonemang är alltså i linje med varandra.

En annan svårigheter som framgick i empirin var tidsaspekten i samband med ett intrång. Detta beskrivs som problematisk dels då virus kan sprida sig på bara tio till femton minuter till flera andra system men även att verksamheter vid ett intrång behöver beakta väldigt många faktorer och aspekter på en gång, vilket gör att det kan ta längre tid att bearbeta intrånget samt bromsa in processen.

6 Slutsats

Syftet med denna uppsats har varit att beskriva vilka informationssäkerhetsutmaningar distansarbetande verksamheter ställs inför i deras arbete med att förebygga och mitigera social engineering-attacker samt hur dessa hanteras. Detta gav upphov till att försöka svara på forskningsfrågan:

Vid förebyggande åtgärder och mitigering av social engineering-attacker, vilka informationssäkerhetsutmaningar ställs distansarbetande verksamheter mot och hur hanteras dessa?

I och med studien som utfördes för att besvara detta förekom några huvudsakliga slutsatser.

Social engineering-attacker

I vår forskning framgick det att förebyggande åtgärder mot phishing är ett stort problem och en svårhanterad utmaning, dels på grund av dess sofistikation. Vidare visar studien på att shoulder surfing är en utmaning eftersom det är svårt att veta om de förebyggande medel som används hjälper. Ett sätt att hantera detta som uppkom i studien var användningen av tekniska skydd samt mer utbildning i medvetenhet.

Informationssäkerhetskultur

I studien visades att avsaknaden av möjligheterna till informell diskussion i samband med distansarbete försämrar informationssäkerhetskulturen hos verksamheter. Detta leder till bristfällig informationssäkerhet. Det framkom ett sätt att hantera detta och bättra informationssäkerhetskulturen, vilket var att utbilda chefer i sin verksamhet, och genom detta möjliggöra att dessa sprider budskapet vidare till fler chefer och i sin tur deras verksamheter.

En annan utmaning som framkom var att arbetet mot social engineering vid distansarbete är i vissa fall nedprioriterat på grund av att ett intrång inte orsakat tillräcklig skada för att motivera högre prioritering, om det överhuvudtaget inträffat ett intrång. Enligt studien finns det däremot grund för att detta kommer påskyndas i och med det generella säkerhetsläget.

ISP

Det framgick att det inte fanns specifika ISPs för social engineering-attacker för distansarbetande anställda. Vidare finns det också indikationer på att det kan vara problematiskt för konfidentialiteten att olika avdelningar inte har samma ISPs. I och med detta finns det belägg för att ISP kan vara ett förbättringsområde för distansarbetande verksamheter.

SETA

Studien visar på att verksamheterna i vissa fall är medvetna om riskerna kring social engineering-attacker vid distansarbete, dock reflekteras inte detta i utbildningen och dess innehåll. Det framgick även att det till viss del beror på lägre prioritering för arbetet mot social engineering. Det kan därför konstateras att det finns ett visst utbildningsmässigt förbättringsområde hos verksamheterna gällande risken att utsättas för social engineering-attacker vid distansarbete.

En utmaning kring medvetenhet framkom i studien, vilket var att trots att en verksamhets anställda generellt besitter en hög medvetenhet kring riskerna för social engineering-attacker vid distansarbete kan en liten andel med sämre medvetenhet utgöra ett riskområde. En hantering av detta är användandet av flera lager skydd.

Mitigering

Studien visar att de tillfrågade verksamheterna utför träning genom tester av social engineering-attacker. Angående mitigering vid distansarbete uppkom det att respondenterna i viss utsträckning anser att mitigering inte påverkas av distansarbete vilket kan vara problematiskt för informationssäkerhetsarbetet.

Det visades också att verksamheter tyckte tidsaspekten var en utmaning för mitigering av social engineering-attacker. Detta berodde på att intrånget behöver hanteras snabbt, samt att det ofta tar lång tid att analysera och utreda.

Förslag till framtida forskning

Som sagt är tidsaspekten vid intrång av social engineering-attacker utmanande. I del av hanteringen kring detta uppkom incidenthantering. Detta är däremot utanför denna studiens fokusområde och skulle istället kunna vara aktuellt som framtida forskning. Vidare hade även phishing-attacker utmärkt sig som ett av de största hoten mot informationssäkerheten, delvis på grund av att attackerna numera är väldigt avancerade. Studier som lägger större fokus vid just denna aspekt hade därför varit värdefullt.

7 Bilagor

7.1 Intervjufrågor

7.1.1 Första intervjun

- Kortfattat, vad gör din verksamhet?
- Vad är din roll på verksamheten?
- Vad har du för erfarenhet och/eller bakgrund?
- Hur många dagar i veckan arbetar ni hemifrån?
    - Har ni några speciella regler för detta?
    - Får de anställda bestämma själva?
- I vilken utsträckning utbildar ni er personal i social engineering?
    - Hur går det till, i vilket format?
    - Har ni någon särskild utbildning för distansarbete?
    - Har ni någon särskild utbildning för social engineering-attacker?
    - Utbildar ni anställda i verksamhetens policys?
        - Hur ofta uppdateras utbildningens innehåll?
        - Sker det kontinuerligt?
- Hur säkerställer ni att era säkerhetspolicys följs av anställda?
    - Arbetar ni särskilt med att säkerställa att de följs av distansarbetande anställda?
- Hur arbetar ni med säkerhetskultur i samband med distansarbete? Är det utmanande, isåfall hur?
    - Hur arbetar ni med att säkerställa compliance av policys, gällande säkerhetskulturen?
    - Hur arbetar ni med att säkerställa riskmedvetenhet hos medarbetare?
    - I er verksamhet, vilken roll har ledningen i denna aspekt?

- Kan du beskriva hur ni skyddar er mot social engineering, i form av dessa typer?
    - Fysiska: t.ex. attacker som shoulder surfing och dumpster diving.
    - Sociotekniska: t.ex. Phishing, m.fl.
    - Tekniska: t.ex. OSINT (Open Source Intelligence), m.fl.
    - Sociala: Manipulera eller övertala t.ex. via telefonsamtal.
    - Gör ni något speciellt för distansarbetande, i arbetet mot social engineering?
    - Använder ni några specifika tillvägagångssätt?
- Vilka utmaningar har ni i säkerhetsarbetet mot social engineering?
- Hur arbetar ni med att behålla obehindrad tillgänglighet på data för medarbetare?
- Hur ser det generella säkerhetsläget ut idag hos er verksamhet, i samband med social engineering?
- Hur ser ni på framtiden, i samband med skyddet mot social engineering? Hur arbetar ni för att kontinuerligt bli bättre på att skydda er?
- Finns det något du vill tillägga som vi inte frågat om?

7.1.2 Uppföljningsintervju

- Har ni policys som är specifikt utformade för social engineering vid distansarbete, isåfall vilka?
    - Om inte: varför inte?
    - Om det finns: mäter ni det?
        - Vad har de gett för effekt?
- Hur arbetar ni med att skydda er verksamhet mot social engineering-attacker vid distansarbete?
    - Vad är era utmaningar i detta?
- Hur anser ni att distansarbete påverkar ert arbete mot social engineering?
    - Och mot phishing?
    - Vad gör ni för att motarbeta det?

- Vilka är de största utmaningen i att skydda er mot phishing-attacker vid distansarbete?
    - Hur hanterar ni det?
- Anser ni att anställda i eran verksamhet är medvetna om att distansarbete medför större risker för social engineering-attacker?
    - Varför, varför inte?
    - Vilka är utmaningarna i att skapa denna medvetenhet hos distansarbetande anställda?
- Hur väl insatta är er ledning i social engineering?
    - Finns det ledningsstöd för skyddet mot social engineering?
    - Är ledningen medveten om den ökade risken vid distansarbete?
- Från ett proaktivt perspektiv, hur jobbar ni med att mitigera, mildra eller lindra skadan av en social engineering-attack, ifall det skulle ske?
    - Är det svårare vid distansarbete, isåfall på vilket sätt?
    - Ser ni att säkerhetskultur har en roll i mitigering, vilken isåfall?
    - Vad är ert största problem eller utmaning i mitigering av intrång, alltså att lindra skadan?

7.2 Kommunikation till respondenter

7.2.1 Meddelande till potentiell respondent

Hej _____,

Vi är två Systemvetare från Lunds Universitet som skriver vår kandidatuppsats inom informationssäkerhet. Därför letar vi intervjukandidater från verksamheter vars anställda jobbar både hemifrån och på kontoret.

Vi undersöker hur dessa verksamheter utför & förhåller sig till sitt säkerhetsarbete, varav social engineering och den mänskliga faktorn är av extra intresse.

Vi eftersträvar att intervjua CISO's samt chefer eller experter inom IT, informationssäkerhet & cyber security.

Din profil dök upp här på LinkedIn och vi tyckte att det vore intressant att intervjua dig om ämnet vid en tid som passar dig! Hur låter det?

Mvh
Tarek Bermalm & Albin Olsson

7.2.2 Meddelande för bokning av tid

Hej,

Tack igen för att du ville ställa upp!

Nu börjar vi närma oss intervjutillfällen och hade gärna bokat in en intervju med dig så snart du har tid. På länken nedan kan du välja vilka dagar och tider som passar dig. Vecka 17 skulle vara optimalt för oss, men annars är alla tider lika bra. Mötet sker troligtvis över Zoom, och länk till mötesrummet kommer närmre intervjutillfället.

[Länk för bokning av tider]

Allt gott!
Tarek & Albin

7.2.3 Meddelande inför intervjutillfälle

Hej ____!

Inför intervjun imorgon, ___, kl ____, kommer vi höras på zoom, på denna möteslänk: _____

Frågorna som vi infogat nedan kommer fungera som underlag för intervjun. Observera att ingen förberedelse från er sida behövs, utan vi skickar med dessa bara så du ska kunna få en chans att se vad intervjun kommer att handla om.

Om någon fråga inte vill, kan eller får svaras på är det bara att säga till så går vi vidare till nästa.

Vi kommer anonymisera ditt namn och vi kan även anonymisera verksamhetens namn ifall så önskas. Däremot hoppas vi på att inkludera din jobbtitel i uppsatsen.

Vi kommer även att spela in ljud & bild, varav vi kommer använda ljudet för att kunna transkribera och bearbeta intervjuerna i efterhand. Vänligen säg till ifall detta skulle utgöra ett problem.

Frågorna:

- Kortfattat, vad gör din verksamhet?
- Vad är din roll på verksamheten?
- Vad har du för erfarenhet och/eller bakgrund?

- Hur många dagar i veckan arbetar ni hemifrån?
    - Har ni några speciella regler för detta?
    - Får de anställda bestämma själva?

- I vilken utsträckning utbildar ni er personal i social engineering?
    - Hur går det till, i vilket format?
    - Har ni någon särskild utbildning för distansarbete?
    - Har ni någon särskild utbildning för social engineering-attacker?
    - Utbildar ni anställda i verksamhetens policys?
        - Hur ofta uppdateras utbildningens innehåll?
    - Sker det kontinuerligt?
- Hur säkerställer ni att era säkerhetspolicys följs av anställda?
    - Arbetar ni särskilt med att säkerställa att de följs av distansarbetande anställda?

7.3 Transkribering

7.3.1 Intervju 1

Intervjuns längd
33 minuter, 20 sekunder

Datum och tid
27/4/22, 10:00

Förkortningar
AO = Albin Olsson
TB = Tarek Bermalm
R1 = Respondent 1

1. AO
Inspelning här då?

2. TB
Perfekt. Det var alla formaliteter också, så nu kan vi, nu är vi redo att köra igång i det då.

3. R1
Yes

4. TB
5. Albin, vill du börja där kanske?

6. AO
Jaa, men då börjar jag med att bara kan göra. Om du vill beskriva lite kortfattat vad vad din verksamhet gör.

7. R1
Ja ni känner kanske till [***] som som fenomen. Jag menar vi, en [***] och en [***] under [***] så att vi det gör oss lite speciella. Vi lyder ju inte under [***] utan vi är ju fri fristående så att säga då.

8. R1
Men i stort sett så vad vi gör det är att vi [***] och vi ska sörja för att vi har ett betalningsväsende i Sverige.

9. R1
Som fungerar och och.

10. R1
Effektivt och sådär och jag [***] så är det ju både internetbankbetalningar så att säga elektroniskt.

11. R1
Men sen, så så ger vi ut [***] också så att det är. Ja, det är vad vi gör. Kort och gott helt enkelt

12. AO
Ja. Men vad vad är din nuvarande roll på [***]?

13. R1
Ja alltså populärt kallas vi för CISO. Men nu har vi ju inga engelska titlar här, men jag är informationssäkerhetsansvarig så heter det. Men men alla interna säger CISO och jag säger det också så att det jag svarar för informationssäkerheten helt enkelt så är det. Och jag sitter ju då i en roll som är en del i en säkerhetsavdelning kan man säga där. Jag har en säkerhetschef som är det jag sitter direkt under så att säga så att då informationssäkerhet är en del som har med fysisk säkerhet och så har vi personsäkerhet kan man säga det är de delarna.

14. AO
Super, men om man blickar tillbaka lite. Vad har du för erfarenheter och eller bakgrund var va du innan detta?

15. R1
Ja, men jag har varit till att börja med har jag varit i finansbranschen väldigt länge sedan 96 ungefär så att jag har varit inom bank och finans med mycket inom affärsbanker då. Jag började som tekniker och har egentligen jobbat halva min karriär med teknik så att säga handfast och sen så andra halvan har jobbat med analys infosäk, IT-revision och den typen av så att säga arbeten helt enkelt. Och så sitter nu som informationsansvarig sedan 2 månader tillbaka bara så det är ganska färskt i den här rollen.

16. AO
Spännande [xxx] vad har du pluggat någonting eller har?

17. R1
Ja alltså, jag är officer i grunden och sen så har jag pluggat. Jag har ingen universitetsexamen. Jag har läst en del en hel del enstaka kurser då. Så jag har väl samlat ihop en halv examen kanske, men det är ganska blandat och det det har varit ut efter vad jag behövt så som revisor har jag pluggat en del juridik och en del filosofi. Etik och den typen av ämnen då så.

18. TB
Ja vi undrar också lite där kring distansarbetet, hur många dagar i veckan arbetar ni i snitt hemifrån?

19. R1

Vi har satt upp det så här efter covid som som många andra så har vi ju skaffat distans arbetsavtal som man kan signa då och då brukar vi säga att man ska vara på jobbet 3 dagar och sen så får man jobba hemma 2 dagar och få styra det där lite grann själv. Sen har vi ganska mycket som är säkerhetsskyddsklassat här på på banken och då då får man ju inte jobba hemma med det alls så att det här är beroende på informationsklassificering. Vad som går att göra helt enkelt så att vissa människor har tjänster, då måste jobba här helt och hållet och det är det är tjänstens natur om man säger så då. Men ja, vi har distansavtal för de som kan jobba hemma och då är det 2 dagar hemma och 3 på jobbet.

20. TB
Okej, är det där distansavtalet för dem som för dem som är aktuellt för att de som vill.

21. R1
Ja, yes.

22. TB
Okej.

23. TB
Ja så undrar vi lite kring utbildning i vilken utsträckning utbildar ni er personal i social engineering då?

24. R1
Ja ja alltså, all personal får ju en utbildning och den har tidigare varit fysisk, nu har vi kört den alltså över teams sedan covid kan man säga då. Så introutbildningen är ju en byggsten i det här. Sen har vi haft sådan här nano utbildningar. Alltså en extern firma som sätter ihop nanoutbildningspaket på 5 till 10 minuter lektioner som vi har kört under en tid. Den har vi pausat just nu, för vi har lite bekymmer med leverantören där, men vi har testat konceptet och vi är ganska nöjda ändå med att det funkar bra. Sen har vi ju särskilda behov så att säga så kör vi ju utbildningspaket på teams exempelvis. Nu har vi haft under under Ukrainakrisen så så har vi. Mera målinriktade utbildningar. Att nu pågår det [xxx] kampanjer. Nu pågår det så att säga ditten och datten då. Så att så tillvidare utbildar vi dem också. Vi har ju ett intranät där vi går ut med nyheter också. Vi går ut med artiklar och kortare, kortare saker då och och där kan vi mycket väl peka på det gjorde vi för ett par veckor sedan externa utbildningar som är [***]. Till exempel källkritisk utbildning och så så att vi nyttjar även sådana resurser då.

25. TB
innehållet på de utbildningarna är det. Det är informationssäkerhet och social engineering och de aspekterna eller.

26. R1
de ja där som jag svarar för i alla fall så finns det andra avdelningar som har andra utbildningar. Men absolut jo, så är det. Det är infosäk aht yes.
information security

infosec

27. TB
Ah just det. Och sen kring distansarbetet där och har ni någon typ av utbildning som är särskilt lämpad för just distansarbetet?

28. R1
Ja, det har vi haft och det, den ska inte säga i återkommande utan det var en one off när vi började med distansavtalet och det får vi se hur vi gör framöver, men vi hade en one off utbildning där vi tittade på så att säga eller det var ju utbildade i vad vad man får göra och inte göra hemifrån och vilka risker det finns och så vidare då. Dels hade vi lite ny teknik på plats också som som möjliggör distansarbete också så att det det ingick också i den utbildningen.

29. TB
Och mer mer specifikt för social engineering att [xxx]. Har ni någon typ av utbildnings om som täcker det?

30. R1
Nej alltså. Det ingår ju i de de andra utbildningarna kan man säga, men hur alltså hur påverkan kan ske och vad vad som rör sig där ute om man säger så .. Det ja, det ingår väl inga egna utbildningar där det inte nix

31. TB
Ne förstår och kring policys utbildar ni anställda i verksamhetens policys.

32. R1
Ja, det gör vi och det ligger också i det ligger både i anställningsförfarandet att man skriver på dem, men sen så utbildar vi dem i introutbildningen också.

33. TB
Just det.

34. TB
Hur ofta uppdateras utbildningens innehåll där?

35. R1
Det sker alltid små uppdateringar inför varje gång vi håller den. Det gör det. Sen bygger vi inte om utbildningarna särskilt ofta skulle jag säga utan det det handlar ofta om att anpassa till aktuell bild. ibland så har man sådana här exempel i utbildningarna som kanske börjar kännas lite utdaterad så att då fyller man på med nya och ibland kan en regel vara uppdaterad och då får man anpassa utbildningen.

36. TB
Jag förstår.

37. AO
Ja, men nu får ni dom anställda och hålla sig uppdaterade då med de nya där uppdateras hur. Hur går det till?

38. R1
Ja alltså introutbildning satsar vi ganska mycket på, men det är den fråga som du är på nu, den är lite den kanske inte är... Lite självkritisk här. Nej, men den kan nog förbättras. Vi gör mycket, tycker vi med artiklar och vi sprider på intranät och så där, men att vi har ingen regelbunden uppföljningsutbildning, det har vi inte.

39. AO
Nej okej, men har ni något sätt får säkerställa att säkert att de här policys följs av anställda.

40. R1
Ja alltså vi. Vi mäter vår informationssäkerhet. Jag har ett LIS på plats, ledningssystem för informationssäkerhet så att vi vi gör ju viss mätning, det gör vi och vi följer ju upp på på vissa nyckeltal där. Sen kan vi inte säkerställa att varje enskild anställd aldrig bryter regler eller policy såklart. Men men vi har mätmetoder, det har vi för att säga ungefär vad vi ligger.

41. TB
Hur funkar det med justeringen där om det visar sig att nyckeltal ligger lågt. [xxx] vidareutbildning eller vad man kan det röra sig om.

42. R1
Det är det absolut och vi vi har ju. Vi har ju nyckeltal som alltså. Vi har ju lite tröskelvärden som vi ska hålla och det gäller ju alla områden, men då på på informationssäkerhet på de anställda och andra typer av säkerhetsskydd då så att tanken är att det här ska mätas kontinuerligt då att när det här det här har jag på mig att att lägga fram för direktionen då. Med viss periodicitet resultaten här och är resultat av att den försvagade. Ja, men då då får vi utbilda helt enkelt.

43. TB
Jag fattar och även där omkring distansarbetet. Har ni något specifikt arbetssätt för att se till att det följs av distansarbetande anställda?

44. R1
Ja, jag ska väl säga såhär att distansarbete ändå är ganska nytt för oss så att vi har nog inte riktigt kommit igång med så att säga, vi har inte fått någon output från det och delvis på grund av att vi är ganska vi är hyggligt hårda med distansarbete. Det finns ganska många områden här på banken som inte kan ske på distans, alltså det det är tekniskt hindrat att vi hindrar från visst arbete utanför lokalerna så att säga så där känner vi oss ganska trygga med att man inte kan göra saker hur som helst. Men sen har vi ändå lite mjukare, mjukare styrning också på vissa typer av information klasser så man får ta med sig utanför och inte då och vissa saker

kan man ju ta med sig ut fast det är under vissa villkor då och då ligger det mera på den anställda och där har vi inte det har vi inget. Vi har inte fått den erfarenheten om man säger så.

45. TB
Ja just det.

46. R1
Så vi kan på påvisa någonting.

47. TB
Det tidigt skede med distansarbetet här.

48. TB
Fast, det här är säkerhetskultur hur har det blivit det där med säkerhetskultur. I samband med distansarbete är det utmanande att etablera en bra säkerhetskultur?

49. R1
Ja, det skulle jag nog säga att det är dels så beror ju den lite grann på personalomsättningen. Hur många som kommer in från andra platser och jag menar hur mycket man kan behålla innanför väggarna. Jag kan ju säga att det här med distansarbete har ju föregåtts av ett projekt också. Hållbara arbetsformer har vi valt att kalla det då så att där har ju sådana saker kommit in hur man blir kulturbärare i en sådan här organisation. Och den är inte bara informationssäkerhet centrisk utan den tar vi fasta på hur. Hur är man en bra [***] och hur där man. Ja, det är ju många aspekter på och hur? Hur påverkas det av att folk inte de facto här? Här och det ligger både i det här med med distansarbete, men också i hela covid efter covid för då var ju då distansarbetare vi 100 % i stort sett många av oss så att det blev en kulturfrågan det hamnade på agendan.Om man säger så så vi kände ju där och det det hade vi inga särskilt bra mätmetoder kanske men vi kände ju det att vissa människor hamnade ju längre ut från [***] kulturen eller eller [***] och kultur och då är ju informationssäkerhet en av dem naturligtvis då. Så tycker jag ändå att vi satsar ganska mycket på informationssäkerhet, för det är det är ganska viktigt för oss det kan vara att man kanske inte är. Man kanske inte har förstått [***] , men det kanske inte är lika allvarligt som man att man inte förstår hur man använder vår information så att medvetenheten, skulle jag säga är hög

50. TB
Ja okej.

51. AO
Lite off topic Vad har ni för… Har ni någon som arbetar mycket? Alltså nästan primärt med kultur, hos [***]. Det gör ju. Jag är mer erfarenhet av privata sektorn kanske och där är det känns det lite mer förekommande. Men nu är det på en myndighet.

52. R1

Nej alltså. Vi är ganska liten myndigheten då vi är ungefär hundrafemtio pers att det finns ju. Jag ska inte säga att det finns någon som jobbar enbart med kultur, men vi har haft i de projekten som vi driver så är det här en fråga och då då finns det med i projekt. Sen, men vi har ingen kulturbärande roll. Ja, man kan ju tänka sig att hon skulle ligga hos HR. Att HR på något sätt etablera en kulturbärare funktion eller så, men det har vi inte. Inte en heltidstjänst i alla fall. Vi har väl några människor som är intresserad av det så kan man nog säga. Men frågan lever i alla fall skulle jag säga sen sen hur mycket krut vi lägger på den, det kan det kan vara. Det kan diskuteras så ja.

53. AO
Men okej, men då går vi vidare lite. Hur arbetar ni med att säkerställa compliance av policys med kulturen? Nu sa du att det var lite varierande.

54. R1
Ja, jag vet inte hur. Hur bekant är ni med three lines of defence modellen?

55. TB
Personligen är jag inte särskilt bekant med den.

56. AO
Nej nej, jag har inte heller.

57. R1
Alltså så som finans och alltså alla affärsbanker och även även vi då som förvisso är [***] då så jobbar ju med three lines of defence där man har på något sätt. Alla kontroller och allt risk ägande ligger i första linjen och andra linjen är ju risk och compliance och tredje internrevision. Det är ju så man bygger kontrollapparat om man säger så och den ska ju vara det ska ju. Det ska ju finnas ett djup tänk i det här, ett djupförvar om man säger så allt ska ju ske första linjen. Men sen har man risk och compliance och sen har man internrevision då och just det med att säkerställa compliance. Det ligger på inte att säkerställa kanske, men att övervaka compliance det ligger på en roll. Alltså en compliance roll i andra linjen. Och andra linjen är risk och compliance avdelningen här på banken så att det finns där finns det funktioner som ska i alla fall monitorera compliance, monitorera och mäta compliance. Så det är ganska uttalad roll i finansbranschen och en hyggligt etablerad roll hos affärsbankerna som är lagstadgade. Det måste ske helt enkelt och det finns många paralleller med med [***] här också då.

58. AO
Ja hur hur arbetar ni med att säkerställa riskmedvetenhet hos medarbetare.

59. R1
Är det på sätt och vis samma svar som som den förra att vi har alltså andra linjen där den ska monitorera både compliance men också risker och då pratar vi både finansiell risk och vi pratar operativa risker och vi pratar, jag egentligen alla risker då som som finns i

verksamheten så att den det är det ligger i den här tre linje modellen så att även även riskmedvetenhet hos medarbetarna ska monitoreras av den andra linjen. Går man över till att titta på tredje linjen så är det internrevisionen och de jobbar ju helt och hållet. Friställd från verksamheten så de har yttrar sig alltså andra linjer mäter och till viss del stödjer tredje linjen. De mäter ju bara och rapportera till absolut högsta ledningen. Helt oberoende av så att det finns egentligen 2 kan man säga kontrollfunktioner som ska ta om hand de här sakerna så att det det läggs ganska mycket på kontroll struktur i finansiell sektor.

60. AO
Spännande alltså. Ja, men i er verksamhet hos [xxx] då. Vilken roll har ledningen i det här?

61. R1
Det ledningen är skulle jag säga väldigt medvetna om allt det här, både medvetna om om risker och medveten om om alltså om hur hur viktigt det är så att säga och jag skulle säga också att de lägger de medel på det här som en ledning kan göra. Jag menar de styr egentligen bara med vilka medel vi får då, men de lägger de medel som vi behöver skulle jag säga så att det finns en en god medvetenhet om om det här. Jag menar vi, vi jobbar ju väldigt mycket med med digitala digitala resurser och digitala värden här, så att det det är viktigt, helt enkelt. Det passerar 700 miljarder genom [***] vårt system här varje dygn så att det ja, det är viktigt.

63. TB
Stora siffror.

64. R1
Ja, ja, herregud.

65. TB
Ja ja, men vidare så undrar du lite man kan ju kategoriseras så här social engineering-attacker på lite olika sätt men vi har ju pratat om dig kring fysiska sociotekniska, tekniska och sociala och så där, så vi undrade, hur skyddar ni er mot i första hand då fysiska attacker till exempel? Hur funkar det där?

66. R1
Ja alltså [***] och det kommer vi in på distans biten. Den är ju lite så det är lite intressant faktiskt. [***], jag vet inte om ni har varit i närheten av byggnader och så där vi är skyddsobjekt och det är. Det är ganska alltså det är väldigt hård fysisk säkerhet här bara att komma in det som att komma in på en flygplats där metalldetektorer och allting när man kommer som besökare så att alltså våra lokaler är ganska ganska rigida men så har vi distansarbete och det där ligger ju utanför vår kontroll så att det där är lite intressant för det är det är lite grann, en ny verklighet. Vi kan ju inte veta om någon shoulder surfar på vare sig hemma eller om man sitter på pendeln med telefonen. Där vi har det är ju ändå att vi skiljer ju på vad man får göra hemma och inte så att säga så att det är klart de kan läsa ett mejl som som är känsligt på på pendeln, men det det hänger ju helt och hållet på hur medarbetarna agerar

och det kan vi inte göra så mycket åt mer än att utbilda folk. Sen våra lokaler kan vi styra väldigt mycket, vilka skydd vi ska ha här. Jag menar tjocka gardiner och allt det där så att ja.

67. TB
Ja, men det är ju faktiskt riktigt spännande där. Har ni har ni haft någon möjlighet och kanske utöver utbildning och följa upp på det eller så är det funka eller se ifall det sker intrång där och så där typ shoulder surfing och liknande grejer.

68. R1
Alltså, den är svår att komma åt skulle jag säga, och jag har inte riktigt knäckt den nöten heller utan det är knepigt för det är en risk. Det är det absolut. Jag menar, det enda vi kan göra är egentligen att utbilda och följa upp är svårt. Jag menar det, det kan läcka den vägen. Jag vill tro att människor som sysslar med riktigt känslig information här, alltså, de agerar så som man bör agera. Jag upplever att människor är ganska mogna, men risken är absolut inte. Ja, den är nog inte ens minimal. Det kan hända, så är det.

AO
Nej, men det är inte så här när ni är på distans. Jag har några krav på alltså ska man vara hemma eller kan det vara så att en anställd sitter på ett café någonstans?

69. R1
Nej det, det säger vi att i vårt vårt distansavtal då ska man vara hemma alltså. Det är till och med så att vi har sagt nu i senaste versionen att man ska vara på på alltså där man är skriven helt enkelt så att det ska. Det ska inte vara var som helst. Det har varit lite snack om lantställen och såna här saker utomlands, definitivt inte och sånt kan vi som kan vi hindra också så att det är lite lättare då. Men vi har ju ändå folk och det rör ju till det lite grann. Vi har ju folk som reser i tjänsten och då är det ju tjänsteresa och då kan man ju jobba var som helst ifrån. Men det är fortfarande så att vi har tekniska hinder. Man kan inte göra vad som helst utanför landets gränser och sådana saker så att visst. Men, men samma sak där man kan ju shoulder surfa på ett flygplan till exempel, så att det är också det landar tillbaka i en omdömesfråga igen då och medveten medvetenhet så att.

70. AO
Ja nu går jag lite off topic här. Du får koppla in det finns här filter man kan sätta på mobiler som man bara kan se skärmen från en viss vinkel.

71. R1
Ja, det har vi absolut. Att den typen av utrustning det det har vi ju så att yes. sen kan man ta bort dom också.

72. AO
Ja ja okej. Är det någonting ni tänker på?

73. R1

Det gör medarbetarna själva också så att men jo, men vi har en del tekniska grejer. Det har vi absolut.

74. AO
Ja okej ja. Men så lite mer åt det sociotekniska här typ som alltså phishing och spear phishing och sådana attacker.

75. R1
Japp ja alltså. Vi har ju naturligtvis en del. Även där har vi naturligtvis teknik i form av filter lösningar då alltså det sker ganska mycket behöver inte gå in på exakt, men det sker inte bara på en punkt heller utan vi vi skyddar oss tekniskt i många lager och så där där det gör vi ju. För att försöka få in så lite som möjligt att träffa användarna, men sen är det ju ändå så att man. Det som ändå träffar användarna kan man utgå ifrån det ganska sofistikerat då om vi kommer förbi så att säga våra våra tekniska skyddsmekanismer. Men även där skulle jag säga användarna ganska medvetna där. Dock är vi inte immuna naturligtvis då. Mot vad som vad som kan hända så att säga då. Sen vad som eventuellt kan bli någonting av det här. Vad kan man få ut pengar ifrån oss och så vidare. Det är ju någonting som vi alltid funderar på hur vi alltså vilka värden kan man komma över om det är värde man vill komma åt, man kan ju vara utefter förstörande verksamhet också, naturligtvis då.

76. AO
Nej, men man tänker väl mycket på så här ransomware som var lite efter coop incidenten

77. R1
Ja precis, absolut, och det har ju varit högt på agendan här också. Just de riskerna då och det skulle man kunna säga ganska mycket. Men det kan jag inte göra eller vilka skydd, vilka skydd vi har. Men vi har ju absolut tagit vi har ju tagit fasta på det som har hänt på både coop och andra liknande händelser också som vi formar ju ganska mycket tekniska skydd runt det här. Men om man om det nu, människan som ni är ute efter med det här, så så ja. Det är ju inga. Det sker inga egentligen phishing utbildningar utan vi är. Vi informerar om det här på på den basis vi tycker att vi behöver. Vi har en del övningar på ämnet också. Vi kanske inte ska säga så mycket mer om det heller. Men men vi har en del övningar på på phishing temat också.

78. TB
Jag undrar också lite kring? Ja, men det finns ju mer tekniska attacker som när man OSINT och så open source Intelligence när man letar på allmänt tillgänglig information och sådär hur slut på den biten har ni gjort något för att skydda mot något sådant?

79. R1
Ja nej, men absolut så alltså. Vi lägger som sagt ganska mycket på på vårt försvar. Jag menar vi har ju. Om man backar till 2019 fram till nu så har vi väl ungefär personellt. På [***] har vi väl ökat på personalen på säkerhetsområdet med gånger 3 ungefär. Och sen så har vi lagt på ganska mycket på tekniska sidan också med med att vi har handlat upp en extern sock till

exempel och i socken ligger en del intelligens tjänster också. Så att vi köper intelligence, det gör vi. Så har vi ganska mycket forum och det är samma sak där. Jag kan inte säga så mycket om det, men vi har ju forum där vi känner folk mellan [***] så att säga då både formella och sen lite mindre formella också kontakter med med andra [***] och även till viss del affärsbankerna då affärsbankerna ska jag säga de är extremt starka på de här områdena där de har resurser för det här verkligen så att det vi samarbetar ju på de här områdena, ja, det gör vi.

80. AO
Men om jag går in på lite mer sociala, om med alltså övertalning, telefonsamtal, till era anställda har det någonting om validering skydd eller ja, autentisering.

81. R1
Alltså validerings skydd och sånt. Då har vi på mejlen som det ser ut idag egentligen inte via telefonsamtal. Inga tekniska skydd nej.

82. AO
Ja okej, ja men då går vi vidare från den. vi vilka skulle säga de största utmaningarna med säkerhetsarbete, mot social engineering?

83. R1
Det ja alltså. Vi har ju en del tredje part, alltså vi använder tredje parter. Vi outsourcar vissa saker och det är klart, de har ju också personal. Och som sagt vi är ju ändå under ganska stark lagstiftning så vi säkerhetsprövar ju all personal som jobbar med våra lösningar och det är ju ett skydd för det. Den säkerhetsprövning är ju ganska rigid, genomlyssning av personer. Men vi har ändå folk hos tredje part som jobbar med [***] information och det är klart de känner ju de har mindre, samhörighet med [***]. Det har de, även om vi gör vårt bästa för att berätta att de faktiskt jobbar åt oss. Så det skulle jag nog säga en stor risk.

84. TB
Alright kring tillgängligheten på data för medarbetare hur, hur arbetar med att försöka åstadkomma obehindrad tillgänglighet?

85. R1
Ja, det är ju främst tekniskt och det gör vi på många olika sätt med hur vi bygger våra system miljöer för. Beroende på vad det är för alltså. Vi har ju ganska många system miljöer, men vad det är för systemmiljöer så så bygger vi dem ju efter vad som behövs tillgänglighets mässigt tar man [***] systemet som är vårt huvudsakliga system så är det byggt för för att vara tillgängligt för det behöver vara helt enkelt och då är det ju. Då bygger vi det med en arkitektur som behövs givet att de behöver finnas olika datahallar och sådana hör saker då och och även även hur vi opererar datat så så tänker vi ju på vart den personalen ska sitta. Så det finns ju flera platser för den också så att det är både den tekniska. Teknisk location, men också personnel location. Var kan människor sitta om vi inte kommer in en dag på [***] i våra lokaler här? Så att det är fler dimensioner.

87. TB
Ja just det. Och så vidare. Det undrar vi, har ni upplevt att data förstörts, blivit korrupt och rekryterar alltså i samband med intrång?

88. R1
Ja, den kan inte kommentera tyvärr.

89. TB
Jag tänkte efter jag läste den här. Ja ja. Vet inte vad vi tänkte när vi skrev den där. Vad mer har vi här ska se vad vi ville kanske runda av med en sista fråga här där. Hur ser det generella säkerhetsläget ut idag också verksamheten i samband med social engineering.

91. R1
Ja, men det kan man ju ta i lite svepande termer så där att jag menar vi har ju, vi har ju krig i Ukraina och det är ju stökigt i Europa så är det och alltså social engineering, det vill säga att någon vill påverka oss att göra saker. Vi tänker väldigt mycket på nato frågan nu. Vad händer om Sverige går med i Nato eller indikerar att vi går med i Nato eller Finland går med i Nato eller vi gör det båda 2? Så kommer det ju hända saker och vi vet inte vad som kommer hända kommer kommer vi att bli attackerade med med alltså någon form av riktade cyberattacker? I vilken form kommer det att se ut? I så fall kommer det vara. Direkt mot vår systemmiljö eller kommer det vara via människor? Och då kanske social engineering kommer vara aktuellt. Så att det det finns definitivt på kartan. Det är inte så svårtippad den risken, men det är väldigt många som som tänker på den idag och det är klart vi är [***] så att vi vore ju en.

92. TB
Ja nej ja.

93. R1
Vi är en måltavla. så så är det, vill man ställa till i samhället då? Då är ju vi en spelare bland många andra. Jag menar kraftbolag och sånt har ju samma tankar såklart. Så vi är inte de enda, men ja, det är en risk.

94. TB
Så undrar vi det också här kring kring framtiden? Lite grann i samband med skyddet mot social engineering . Hur arbetar ni kontinuerligt för att bli bättre på att skydda er.

95. R1
Alltså, det är ju väldigt mycket örat mot rälsen. Fråga det här att se vad som händer ute ute i samhället så att jag har ingen sådan treårsplan. Det har jag inte utan det handlar väldigt mycket om att vara med. Alltså vi, jag både jag och vi är ju med i många olika forum för att se vad som händer på marknaden och det är nästan enda frågan att det enda sättet att hantera den frågan skulle jag säga. Pratar man med folk och man börjar se hämta se att det här sker tendenser till det ena och det andra så måste man på något sätt reagera på det så att det därav det är ganska korta perspektivet ändå.

96. TB
En lite av topic fråga här egentligen. Jag bara nyfiken på. Det gäller kring att varje den säkerhets världen är det att ha ett öra mot rälsen är något som är på arbetstid och sa det får i ditt personliga liv som man investerar lite under för att hålla sig aktiv så eller?

97. R1
Ja alltså.

98. TB
Om det går att svara på.

99. R1
Det blir ett fritidsintresse också.

100. R1
Ja jo, men det blir det här. Ja och det blir ju inget viktigt och det är därför jag tog jobbet här också. Jag har jobbat på [***] längre än de här 2 månaderna har suttit här förvisso, men då var jag IT-revisor, men det är ju utmaningen i den här rollen. Att man, det är inte riktigt en 8 till 5 tjänst heller. Man måste vara jag menar måste köra mina Google alert dygnet runt för att se vad som händer när det händer så att säga så att det är intressant. Det är jätteintressant det.

101. TB
Ja just det.

102. TB
Sedan då?

103. R1
Så får man se hur länge man pallar.

104. TB
Precis. Det blir det riktigt, riktigt intressant och spännande arbete men många timmar.

105. R1
Ja, det är lite lite jobbigt med sånt arbete när när ingenting händer oss så har jag gjort mitt jobb, men jag kan ju inte visa det?

106. TB
Ja, ja precis, det är ju samma bit i generellt mer. Ja.

107. R1
Lite motsägelsefullt? Ja, men precis det ska bara funka. Ingenting ska hända så att ja.

108. AO
Ja exakt. Vi vi har ju snackat lite om det här, att säkerhet känns som ett väldigt otacksamt jobb. Att att när det går bra så då du är det märks inte. Men när det skiter sig.

109. R1
Då sitter jag där, men. Då får jag väl se vad jag gör, men ja, nej, jag är inte ensam heller i min roll. I min roll är jag ensam. Jag menar, det är en organisation som gör jobbet, så är det. Vi är ett gäng på säkerhetssidan och jag menar vi visst, ja. Man är inte helt ensam heller, utan när det brallar is och då formas de grupper jag menar. Vi har haft krisledningen under covid och vi har krisledningen under nu ukrainakrisen så att det. Vi jobbar ju team definitivt, så är det. Det behövs många olika kompetenser där.

110. TB
ja ja, men avslutningsvis så är det bara ifall det ifall du vill lägga till om tänkte som inte vi nämnt och sådär.

111. R1
Nej bara nyfiken var vad resulterar det i? Vad, när kommer produkten?

112. TB
Men vi har ju inlämning och så där är 18 till maj och sen så är det väl några veckor till efter det. Så vad tror du Albin kan den vara ute redan i juni? Kanske lite optimistiskt Ja vi ska ja, men jag tror vi publicerar någon gång i början av juni på laddar upp den, så då kan vi ju bara skicka över den till dig.

113. R1
Ja men toppen ja, det vore kul att se vad det är alltid kul när man är delaktig i en liten del av något sånt här. Se vad vad produkten blir ju så att.

114. AO
Ja ja.

115. TB
Verkligen spännande nej, ja, givande ja. Men verkligen riktigt givande och super intressant.

116. AO
Ja absolut.

117. R1
Tack, ja då ser jag fram emot era era jobbansökningar så småningom.

118. TB
Ja absolut.

119. AO
Ja, men tack så mycket.

120. R1
Okej, ja tack så mycket.

7.3.2 Intervju 2

Intervjuns längd
26 minuter, 13 sekunder

Datum och tid
27/4/22, 13:00

Förkortningar
AO = Albin Olsson
TB = Tarek Bermalm
R2 = Respondent 2

1. AO
Så där så.

2. TB
Där vi kommer ta bort inspelningen sedan efter ungefär 30 dagar också.

3. R2
Ja, jag godkänt inspelning, så har du det på.

4. AO
Ja ja exakt.

5. TB
ja exakt. Och ja, deltagande till frivilligt så det kan avsluta ditt deltagande när du vill.

6. TB
Och om det är någon fråga som inte kan svaras på eller så där då är det bara att säga till så går vi vidare till nästa direkt.

7. TB
Någon mer har vi här?

8. AO
Ja, du kan få tillgång till transkriberingen. om det är någonting som inte stämmer eller du tycker vi ska ta bort, så kan vi fixa det. ja, men nu drar vi igång med själva intervjun då? lite lite kortfattat. Vad vad gör din verksamhet?

9. R2
Jag såg frågan verksamhet nu vill du ha hela företaget inte vad min avdelning jobbar med väl.

10. TB

Var bra att höra både och.

11. R2
Vi är ett globalt retailföretag. Det är ungefär så långt jag kunde gå utan att [xxx]

12. TB
Ja absolut, bra svar. [xxx]

13. R2
Jag arbetar på den digitala verksamheten. I en avdelning som heter cyber security and privacy. Vår kärnfråga är att skydda oss mot både alltså cyber threats och liknande, men även se till att vi har en fungerande privacy som överensstämmer med våra Etiska commitments till kunder och coworkers.

14. AO
Yes, vad, hur skulle du beskriva din roll?

15. R2
På papper säger min roll senior security engineer. Jag arbetar just idag främst med våra audits, att det är till att vi är compliant med till exempel kreditkortsdata regulations. Sedan jobbar jag även med datainsamling av all säkerhetsdata, så just nu så sitter jag och bygger upp tillsammans med mitt team en en plattform som hanterar då säkerhetsdata.

16. AO
Vad, vad har du för erfarenheter och bakgrund med studier och tidigare?

17. R2
Jag är informatiker, jag gick också i Lund en kandidatuppsats för i informatik. Jag har sedan gått vidare. Jag har ju läst alltså fortsätta lite på universitetet, men främst gick jag ut och börja arbeta direkt. Jag arbetat i roller såsom. Produktägare, IT-arkitekt och senare då security engineer. Ja nu senast senior security engineer.

18. AO
Toppen, men då går vi in lite mer på hur ni arbetar då så vi bara börjar med att ställa. Hur många dagar arbetar ni hemifrån med distansarbete?

19. R2
Val nu får man skilja lite från retail verksamheten vi har versus den digitala, det digitala enheten och vi som kan jobba hemifrån. Har idag ett fritt val beroende på vad ens manager säger. Så det helt upp till de olika enheterna. Vissa jobbar 5 dagar remote. Vissa jobbar alla dagar inne.

20. AO
Alright har ni, finns det några speciella regler för för det här, eller är det bara helt fritt.

21. R2
Vad sa du om det finns några speciella regler?

22. AO
Ja för distansarbete.

23. R2
Ja, det finns det får nog specificera lite.

24. AO
Ja vad, hur ska man formulera sig?

25. TB
Kanske. Alltså är det valfritt bara enligt manager där om man ska få jobba hemifrån eller inte eller eller finns det någon annan typ av reglering för vem som faktiskt får?

26. R2
Det finns reglering på vem som får beroende på vilken yrkesroll man innehar och sedan är det också upp till ens manager att bestämma vem som kan göra det. just nu har vi en av de friare om man ser från alla diskussionerna vad gällande hybrid arbete har blivit väldigt uppmärksammad och den verksamhet jag jobbar på där har vi det på det sättet att den digitala enheten får jobba väldigt fritt, så vi har det egentligen praktiskt taget att vi jobbar 5 dagar remote om vi känner att det passar oss bäst. Och vi är mest produktiva när vi gör det.

27. TB
Okej och så vidare. Lite kring utbildning här då när vi undrar vilken utsträckning utbildar ni er personal i social engineering?

28. R2
Vi har en awareness Security awareness training som innefattar social engineering sedan det är en del. Den är årligen och sedan har vi den andra delen som är att vi har även. Det är inte riktigt honey pot på att, men vi har satt ut det. Förlåt jag måste bara tänka om jag får svara eller inte. Jo, det borde jag. Vi har haft awareness veckor så vi har både privacy awareness vecka och sen har vi haft en [***]-event. Vi kan nämna vad den heter, men säg en säkerhetsvecka de 2 delarna har vi. Där vi har säkerhets events. Vi pratar om sociala engineering och liknande. Där har vi även lagt ut tester. Hur bra vi performar som vi då kan mäta i förhållande till tidigare gånger. Ett exempel på ett test man kan göra? Jag säger inte om det är det vi har gjort eller om det är ett annat. Men ett test kan till exempel vara att vi skickar ett falskt phishing mejl och så ser vi hur många klickade, hur många, hur många la in credentials och vidare?

29. TB

Är de här de här testerna som du beskriver i utbildningen och så där är det hos er säkerhetsverksamhet där som det var del av eller [***] i stort. Tar såklart bort verksamhetens namn i transkriberingen. Ja ja [***] i stort. Men vi höll i den tekniska implementationen av experimentet.

30. TB
Just det just det.

31. R2
Med limited fuse så vi hade även personer på säkerhetsavdelningen som råkade gå i fällan.

32. TB
Har du någon speciell utbildning för just distansarbetande medarbetare?

33. R2
Inte från säkerhet direkt, men vi har en för vad som gäller om man jobbar hemifrån. Den inkluderar inte bara sociala engineering, för den är den är bara en liten sån här. Det ingår i annat när du har en utbildning i att jobba med någon hemifrån så finns det vissa regler man ska ha och uppfylla även sådana saker som att man ska även kunna sitta bra och ha en bra arbetsmiljö hemifrån.

34. TB
Just det. Så den är utan inte specifikt säkerhet som riktad så utan den lite mer heltäckande.

35. R2
Den är heltäckande istället.

36. TB
Ja ska vi se. Ja, du gick väl in lite på det. Jag undrade också om hur det ser ut, men för social engineering-attacker men har jag uppfattat det korrekt om det är så att det är är del av den heltäckande utbildningen. Det inte finns en specifik jo, vi hade en fråga ifall någon särskild utbildning för social engineering-attacker men.

37. R2
den ingår ju i säkerhetsutbildningar, inte i den allmänna som är för hemarbete, men för säkerhetsarbete eller för säkerhet awareness.

38. TB
Just det ja, det kanske också du har egentligen svara på här, men vi undrade också nästa fråga ifall ni utbildar anställda i verksamhetens policys. Ja, hur ser det ut där, policys, är det del av den den heltäckande allmänna?

39. R2

Här beror det lite på vart man är anställd? Helt klart, men om jag skulle prata ut ur mitt perspektiv. från en digital enhet så, där krävs det att man ska vara uppdaterad om de policys och principals som gäller på företaget. Men det är ett eget ansvar. Det är inte så att vi har en proaktiv träning i policys.

40. TB
Så då vi undrar också ifall det sker kontinuerligt, men om det är eget ansvar, hur ser ut som det är den biten man ska försöka hålla sig uppdaterad själv?

41. R2
Ja som sagt, försök mäta den.

42. TB
Ja, verkligen. Ja, Albin du kanske vill gå in.

43. R2
[xxx] om du vill ha ett officiellt svar så är det nej, vi mäter inte det.

44. TB
Ja, jag gissade det något i den stilen.

45. AO
Okej, hur säkerställer ni att de här policys följs? Har ni något mätverktyg eller? Åt det hållet?

46. R2
Det beror ju på. Alltså det kan låta enkelt att säga hur man vet att policyn följs. För det första så brukar företag generellt ha rätt så många policys och de är på olika nivåer och sen ska man inte mäta policy sig förutom om de är lästa eller inte, utan det är mer när man kommer ner på det till principle nivån och hur man implementerar dem. Det är där man får mätpunkten. Idag mäter vi inte det utan vi mäter till exempel specifika känsliga produktteam som vi har som har väldigt hög konfidentialitet eller integritetsproblem. inte problem, men de har krav på detta. De kollar vi att de har kontinuerlig uppdatering av deras läsande om policys och vet vad som är ute. Vad som finns. Men vi arbetar mot att kunna ha den här kontinuerlighet, skapa en kontinuerlig läsning av policys. På andra sätt än traditionell bara dokument.

47. AO
Ja, arbetar ni särskilt med att att de här följs av distansarbetande anställda. Är det någon skillnad?

48. R2
.. Nej, vi har inte särskilt det.

49. AO
okej, men hur arbetar ni med säkerhetskultur? I samband med distansarbete?

50. R2
Vi har ju awareness veckor så vi har satsat mycket mer på att vara en, alltså närmare mot product team och verksamheten så att vi försöker arbeta mycket närmare till dem som faktiskt utför säkerhetsarbetet. För man kan säga så här en säkerhetsavdelning gör mycket säkerhetsarbete. Men det är varje individ i verksamheten som egentligen gör det stora arbetet och då har vi sett det som att det handlar mycket mer om en mindset change än att ge fler policys eller ge fler verktyg. Så det är det vi har satsat på nu under tiden det har varit pandemin.

51. AO
Exakt, ja hur arbete mera. Ursäkta, hur arbetar ni med att säkerställa compliance av policys gällande säkerhetskulturen då?

52. R2
Nu vill jag gärna att du förtydligat frågan.

53. AO
Ja men.

54. R2
Vad menar du?

55. AO
Hur hur ser ni till att ja, arbetar ni på något särskilt sätt, med och se till att ja, de anställda faktiskt följer policys.

56. R2
Compliance brukar ju vara så att det är när du har ett krav ställt mot dig som till exempel [xxx] gdpr following. Så det är helt beroende på vart är ni undrar, men generellt så sker det en dubbel checkning av de delar av organisationen som har krav på sig som kräver en compliance check så gör vi det.

57. AO
Alrigh, okej, men då går vi vidare då, hur arbetar ni med att säkerställa riskmedvetenheten hos era anställda?

58. R2
Awareness, fortfarande, det är mycket… det är de största bitarna.

59. AO
Yes och i verksamhet. Vilken roll har har ledningen i denna aspekt?

60. R2

Förutom att vara ledning vad menar du förlåt.

61. AO
Ja det gick.

62. R2
För att stötta upp säkerhetsarbetet?

63. AO
Ja exakt.

64. R2
Där sätts det ju oftast på ett företag så brukar man ha en strategi för hur man arbetar och en av de viktigaste delarna av strategin idag, jag kan säga den delas upp i 5 och det är ju att vi ska kunna arbeta snabbare och vi ska inte bygga saker som skapar, alltså teknisk skuld och liknande. Och en av de 5 är. Att vi ska ha en säkerhet och privacy. Inbyggt i allt vi gör. Så ledningen har stöttat upp säkerhetsarbetet vi gör via strategi och policy för att trycka ut att detta inte är någonting vi tar.. We take lightly.

65. TB
Ja, vi undrar också lite kring. Det finns olika sätt att kategorisera social engineering-attacker. Vi har sett på det som fysiska sociotekniska, tekniska och sociala. Så på den aspekten. hur skyddar ni er mot fysiska attacker till exempel?

66. R2
Vi testar fler, alltså. Vi har tester som vi utför både inhouse och utan, utanför. Ja, så man kan säga så ja.

67. TB
Så typ.

68. R2
Man kan säga att det blev som punktinsatser. Vi kollar av hur det fungerar.

69. TB
Är det på punktinsatser på en kategori eller på en specifik attack eller hur ser det ut? Om det går att svara på.

70. R2
Pass vill jag säga, för där vet jag inte hur dem.

71. TB
Absolut nej, jag förstår det. Ja men kring sociotekniska attacker lite samma svar där eller?

72. R2
Ja tyvärr, det är där det börjar gå. Ja.

73. TB
Ja, men det är ingen fara. Ja, jag förstår och då kanske vi hoppar till nästa.

74. R2
Ni får börja jobba för oss innan vi kan säga.

75. TB
Ja då blir mer, kanske lättare att prata. Men vi hoppar vidare till nästa fråga här då, så i det generella säkerhetsarbetet mot social engineering, vilka utmaningar har ni där? Skulle ni säga?

76. R2
Ja stress. Är oftast har man jobbat någonting med social engineering vet man precis vid vilken tidpunkt man ska fånga en människa. De känner till de mänskliga beteendena. Man är stressad 5 i 8 för man ska iväg och så ser man ett mail och shit och klick. Ett exempel, eller det är stress, om vi säger en fysisk av att man vill in i byggnad.. och man snackar sig in. Då är det sjukt bra att göra det fem i ett när alla andra går in från lunch. Ingen plockar oftast passerkort eller liknande då. Största problemet är stress och mänskliga beteenden för vi kan träna hur mycket vi vill, men det är bara någonting vi lägger ovanpå. De här beteendena är någonting som.. Kommer automatiskt och då man kan ha hur mycket awareness som helst men för att bryta det så behöver det vara ett mindset change hos människan.

77. TB
Det är väl den svåraste aspekten, att faktiskt ändra på sig.

78. R2
Ja human, ja precis alltså. Man kan ha hur mycket säkerhet som helst, men har man, när man får in den mänskliga faktorn så är det oftast där man har störst problem, för den är svårkontrollerad.

79. TB
Ja, verkligen, verkligen. Jag tror att det är. Vi har läst mycket som säger att det är så här. Det har absolut inte tillräckligt mycket fokus på det, men det verkar kanske som att det börjar folk få upp ögonen, för det är att det faktiskt är en svag punkt som behöver adresseras.

80. R2
Ja och jag tror att det handlar också om vilken generation som växer upp. Vi haft generation som kanske inte varit så tech heavy innan i branschen. Men nu är allt fler som kommer in. De är redan medvetna om för privacy lagar eller privacy notices de skriver på, de vet redan till exempel också, Ja, men vad är det jag loggar in på? De kommer uppdateringar på iphone alltså. Visst alla läser inte allting, men på något sätt är alla de här diskussionerna som väcks

nu kontinuerligt skapar en förståelse för att, okej Jag behöver i alla fall fundera en stund till och det är den största fienden för en hacker att någon funderar en extra gång till, för det är oftast då det hindras.

81. TB
Verkligen. Det är intressant faktiskt. Det är den generella tech medvetenheten som gör att det blir mer utmanande för hackern. Och så undrade vi här. Hur ser det generella säkerhetsläget ut idag hos er verksamhet då? I samband med social engineering skulle du säga?

82. R2
Pass

83. TB
Och kring framtiden hur ser det ut i samband med skyddet mot social engineering. Hur arbetar kontinuerligt för att bli bättre på att skydda er

84. R2
Jag skulle säga det, en sak som vi som är högprioriterad. För att skapar vi inte bra kultur av säkerhetsarbete ut mot den generella massan, alltså resten av coworkers. Så kommer vi inte kunna skala det säkerhetsarbetet vi gör. Det blir allt större. Den sociala engineering som skedde för 10 år sedan funkar inte längre idag alltid. Och det blir förfinat på ett helt annat sätt, vilket kräver att vi utbildar oss. Vi har en väldigt hög högt ansvar som anställd här att faktiskt vidareutbilda oss i området så har man ett fokus på Social engineering så får man ta också ett grepp om att man håller koll på vad som händer i branschen. Men det är även titta på nya tekniker och så går vi på det sättet. Sedan har vi då även att vi arbetar strategiskt mot till exempel att i och med att cybersecurity privacy sig ligger i strategin så arbetar ju hela verksamheten mot att förhindra det.

85. TB
Ja, men då är det egentligen bara en sista fråga här, ifall det är något som du vill tillägga som inte vi har nämnt eller gått in på.

86. R2
… Nej, jag tror ni har täckt rätt bra, sen det är ju svårt att veta för mig, för jag vet inte exakt hur ni kommer framea uppsatsen och och skulle ni ha någonting ni känner shit det här behöver vi få svar på, så är det bara att höra av er så kan vi komplettera. Ibland blev det så att han tänker man man fattas någonting liknande.

87. AO
Jag ju egentligen. Jag har bara en sak som jag glömde fråga om bra, men jag tänkte när ni arbetar på distans har den har några krav på er var får vi vara? Får ni sitta sitta var ni vill eller måste ni vara hemma eller?

88. R2

Jag gillar den. Det beror på vart i organisationen man jobbar. Det finns ju inte uttalade krav och jag tror det är den som är den största nackdelen. Till exempel jobbar du inom säkerhet så finns det krav på att man har privacyfilter på sin dator. Man jobbar aldrig mot ett publikt Wi-Fi och så. vi har en rätt så uppstrukturerad, men vi har samtidigt även andra coworkers som inte har de kraven på sig, vilket gör att de kan sitta med en helt öppen skärm på tåget eller vad som helst och visa känsliga saker, det finns just för.. Vart man får arbeta och på vilket nät är lite otydligt idag och det är någonting som vi arbetar på att förbättra. Ett tips jag kan säga är också, vi arbetar mot Zero Trust arkitektur. Och har ni Inte tittat på det så mycket så är det också väldigt bra. Antingen för vidare forskning men också i diskussion gentemot social enginering. Som kan vara bra att titta på.

89. TB
Ja, vi har sett så att det är något sånt där var det tror jag. Absolut, det är, ja det är aktuellt verkligen.

90. R2
Tidigare om man säger för 10, 15 år sedan så var det största att man skyddade sitt nätverk. Alla som var inne på nätverket var skyddade och därför gör det att socialen engineering kommer man in det är det fine. Problemet är idag om man vidtar en zero Trust arkitektur så beror det hela tiden på vad är det du vill ha access till. Så du kan ha kommit in en gång, men sen när du börjar försöka komma åt känslig data så behöver du också autentisera dig igen och bevisa vem du är och varför du ska ha materialet och då oftast så är det ju svårare att komma in för ska du då social engineera the same person.. Men då säger du ja och så vill jag ha den här i affärskritiska datan eller tillgång till den. Då kommer fler frågor. Jag skulle säga att vill ni ha någonting som är counter measure mot social Engineering så kan det vara värt. Om man tittar ur ett organisatoriskt perspektiv.

91. TB
Det är väl ett relativt tidigt stadium bara hela Zero Trust Model frågan.

92. R2
Nej, det är alltså Zero Trust har diskuterats i 20 år. Men om man ska vara ärlig, så tror jag det är svårt att hitta någon som har lyckats. Ja, om man säger ja, där kan jag ha ett namn. Jag vill kolla upp det innan jag delar det, men det det finns. [***] har en otroligt häftig Zero Trust presentation. Som man kan se live, men även en person här i Skåne som går ut och föreläser om det som är säkerhetsarkitekt.

93. TB
Okej, det låter ju riktigt spännande.

94. R2
Ja, han har väldigt bra insights för detta och jag skulle. säga att de har väl kommit vad jag tycker, nu kan jag inte se vad hela marknaden har gjort, men problemet att implementera en Zero Trust arkitektur är att man nästan behöver starta om från början. Man swipar allt man har

och så implementerar man det. Det är en väldig, väldigt stor effort att göra, men det kan mycket väl vara en av de mest effektiva. Kanske för social engineering.

95. TB
Har ni, du får väl svara på i den utsträckning som det går? Hur ser det ut hos er med Zero Trust Model? Har ni börjat implementera? Ni funderar på när ni gjort det redan?

96. R2
Vi har implementerat delar utav det. Vi har viss funktionalitet, men vi har inte det fullt ut så jag hade nog inte varit alltså litat på det.

97. TB
Just det. Hur ser det? Ut där det vill ni röra er mer mot det, eller?

98. R2
Vi rör oss mot Zero Trust definitivt.

99. TB
Okej, så är den önskan att implementera det helt fullt ut.

100. R2
Nej, där får man gärna avvägning mellan value och cost.

101. TB
Det är ganska storskaligt projekt.

102. R2
Precis. Men här kan vi väl säga att vi har kommit till den punkten där vi har insett att vi vill.. Ta oss dit i det nya alltså allt vi utvecklar nytt vill vi ha det tankesättet, men att vi låter alla som har utvecklats innan få stanna kvar med extra säkerhet som har funnits på den tiden och att vi då istället har en annan säkerhetsstrategi till det.

103. TB
Kan de spela väl med varandra sen att integrera alla system med varandra?

104. R2
Njaa problemet är oftast är det kommunikationen mellan system som är mest känslig. Så det är väldigt mycket beroende på fall vad det är man implementerar [xxx]

105. TB
Okej lite off topic kanske, men det är ju intressant för inte fråga om

106. AO
Men det var väl det vi hade va, tror jag.

107. TB
Jag tror faktiskt det. Ja nej, det är nog det. Ja, vi ser väl till om det något som behöver fyllas upp med som sagt. Vi avslutar väl inspelningen här då, eller?

108. AO
Ja, det gör vi där.

7.3.3 Intervju 3

Intervjuns längd
52 minuter, 27 sekunder

Datum och tid
2/5/22, 10:00

Förkortningar
AO = Albin Olsson
TB = Tarek Bermalm
R3 = Respondent 3

1. TB
Ja, men då börjar med att vi kan anonymisera ditt namn och din verksamhet om du ville.

2. R3
Ja alltså... Eller vet du vad vi gör så här. Låt oss ta det på slutet på intervjun istället. För att det beror lite på om vad vi ska prata om och hur detaljerade vidare och så vidare, så att jag skulle säga att jag, jag svarar på den frågan sen. Ska vi göra så?

3. TB
Ifall det är så att vi säger verksamhetens namn under intervjuns gång så och om du vill att det ska vara anonymt i slutet så själva transkriberingen, så tar vi bara ut det och då kommer det vara anonymt oavsett.

4. R3
Ja ja, alltså, generellt sett är det ju inte. Alltså det beror lite på hur ni ställer frågorna och så men men generellt jag pratar ju, jag kommer ju inte så att säga avslöja några hemligheter på det sättet så att säga så men men det det kan vara så att när man pratar om just säkerhetsarbete och såna saker så kan det vara lite känsligt beroende på var frågorna är och så. Låt oss ta den diskussionen igen på slutet så kan vi se om jag tycker att det var några känsliga frågor eller inte.

5. AO
Absolut. Okej, det deltagandet är helt frivilligt och du kan avsluta när du vill.

6. R3
Yes, det låter bra.

7. AO
Om, det är en fråga du inte vill eller kan svara på så är det bara att säga till så hoppar vi vidare.

8. R3
Absolut.

9. AO
Och i efterhand kommer du få tillgång till transkriberingen och så kan du säga till om det är något som inte stämmer eller inte, tycker speglar verkligheten riktigt och vi kommer ta bort inspelningen efter 30 dagar. Ja med det då tror jag vi var klara med det det där. Då går vi över till frågorna då. Okej, men kan du berätta lite kortfattat vad? Vad gör din verksamhet?

10. R3
[***] är ju en en verksamhet som sträcker sig väldigt långt tillbaka i historien, men vi jobbar ju med patent och varumärken. [xxx] Hjälper helt enkelt våra kunder hantera patent varumärken och sen har vi då en faktiskt en ny business också som heter digital Brands så att [xxx] förr i tiden så var ju varumärkena kanske lite analoga och så. Men nu är de digitala så att vi kan då hjälpa till att skydda varumärken och även på den digitala fronten, alltså att övervaka till exempel internet. Och så hur är varumärken används och så. Och sen har vi då också en en cyber Security business unit också faktiskt för att man kom på det att ja, men kunderna litar ju på oss eftersom vi förvaltar då deras varumärken och patent och så tänkte man sig okej, men varför inte också hjälpa dem med med IT säkerheten, för det hänger ganska nära samman här att om man har ett patent som man vill skydda någonting som är hemligt och så vidare så bör man ju också ha IT säkerhet därefter så att säga. För att inte någon ska sno patentet från en, till exempel.

11. AO
väldigt spännande. Och vad är din din roll i verksamhet.

12. R3
Jag är IT-säkerhetschef för [***].

13. AO
Yes, och vad har du för erfarenhet och bakgrund? Med studier och så.

14. R3
Jag har jobbat som managementkonsult inom IT säkerhetsområdet och IT i, vad blir det, 12 år. Ja så att jag har varit runt och sett ganska många olika verksamheter och sett vad som fungerar och inte fungerar på andra håll. Jag har jobbat inom många, många olika branscher och industrier. Så att jag tar den erfarenheten och och tar med mig, så det här. Så det är ju faktiskt mitt första jobb som inte är på konsultsidan.

15. AO
Alright, hur länge har du suttit nu som säkerhetschef?

16. R3

Jag började i november förra året. Så jag är ganska ganska ny, men ja börjar bli en ändå bli ett par månader nu.

17. TB
Ville bara dubbelkolla det så så jag förstod det rätt, så det är inte att du agerar konsult nu utan det är IT säkerhetschef på [***]?

18. R3
Ja precis. Sen kan man ju också betrakta är det är lite vad man lägger in, men alltså en del av CISO-rollen och IT-säkerhetsrollen är ju att agera konsult åt alltså internt kan man säga. För det handlar ju mycket om att hjälpa alltså hjälpa verksamheten att förstå IT säkerhet, att arbeta med det och göra rätt har rätt beslut så att säga. Nej, så att det det är ju när man får fortfarande använda sina konsultskills ganska mycket skulle jag säga.

19. TB
Ja, det går väl lite hand i hand?

20. R3
Gör det definitivt.

21. TB
Men det kanske jag fortsätter här och fråga, hur många dagar i veckan arbetar ni hemifrån?

22. R3
Vi brukar faktiskt ha. Det är lite speciell. Jag har lite speciellt upplägg för att resten av gänget jag jobbar med sitter i Göteborg. De är ju bara Köpenhamn varannan vecka, så jag är ju i Danmark en eller ungefär en vecka och sen är jag hemma en vecka så det är lite fifty fifty.

23. TB
Ja, jag förstår och sen för de andra som är i samma, nu kanske inte samma sits när det inte är samma team som du sitter i. Men generellt skulle du säga, att det är många som kan jobba hemifrån som de vill och ganska mycket eller ska man vara på kontor eller?

24. R3
Nej, men vi har väldigt. Vi hade en en filosofi innan att man skulle vara på kontoret, men sen kom pandemin och sen har vi ändrat faktiskt vår policy nu. Folk trivs att jobba hemifrån och man upptäckte också att verksamheten och resultaten blev faktiskt inte sämre. Utan snarare att man kunde faktiskt se nästan en ökad effektivitet, så att jag tror inte vi kommer gå tillbaka till en sådan här policy som säger att alla ska på kontoret alltid och det tror jag inte. Det tror jag inte vi är.

25. TB
Nu för de anställda som kanske jobbar hemifrån. Då finns det några specifika specifika regler för hur det ska gå till, hur ofta eller vilka omständigheter eller så.

26. R3
Oftast har vi en sån att det att det regleras med närmsta chef för det kan ju finnas vissa funktioner inom vårt bolag är ju mer sådana som kanske behöver sitta på kontoret. Vi har en del. Som i och med att vi hanterar patent så har vi ganska mycket typ handläggning, alltså klassiskt pappersarbete, att fylla i patentansökningar såna saker och det gör vi ganska mycket från våra kontor. Men sen har vi ju jurister till exempel som jobbar som ombud och och alltså det är då advokater. Ibland så är de ju ute i rätten och såna saker. De har ju en helt annan. De kan jobba från var de vill.

27. TB
Lite fall till fall om jag förstår rätt, ja Ja och om vi går vidare det här och fråga på frågor kring utbildning och lite så så undrar jag i vilken utsträckning utbilda er personal i social engineering? I skyddet mot detta?

28. R3
Ja, men du sa att generellt utbildning eller ja, det och så du frågar om om våra anställdas utbildningar då?

29. TB
Ja, men vi undrar nog så, det är inte vilken utbildning de haft tidigare innan jobbet och så där utan nu på arbetsplatsen till exempel.

30. R3
Ja vi har ju utbildningar kontinuerligt med personalen är just mer och så väljer vi oftast ut ämnen inom IT säkerhet som vill utbilda personalen inom ett specifikt ämne, så att det kör vi ju löpande under hela året, så sådana kurser.

Så det kan vara lite olika beroende på vad man vill pusha just då och det kan vara att vi känner att ja, men vi behöver arbeta på det här området. Vi har lite, vad ska man säga ett gap där och då satsar vi extra mycket på det utbildningsområdet och så. Det man väljer är lite efter behov och hotbild framför allt också.

31. TB
Har det förekommit, du kanske hade mer att säga. Ursäkta.

32. R3
Jag vad sa du om det?

33. TB
Ja, det lät som du kanske hade mer att säga och att jag avbröt dig.

34. R3
Nej, det är ingen fara, kör.

35. TB
Jo, hur ser det ut med social engineering? Förekommer det att ni har utbildningar som täcker just det området?

36. R3
Ja det det har vi så har vi speciellt då personal som kanske är extra utsatt, till exempel våra receptioner och så. De är ju väldigt utsatta eller de är mer utsatta, kanske än andra för att de har mycket, dels folk som besöker som de kanske inte. De känner inte till alla som besöker. De har folk som mailar dom har folk som ringer så att de har vi ju så att säga speciella utbildningar för för att säkerställa att de förstår det sen sen sen är klart att alla anställda måste ju förstå vad social engineering är, hur det fungerar och så. Men just receptionerna är mer utsatta än resten av bolaget

37. TB
Det är intressant faktiskt tror vi kommer komma tillbaka lite till. Det är flera frågor kring ja, sådana fysiska attacker till exempel, men men de här tbildning då till exempel, hur i vilket format kan de se ut? Är det digitalt eller presentation?

38. R3
Ja, det är E-learnings som vi skickar ut så att det är ju helt digitalt. Så är det oftast ganska begränsat hur lång tid det tar för att vi kan inte. Vi kan inte plocka ut flera timmar så ur ur verksamheten, utan det är ganska korta koncisa. [xxx] på inte utbildningar på ett specifikt ämne.

39. TB
Just det. Ja, har ni någon särskild utbildning för för just distansarbete då?

40. R3
… Nej, inte så distansarbete, att man ska, det har vi inte gjort. För att just hotbilden är är kanske lite annorlunda. Man sitter hemma ifrån, men fortfarande. Det här med distansarbetet har ju förekommit ganska länge innan pandemin också så att det enda som har skilt skiljer sig nu. Det är kanske att det är fler i bolaget som sitter hemma och jobbar, men de har ju fortfarande funnits en beredskap kan man säga innan och ganska stor förståelse för att man har behövt sitta hemma också innan, så det är nog volymen av anställda som sitter hemifrån som har ändrats. Skulle jag säga.

41. AO
Så ni vi särskiljer dem inte på något sätt, distansarbete?

42. R3
Nej, så gör vi inte.

43. TB

Ja du kan ju fortsätta där Albin.

44. AO
Ja, men hur utbildar ni era anställda i verksamhetens policys?

45. R3
Det handlar ju oftast om att plocka ut saker ur en policy som man utbildar på så jag kan ta ett exempel. Det kan vara till exempel. Att att en av de sakerna vi tittar på är till exempel password policy. Vilken typ av password tillåter vi? Hur långa ska de vara och så vidare och då kör man ofta sen. En target [xxx] utbildning på det området som pratar om. Men vilka password ska vi använda? Vilka ska vi inte använda? Hur ska vi tänka när det kommer till lösenord? Hur ska vi hantera lösenord och så vidare? Dos and dont's också med lösenord. Så att det kan man säga. Jag tror inte vi. Vi har ingen utbildning så att säga. Nu ska vi gå igenom den här policyn utan det hamnar mer om vilka avsnitt i policyn är det vi vill Pusha ut och som är viktiga för användarna. Så att det är ganska långa. Policydokumentet det tar mycket tid. Vi har ju också förväntningar att man ska läsa policydokumenten, men vi vet ju också hur verkligheten är. Att man kanske inte läser dokumenten helt så så att därför pushar vi ute. Det är specifika där med specifika delar som vi tycker behövs pushas.

46. AO
Okej och hur ofta uppdateras utbildningens innehåll är det? när policys uppdateras, [xxx].

47. R3
Skulle jag säga varje gång vi skickar ut en kurs så kollar vi hur innehållet känns och om det känns relevant. För det händer saker hela tiden på IT-säkerhetsområdet så att man måste hela tiden bara skruva lite på på grejer. Det om man bara tar en en sån sak som password, till exempel om jag tar det som ett exempel att vi ser ju en trend, att vi har längre och längre passwords vi lägger på mer krav på komplexitet på passwords. Nu pratar vi mycket om passphrases istället för passwords. Och och det där har ju ändrat sig att ta backa bara 5 år så var det helt annorlunda. Då hade man mycket kortare lösenord. Man hade dess börjat fundera på passphrases och så vidare så det där flyttar sig hela tiden, kan man säga. Mognadsgraden också bland de anställda blir högre också över tid, det vi märker att i takt med att det här börjar IT säkerheten börja på poppa upp i Media och blir mer aktuell. Och folk har själv provat på det med med coop till exempel det som hände på Coop. Nu börjar folk förstå, att nu har polletten börjat trilla ner bland gemene man också att det här inte bara är någonting man kan strunta i och sova igenom.

48. AO
Det svarar lite på vår nästa fråga om det är, ni gör det kontinuerligt. Så jag tänker att jag går vidare. Hur säkerställer ni att er säkerhetspolicy följs av de anställda?

49. R3
Vi gör ju tester, alltså ett alltså. Vi gör ju till exempel tester av säkerheten. Så det kan ju vara till exempel att vi skickar ut exempel egna phishing-mejl och ser hur många som klickar på

dem. Vi kan göra andra typer av tester. Vi kan testa receptionerna, till exempel att de skickar ut en pen-testare till exempel och försöker ta sig in fysiskt på bolaget. Ja så att vi gör ju tester på och då går vi olika aspekter. Och se till att det kan ju vara exempel vissa saker kan vi ju också testa internt så att det handlar till exempel om access om man pratar om accesspolicy till exempel. Så det vi ofta gör då är att vi plockar ut till exempel, vem är anställd i HR-systemet och så jämför vi det med vilka har accesser och så ser vi om det är några differenser där och då adresserar vi om direkt ju de differenserna. Så att en del är ju tester av personal och tester av verksamheten och andra är att vi faktiskt gör kontroller att vi jämför helt enkelt accesscontroller.

50. AO
Okay, då går vidare lite då. Men arbetar ni särskilt med att säkerställa att det följs av distansarbetande?

51. R3
Du menar att policys följs av distansarbete.

52. AO
Ja exakt.

53. R3
Nej, det skulle jag inte påstå. Det är också svårt med distansarbete för att du kan inte bara gå in och ställa vilka krav som helst i någons hem. Det är inte så det funkar. Så att jag skulle säga att i takt med att folk jobbar mer på distans så flyttar säkerheten in i applikationer i infrastrukturen i laptops och så vidare, att man säkerställer att man har en säker setup. Och räknar med att den här datorn som de anställda har kommer förmodligen sitta, kanske på ett oskyddat Wi-Fi, kommer sitta med ungarnas datorer på samma nät och så vidare, så vi utgår från att. Vi konstruerar kan man säga säkerheten efter det. Så att det är lite samma [xxx] lite samma problematik har man haft innan, också folk som jobbade på hotell och sådana saker och det har också varit väldigt förekommande tidigare. Folk som är ute och reser så kopplar de upp sig på flygplatsen och så då sitter det samma nät som massa andra så den den tankegången om att skydda devices och sånt har ju, har man funderat på ganska länge och det är lite samma tänk man applicerar nu. men sen är det som ni säger där är ju klart att det finns problematik och här. Ta en sån sak som, jag menar om vi är på kontoret och skriver ut någonting så har vi ju secure print, det vill säga att du måste blippa det in i skrivaren för att få ut utskriften. Så det är en viss säkerhet där. Där är ju också att vi har ju på våra kontor har vi shredders till exempel så att när du då har skrivit ut någonting hemligt så shreddar du det efteråt. Men det är klart det är inte så att vi har shredders som vi skickar runt till folk eller att vi har Secure print på skrivaren som folk har hemma och såna saker så där är ju svårare att skydda ett distansarbetande gäng än de som sitter på kontoret. Så det skulle jag säga. Det är ett problem som jag tror många boxas lite med, hur man ska tänka där och det är också svårt att ställa krav på folk i deras hem. det enda vi kan säga till exempel att ja, men vi säger oftast till våra anställda att använd kryptering på era hemmanätverk och såna saker och så har vi oftast, vi pratar lite också om hur det funkar med WPA2 och vilka typer av krypteringar man

ska använda på trådlösa nät och så. Men sen kan ju inte vi kontrollera att det blir efterlevt. Vi är inte hemma hos folk och vi kommer inte göra slumpvis besök hemma heller så att det är så det är.

54. AO
Men om vi går vidare lite bara. Hur arbetar ni med säkerhetskultur i samband med distansarbete är utmanande, i så fall hur?

55. R3
Ja, men det är lite som jag sa innan att begränsningen är att vi på kontoret kan vi bestämma om hur vi gör och vi hanterar dokument och så här. Men det kan man inte riktigt göra i någons hem. Det vi dock säger är ju att, jag menar, vi har ju sådana policy som säger att efter dagens slut så stänger du av din dator till exempel för det innebär då att om datorn blir stulen så vi har ju diskkryptering och såna saker. Så att en stängd dator är är bättre skyddad än en som är igång till exempel. Sådana saker att vi be folk stänga av sina datorer när du inte använder dem. Att de givetvis inte ska ha, vi har lite såna grejer också att man inte ska få lägga datorerna, att man inte ska förvara dem i bilar och såna saker. För det är väldigt vanligt att folk snor laptops ur bilar och så. Så att såna saker, men sen kan vi ju inte veta hur säkerheten ser ut i ett specifikt hem. Det är ju helt omöjligt.

56. TB
Har ni upplevt någon skillnad där att efter pandemin med distansarbete och så där att säkerhetskulturen har tagit sig annorlunda har ni kunnat uppleva det eller känna det kan man säga.

57. R3
Det är en bra fråga, om vi sitter och funderar på om vi har sett några trender när det kommer till distansarbete. Ja, jag kan inte säga att vi har sett en ökad hotbild av att folk sitter hemma, det skulle jag inte säga utan hotbilden är extern. Så den har ingenting med att vi jobbar hemifrån att göra utan snarare att hotbilderna ändrat sig från internet och så. Men nej jag skulle inte säga att kulturerna ändrats på något sätt, så.

58. TB
Ja men intressant. Vi går vidare lite, då ska vi se. Ja alltså, du har ju varit lite inne på det här kanske, men vi har en fråga som gäller, säkerställandet av policys och så där vid distansarbete men. Ja, om jag förstår dig korrekt.

59. R3
Men det är lite samma sak att de här testerna och det här vi gör. Det görs ju oavsett vad folk sitter, så vi är inte beroende av vad folk sitter när vi gör den här typen av tester och så och phishing testerna som vi snackade om de fejkade phishing email som jag själv skickar ut, de går ju ut oavsett var man sitter så att säga.

60. TB

Ni särskiljer inte på dem.

61. R3
Nej, nej, det är inte så att vi är att vi har ett speciellt phishing mejl som går till de som jobbar hemma eller något sånt.

62. TB
Jag förstår och men om man kollar lite på riskmedvetenhet och så där. Hur kollar ni på att arbete? Hur arbetar ni med det? Att hålla en bra medvetenhet kring risk och så hos medarbetare?

63. R3
Jag skulle säga en av de här som indikatorerna som jag pratade om innan med phishing så att vi skickar ut egna phishing mail och så där tittar vi på hur många som klickar på dem och där ser vi ju att våra anställda klickar på saker. Så att det är ju ingen surprise. Så där jobbar man ju mycket med att försöka få ner, öka medvetenheten och att göra att folk tar mindre risker helt enkelt, att inte klicka på saker som är oroliga eller tycker är konstiga. Så att jag skulle säga, desto mer medvetenhet om IT-säkerhet som finns i bolaget desto mindre kommer folk att klicka på saker det hänger ihop.

64. TB
Just det.

65. R3
Helt klart. Så mer utbildning mer prata om det. Mycket mer vara ute och prata med verksamheten om det. Det hjälper väldigt mycket.

66. TB
Där kan ju verkligen distans vara en utmaning när man är lite begränsad till ja, men intervjuer som dessa sen skiljs man åt efter man [xxx].

67. R3
Alltså så är det ju. Det är klart att det finns en dimension att det är lättare att ta tag i någon på kontoret och fråga någonting än över Teams det blir mer formellt om man ska ringa någon och så på det sättet påverkas det ju att det är lättare att få en informell diskussion om IT-säkerhet på ett kontor än vad det är när alla sitter hemma så är det ju.

68. TB
Hur skulle du värdesätta den informella biten då?

69. R3
Ganska mycket, men.. Ja, jag märker mest att jag tror snarare att det handlar om hur proaktiv man är från från IT-säkerhetsavdelningen och är ute och pratar om det här. Jag märker att jag får mer när jag är ute och pratar med verksamheterna. Har ibland så har vi blivit ombedd att

hålla lite inlägg och sådana här presentationen också och då märker man ju att folk är mer benägna att komma till en annan när man har haft något ämne som man har pratat om.
Så det handlar nog om att göra sig själv tillgänglig också. Det är också en kultursak. Visa verksamheter betraktar ju CISO som en surgubbe som sitter och är lite polis och den mentaliteten försöker jag ju komma ifrån. För jag är jag tycker inte om den där. Jag tycker inte vi ska vara polis. Jag tycker vi ska vara mer hjälpa folk. Jag gillar mer när folk kommer till oss och ber om hjälp om någonting och säger, kan vi titta på det tillsammans, än att folk bara tar massa dumma beslut och kör på. Det är det farligaste skulle jag säga. När folk tar massa egna initiativ och bara kör på, det är jättefarligt.

70. TB
Det är samarbetet där?

71. R3
Ibland är det finns ju vissa bolag har byggt upp en sån kultur att man ska vara rädd för CISO att CISO är någon slags, kommer in och slår en på fingrarna,. Det är inte sådan kultur vill ju inte vi ha överhuvudtaget. Det är inte så vi jobbar. Det är samma sak också vi har en policy att att om någon kommer och säger att de har gjort någonting. Så det blir det aldrig en blame game av det. Det är bättre att folk kommer in och berätta vad de har gjort, att de har klickat på lite saker och laddat ner saker och sånt. [xxx] Det finns kanske bolag som skulle säga okej, men då skickar vi en skriftlig varning av du vet för att du har gjort någonting dumt och så vidare. Men det ju det vi jobbar på att få mer att coacha dem mer till att ta rätt beslut. För det är farligt också om man har en sån kultur där folk inte vågar komma och berätta saker, för det är jättefarligt.

72. AO
Verkligen att om man får en varning kan ju det bara sluta med att man inte rapporterar nästa gång helt enkelt.

73. R3
Exakt exakt.

74. TB
[xxx]. Vi har diskuterat detta med säkerhetskultur och medvetenhet och dessutom kanske informella bitar som vi pratat om. Vilken roll har ledningen i allt detta?

75. R3
Ja, de har en jättestor roll för att om inte ledningen diskuterar det här så kommer inte verksamheten heller diskutera det. Nu kan vi dock se att ledningsgruppen hos oss pratar väldigt mycket om IT-säkerhet och så vidare så att. Det märkts att det har hänt någonting. Jag tror att det handlar om medialt intresse också om att rapportera om IT-säkerhet på ett annat sätt nu än vad man gjorde innan. Så att jag det jag tycker var medvetenheten är ganska stor, i alla fall i vår ledningsgrupp om här om att det här inte är någonting vi kan strunta i. Och vi, vi kanske utmärker oss också inom den här branschen som är ganska, vi kommer från en ganska

traditionell bransch som har ganska låg IT-säkerhets mognad. Där har vi ju sagt att vi ska vara bäst inom branschen på det här och jag tror att vi satsar mycket mer på det här än vad våra konkurrenter gör.

76. TB
77. Albin vill du fortsätta där med nästa fråga?

78. AO
Ja, absolut om du kan. Vi har delat in social engineering i några olika typer som fysiska, sociotekniska, tekniska och sociala. Kan du beskriva lite hur ni skyddar er mot dessa? Man kan ju börja med att fysiska som typ shoulder surfing och dumpster diving till exempel.

79. R3
Shoulder surfing det är ju lyckligtvis en sådan grej, som kanske har blivit lite mindre av under pandemin eftersom folk reser mindre. Men där är det ganska klassiskt att skapa awareness runt det här med shoulder surfing, så vi har faktiskt haft kurser som har varit shoulder surfing alltså som handlar om shoulder surfing, så det har vi haft. Sen handlar det mycket om att se till att folk använder screen protectors och sådana saker på flygplatser. Vi har faktiskt laptops med inbyggd sådana som du kan slå på, så du behöver inte ha en sån här skärm som du sätter utanpå utan du kan. Det finns ett läge på skärmen som du slå över till så då kan du inte se det från en vinkel till exempel.

80. AO
Det är spännande. Ja sociotekniska har du diskuterat lite om phishing och sånt?

81. R3
Phishing är ju ett jättestort problem skulle jag säga och har seglat upp till och nog bli ett av de största säkerhetsproblemen mycket större än shoulder surfing och dumpster diving och sådana saker där. Dumpster diving det är ju ganska svårt i praktiken nu med tanke på att det mesta shreddas och folk har ganska god medveten om att den måste shreddas också och sen är det också en sak med att folk börjat skriva ut mindre. Vi ser ju också volymerna på print outs går neråt. Så att tack och lov så är dumpster diving inte ett jättestort problem. Som phishing då till exempel som är upp på uppsegling och det har verkligen exploderat phishing området. Vi ser ganska avancerade phishing försök, impersonation attacks. Man pratar mycket om BEC business email compromise. Man komprometterar någons mailkonto som skickar man ut illegitima mail från det kontot till andra verksamheter. Det har vi ganska mycket av också. Ja och det där är jättesvårt för att ibland kan det där de där attackerna kan vara jättebra gjorda. De använder samma signatur och de använder kanske ibland så hijackar de en mejltråd som de hittar då i någons inbox skriver vidare på den mejltråden använder samma språk, typ. Jag skulle säga att email och phishing och så har blivit ett av de största, absolut största hoten som vi har.

82. AO

Spännande om man går in på de tekniska då så har vi alltså till exempel OSINT om du har hört talas om det, open source Intelligence där man typ letar efter personer i bolaget via sociala medier och kommer in på det sättet och attackerar dem genom att hitta information om de utanför organisationen.

83. R3
Man använder exempel oftast den typen av öppna källor när man gör en sån här pretexting social engineering. Vilket innebär att man bygger upp den här kunskapsbanken om en person redan innan man försöker attackera. Så jag skulle nog säga att det där förekommer absolut säkert och vi vet ju också att folk sitter och researchar oss. Man ta reda på vem som är i vår ledningsgrupp och skickar specifika mail till dem. Phishing mejl då till exempel. Så att vi vet att det förekommer jättemycket. Du kan göra ganska avancerade social engineering upplägg där med hjälp av information du kan hitta på linkedin till exempel. du kan hitta relationer, du kan hitta attackvinklar som man kan se helt klart i den offentliga informationen, men det är det är ju å andra sidan någonting som är väldigt svårt att skydda sig mot så att det är inte riktigt någonting du kan göra åt det mer än att utbilda folk i social engineering och att de förstår. Just det där med att folk sitta och göra research och sånt, det är det vet vi att det förekommer.

84. AO
Okej ja ja sociala då. Men det var vi inne på lite med receptionisterna, som att manipulera och övertala via till exempel som telefonsamtal. Upplever ni att det är ett problem eller hur ni gör ni? För att skydda mot det?

85. R3
Ja, men bland annat handlar det ju om att utbilda receptionen. De är mer misstänksamma än resten av verksamheten. Ja, men det handlar mycket om också att säga, alltså det är en utbildning sak skulle jag säga. Dom litar till exempel inte på nummer, alltså ringer ett nummer så är de ganska väl informerade om att ett nummer kanske spoofas till exempel, så man kan inte lita på ett nummer som ringer in. Man använder mycket såna här typ. Okej, vi tar ett meddelande och så får de ringa tillbaka så att man verifierar. Kanske sparar informationen till oss och sen får vi se är det här faktiskt en kund som ringer? Vi har ju interna kunddatabaser och sen så också. Vi har ju möjlighet att göra research själva om den som ringer och verkar det väldigt misstänksamt så blir det ju rapporterat till mig till exempel och då sätter jag igång en utredning på det. Där man tittar närmare på det Det är ett, jag skulle inte säga att det är jättestort problem, men det är någonting som man måste ha väldigt observant på samma sätt till exempel receptionen.

86. AO
Gör ni något speciellt för distansarbetare i arbetet mot social engineering?

87. R3
Nej, det gör vi inte.

88. AO
Vill du fortsätta där, eller?

89. TB
Absolut ja, det är lite generella frågor i det här kan man säga om det är några specifika utmaningar så som ni upplevt I säkerhetsarbetet mot social engineering. Ser du några utmaningar som du tänker på.

90. R3
Alltså jag utmaningen återigen phishing mail, extremt svårt i och med att det inte finns något system för att i och med att angriparna kan sända mejl från en potentiell kund eller affärspartner och att när mejlen kommer till oss så ser vi ju ingen skillnad på det. Så det man kan göra där eller det vi jobbar. Det är ju mycket med att hitta på. Det finns lite nya lösningar som arbetar eller använder machine learning, till exempel för att titta på email. Man tittar bland annat på man har en NLP, natural language processing för email text och så vidare. Man kan se avvikelser för om du brukar skriva hej och så skriver de plötsligt hejsan så kommer NLP e reagerar på att språket avviker till exempel så att för att skydda sig mot det så använder man mycket såna här. Vi kan titta till exempel på IP adresser att det här mejlet som kommer från den här kunden brukar komma från den här ip adressen. Men plötsligt så kommer det från en annan ip adress till exempel. så att det handlar om såna små clues som det finns lite mjukvara som tittar på sånt för att detektera avvikelser. Det är någonting som vi satsar mycket på och som är ett bekymmer inom branschen. Speciellt, kanske inom vår bransch där man är email beroende. Vi skickar väldigt mycket email och tar emot väldigt mycket email så att vi kanske är mer utsatta än andra tror jag.

91. TB
just det. Men så vidare till. För man vill ju gärna hålla goda strikt rättigheter på data så att rätt person ska komma åt innehållet. Men samtidigt vill man även ha en bra tillgänglighet på datan obehindrad tillgänglighet. Är det här något ni jobbar med för att behålla obehindrad tillgänglighet för medarbetare.

92. R3
Du menar. Bara så jag förstår frågan, men för du menar alltså om man vill alltså nu tänker på tillgänglighet, till exempel ha tillgänglighet för olika devices, eller hur tänker du med tillgänglighet?

93. TB
Ja, mer tillgänglighet på data och sådär så att om du har ett större system er verksamhet i det här fallet då så finns det mycket datainformation som en viss medarbetare kan vilja tillgång till. Och hur arbetar med den här tillgängligheten att rätt person ska ha tillgång samtidigt så? Samtidigt som man vill ha obehindrad tillgång för dem som faktiskt använder datorn. Albin skulle du säga att jag formulerat frågan korrekt här.

94. AO

så jag tänkte ja.

95. R3
Jag tror det du försöker säga det du nämner är lite mer alltså access control, hur man säkerställer till exempel att vi inte har för breda roller och alltså för att det är ju så att inom i vårt bolag så kanske man jobbar med några specifika kunder och då är det ju då specifika kunder när man har tillgång till. Så vi försöker komma bort från att ge alla tillgång till allt det. Den typen av tillgångsallokering kan man säga undviker vi så långt det bara går så att du har tillgång till dem kunderna du ska jobba med kan man säga. Så på det sättet försöker vi alltid begränsa accesser så att man inte har för breda accesser. Detta gäller ju på kundnivå också, att man inte kanske har tillgång till alla kunder utan specifika kunder.

96. TB
Ja just det, och hur skulle du säga att hos er verksamheter idag att det generella säkerhetsläget ser ut?

97. R3
Ja, men jag. Jag tror hotbilden har nog aldrig varit så hög som just nu. Men det handlar inte om en hotbild generellt mot vårt företag, utan det handlar om en generell hotbild som bland annat har förstärkts av kriget i Ukraina. Väldigt mycket rysk aktivitet på internet. Så det har inte, det är inte vårt bolag som är under ett extremt hot, utan det är generellt, en generell hotbild som sträcker sig mot alla företag skulle jag säga alla är fair game just nu. Sen är det klart att man blir mer. Vi har sett sådana trender också, bland annat så var det en europeisk verksamhet här nu för någon vecka sedan som när de då de pratade om att de skulle göra ett exception att skeppa gods till Ryssland. Det finns ju exception mot sanktionerna och då funderar det bolaget för att alltså att ansöka om en sådan exception. För att kunna sälja till Ryssland och sen så valde de att inte skicka in en sådan ansökan om att få ett exception och då inom 24 timmar blev de angripna av rysk ransomware. Så vi vet att man kan hamna på radarn av den ryska staten till exempel och och då är det inte jättekul. Så att någonstans handlar det här lite om att försöka se till att hålla sig borta från radarn lite att inte ploppa upp på radarn för mycket. Ja så att.

98. TB
Spännande

99. R3
Det skulle jag säga att jag tror inte att hotbilden mot oss så att säga är på något sätt ökad.Men jag tror att den generella hotbilden har definitivt ökat och vi är ju mer utsatta och ransomware är ju ett jättestort problem, för jag skulle säga alla stora företag. Så att. Det är någonting som man sitter och funderar på mycket hur vi ska kunna klara ett sådant angrepp.

100. TB
Så kring framtiden. Hur ser ni på ert skydd mot social engineering? Hur arbetar ni kontinuerligt för att bli bättre på att skydda er?

101. R3
Men det är ju utbildning och utbildning, alltså. Jag tror när det kommer till social engineering eftersom inte du kan. Det är få tekniska prylar eller kanske phishing.

Där finns lite tekniska prylar du kan installera som jag pratade om tidigare. När det kommer till sådana här saker som att någon ringer till dig och försöker få ur information eller få dig att göra någonting. Det finns ju inga tekniska prylar du kan köpa för att skydda dig mot det, utan det handlar om utbildning av personalen. Se till att de förstår det att de tar det till sig. Att också testa dem ibland, att utsätta dem för såna här saker och se hur de klarar det. Ja, det är nog bästa skyddet skulle jag säga. Jag tror inte det är, det är ju det som det är, det man kan ha och jobba med så att säga.

102. TB
Använder ni det att testa använder nu det lite i samband med utbildningen som att utbilda på det som kanske inte gick så bra till exempel.

103. R3
Det skulle man kunna tänka sig att man gör absolut. Jag tror inte vi har kommit så långt att vi är där nu när vi alltså vi kopplar ihop det på det sättet. Men absolut. Det är klart att det finns. Man vet kanske vissa delar av bolaget kanske är mer utsatta och exponerade än andra och det är klart att det är viktigare att deras medvetenhet är högre än resten så är det ju. Men det där jobbar vi faktiskt inte. Vi jobbade med lite utbildningar som riktar sig mot specifika grupper anställda.

Bland annat så är ju ledningsgrupp är väldigt utsatta så de har vi faktiskt speciella vi för extra utbildning för ledningsgruppen och sen kan det finnas vissa funktioner eller HR och finance till exempel som också är utsatta. Ja och där så har vi också special upplägg med dem.

104. TB
Intressant. Då egentligen bara en sista fråga om du vill tillägga som vi inte frågat om eller gått in på?

105. R3
Nej, det är väl. Det är väl lite det ni med frågorna om distansarbete så att det man kan säga generellt sett som har ändrat sig inom IT-säkerhetsområdet är ju att innan pratar man väldigt mycket om perimeter defence, alltså att vi ska bygga, vi ska ha höga staket, vi ska ha övervakningskameror. Vi ska ha larmsystem, vi ska ha allt det där vi ska bygga en borg på vårt kontor till exempel. Den typen av tänk är ganska mycket föråldrad och det är inte riktigt så man tänker nu för att den här klara perimetern som man har haft tidigare har ju försvunnit med tanke med på distansarbetet.

Vi har ju inte samma tekniska säkerhet hemma hos våra anställda. Så att nu ska ni säga att det största skiftet är just de här perimetern har försvunnit.

Nu sitter alla. Innan så byggde många bolag byggde traditionellt för att bygga ett starkt försvar runt om och sedan när du väl var inne på nätet kunde du göra vad som helst, fri tillgång och så vidare. Så jag tror att den här tankegången att man antar. Man pratar mycket om zero trust man pratar mycket om att man ska utgå från att vi är breached, till exempel assume breach. Den typen av tankegång blir ju mycket mer aktuell med tanke på distansarbete så man antar egentligen att ens perimeter är. Att något tagit sig genom perimetern och att säkerheten inte ligger i perimetern utan ligger i applikationer i kryptering i hur man styr access och såna saker. Så att det tror jag är ett stort skift.

106. TB
Där är jag också nyfiken på alltså hos er verksamhet bland det distansarbete anställda och de som råkar befinner sig på kontoret. Ser ni på det som någon annan typ av alltså en större säkerhetsrisk och så där eller ser ni mer som att det bara råkar vara någon plats eller ett annat sätt att arbeta?

107. R3
Nej, jag skulle nog säga att det är större säkerhetsrisk för att det är ju istället för att vi har ett kontor som jag kan se till att jag har kontrollen över. Vi har övervakningskameror och vi har alla de prylarna vi har där. Det har ju inte hemma hos folk på samma sätt. Så att på det sättet, skulle jag säga att det är, det är svårt. Ja, men det är större risk med att folk sitter hemma. Det är det.

108. TB
Ja får utbildningen större vikt då? När man inte har samma tekniska möjligheter.

109. R3
Ja, men det får den ju i någon mening. Det är klart att utbildningen blir ju viktigare. Framförallt kanske den aspekten som vi pratade om innan att med social engineering kan det vara så att om någon ringer in och frågar någonting om det så är det lättare för dem direkt och fråga en kollega och säga att vad tror du om det här. Hemma, så kanske inte du alls tar dig tiden att ringa en kollega och fråga utan du bara ja, men då lämnar jag de här uppgifterna. Så jag tror kanske det där med att man sitter i ett sammanhang bland kollegor gör att man diskuterar saker mer kanske. Eventuellt, jag vet inte att det är svårt att veta.

110. TB
Intressant i alla fall. Jag tror vi fick med allting i så fall.

111. AO
Ja då kanske vi ska fråga igen om anonymisering.

112. R3
Ja, jag tror nog att vi gör så att vi inte tar med vårat namn bolagsnamn om det är ok mer.

113. AO
Ja ja, absolut.

114. R3
Ja sen antar jag antar att mitt namn inte hängs ut heller. Nej, nej.

115. TB
Det anonymiseras.

116. R3
Nej, men då gör vi så ja.

Det, det hänger ihop med det jag pratade om innan med att mycket. Ja, det är faktiskt så att vi märker det att desto mer du sticker ut hakan inom IT-säkerhets. Vi har ju märkt det våran business unit som jobbar med cybersecurity. När de så att säga de umgås i kretsar med folk som är lite speciella. Ja, alltså nej, men att.
Jag vet inte om hur mycket ni har jobbat med penetrationstester och såna saker. Men det finns en del penetrationstestare som är jävligt duktiga, men är lite halvt gränslösa det där med. Jag har faktiskt en kompis som jobbar som penetrationstester han har ju en filosofi att han går ut och hackar bolag och sen ringer han dem och säger jag har hackat er, vill ni ha min hjälp? Det är ingen affärsmodell jag rekommenderar, men han har faktiskt haft ganska stor succé dessutom och det är inte jätteetiskt och så vidare, det kan vi diskutera om Det är bra approach men det finns ganska mycket folk som är lite halv gränslösa som tycker att ja, men nu sitter ni här skriver att ni har bra säkerhet då innebär det att jag blir lite triggad av det och då blir ni en target. Så att man ska tänka på hur ens varumärke är, därför jag säger att jag nog inte vill ha vårt företagsnamn med för att vi vill minimera riskerna. Så det är inte så att vi har lämnat ut några hemliga uppgifter, men det är lite mer för att just att exponera sig själv i fel sammanhang och det är samma sak med företag som cirkulerar mycket på darknet, till exempel. De vet att vi blir mycket mer utsatta. Vi, vi har ju folk som sitter och monitorerar darknet. Vi säljer faktiskt det som en tjänst till andra bolag. Så att man tar. Vi har en tjänst och så tjänsten är då att vi håller koll på darknet forum och ser deras bolagnamn börja dyka upp i massa databasdumper och såna saker då heller. Då gäller det och spänna fast sig är när det händer. Så att det där är också någonting som är ett viktigt hur mycket man exponerar sig själv att verkligen.

117. AO
Yes yes, men då.

118. TB
Ja kan bara tillägga det lite kort här att vi kommer skicka ut. Transkriberingen till dig också. Så förutom företagsnamnet, ifall något som du inte vill ska vara med, då kan vi korrigera det.

119. R3

Alltså, man kan säga så det jag har nämnt här så länge vi inte nämner att vilket bolag jag jobbar på så är det lugnt. Det är ganska känt inom industrin. Det jag har sagt så att det men det är klart att olika företag upplever ju situationen olika, så är det ju alltså hur man exponerar sig och såna saker skiljer sig väl mycket. Vissa bolag kan ju inte vi. Vi kanske kan göra lite så här att vi seglar under radarn, men andra kända varumärken. Jag har lite folk att känna på [***] till exempel de är ju redan exponerade och utsatta i jättemycket, för allt möjligt och de var faktiskt med i ett sånt här bug bounty program ganska nyligen med femtontusen etiska hackare då som angrep dem. Så att det är skillnad där om har man ett väldigt känt varumärke. Då är man redan på radarn, då kan det kvitta kanske, men är man ett litet varumärke som inte är så känt och inte ligger på radarn ännu nu så försöker man att hålla sig borta från radarn?

120. TB
Ja intressant.

121. AO
Men då tackar vi för oss då så stänger jag av inspelningen här.

122. R3
Ja tack själva.

123. TB
Tack så mycket.

7.3.4 Intervju 4

Intervjuns längd
42 minuter, 53 sekunder

Datum och tid
2/5/22, 15:00

Förkortningar
AO = Albin Olsson
TB = Tarek Bermalm
R4 = Respondent 4

1. AO
Så där. Då börjar vi med och nämna att vi kan anonymisera ditt namn och verksamhetsnamn. Om, det är så du vill ha det.

2. R4
Ja, det beror ju på vilken nivå av sång eller svar ni förväntar er. Jag är ganska generalist så jag tror inte det kommer bli. Någon känslig information som ni tar del av, så det är inga konstigheter där.

3. TB
Ja, vi lär i alla fall göra ditt namn anonymt i efterhand så kan vi komma tillbaka till frågan och se om verksamheten också ska bli anonymt. I så fall kan vi plocka bort i transkriberingen de gångerna du eller jag nämnt verksamhetesnamnet.

4. AO
Ja och sen så vill vi bara säga deltagandet inte är frivilligt och du kan avsluta när du vill. Om det kommer upp en fråga som du inte kan eller vill svara på så går vi bara vidare. Och du kommer få tillgång till transkriberingen efterhand, så du kan säga till om det är någonting du inte tycker stämmer eller om vi vinklar det på något speciellt sätt, och vi kommer ta bort inspelningen efter 30 dagar.

5. R4
Ja, men det går bra.

6. AO
Bra med det sagt så kör vi igång. Okej, kan du beskriva kortfattat vad din verksamhet gör idag?

7. R4
Tänker du bolaget som jag är anställd på, eller? Ja, det är ju så att jag är konsult och jag är anställd på ett danskt bolag. De har huvudkontoret i Örestad. Det är alltså det är ganska

gammalt bolag hundrafemtio år och det men det är mest jurister, så det är mycket varumärken och domänhantering och patent och sånt typ fyrahundra femhundra anställda som jobbar med det. Jag är mer då på administrations hållet där alltså jag jobbar med managementfrågor och hur bygger man eller styr man upp en verksamhet kring det här med informationssäkerhet och hantering. Så jag jobbar väldigt mycket med olika standards och ramverk och sånt där då så de används då och så

8. TB
Men vad är din yrkesroll?

9. R4
Ja, jag är ju konsult så jag jobbar ju 100 % ute på kunduppdrag så är mitt företag nöjda.

10. TB
Som säkerhetskonsult?

11. R4
Ja precis så är det, just nu är jag på uppdrag där vi jobbar med vehicle cyber security.

12. TB
Jag undrade också då vad du har för erfarenhet och bakgrund och så, kanske i form av vad du pluggat och tidigare arbetsplatser.

13. R4
Tekniskt gymnasium och så vill jag inte jobba med datorer sista året och så pluggar jag 3 år ekonomi och inom då nationalekonomi och sådant där. Men sen hamnade jag i Lund.

14. AO
Men då tänkte vi gå vidare lite. Hur många dagar i veckan arbetar arbetar ni hemifrån?

15. R4
I och med att jag är konsult så jobbar jag ju nästan 100 %. Jag har ju in 3 4 dagar i månaden på kontor på vårat kontor, men jag sitter ute hos kunder kanske 2 dagar i veckan och sen sitter jag hemma 2 dagar i veckan och så är den fördelningen ungefär.

16. AO
Yes, vill du fortsätta TB?

17. TB
Ja absolut, så vi undrar lite kring utbildning . Vilken utsträckning utbildar ni personal, i social engineering. Går ni i några utbildningar kring detta?

18. R4

Ja alltså vi har, vi på vårat bolag, har en introduktionskurs, kan man säga. Alla nyanställda går ju igenom lite olika utbildningspaket där IT och infosec och levererar en bit. Sen finns det ju då, vad man ska man kalla det för? Riktade kurser. De här vännerna i Indien. De har ju lite såna här microlearningverktyg då. Men det är kanske någon eller ett par gånger om året och det är inte bara social engineering då, men de kör lite såna här tester med phishing attacker och fejkade mejl. Men annars är det ganska mycket upp till var och en alltså. Det finns information att hitta, men då måste man ju själv leta upp det, så det är ingen som sitter och naggar oss anställda för att hålla oss uppdaterade i vad som händer och sker. Utan det är i det allmänna informationsflödet på bolaget. Sen är det klart att alla vi som sitter inom det här som jag kallar cybersecurity och vi är 50 man i Sverige anställda inom det området. Alla de 50 personerna har ju ett eget intresse av att ha koll på det här, så det behövs ju inte någon utbildning av företaget om vi säger så.

19. TB
I det här med de introkurserna där, vilket format är de, är de digitala eller i fysiskt eller?

20. R4
Ja det är möten. Det finns ju skrivna dokument så klart då. Men IT chefen har en timmes genomgång, HR-chefen har en timmes genomgång. Så det är lite de i direkt närhet då, som kör introduktionen. Men om det görs fysiskt eller om det görs via teams eller så det, det vet jag inte.

Jag utgår från att det blir i teams i och med att vi sitter både i Stockholm och Göteborg och Malmö och Köpenhamn och så jag tror inte det folk åker fram och tillbaks där.

21. TB
Nej just det. Har ni någon specifik anpassning där till distansarbete och utbildning. Då menar jag inte i form av om den utförs på distans eller så utan jag menar innehållet.

22. R4
Nej, det är inget specifikt för det.

23. TB
Har det varit någon utbildning, inte då introutbildning, utan kanske under själva anställning, som har varit anpassad till distansarbete?

24. R4
Nej, det har vi inte haft något. Vi har vuxit in under de här 2 pandemi åren så har väl folk lärt sig hur man jobbar hemifrån. Men det har inte varit någon ordnad utbildning så att säga. Det har inte varit så att företag har talat om för oss anställda: “vi vill att ni agerar på det här sättet.” Eller “när ni jobbar remote vill vi att ni gör så här och så här.” Det är snarare tvärtom. Jag skulle nog mer säga att om kunderna har krav på oss, alltså vi som jobbar då med externa kunder. Då är det kunden som har rätt. Alltså om de om de har krav på hur vi ska jobba remote så efterlever vi kraven som kunderna har. Har det varit utbildningar i verksamhetens

policys? Det har vi väl det ingår i de här introduktionsutbildningarna i samband med anställning. Alltså där finns ett antal policys som ju rör hela bolaget då och där finns ju framför allt alltså det som om vi nu pratar informationssäkerhet så är det ju… Vad ska man kalla det för, end user guidelines? Alltså hur agerar man? Vad är det för information vi delar och när delar vi den? Vad ska man tänka på om du sitter på ett flygplan eller en flygplats? Du kanske inte ska sitta och titta om, om det är patent och varumärken något sånt där. Så länge det är under den registreringsprocessen så är det ju väldigt känsligt. Men i samband med att ett patent är registrerat eller ett varumärke är registrerat då är det nästan tvärtom. Då vill man att det ska bli publikt. För då får man ju sina royalties eller man kan ju ha den hanteringen, men innan det är ett godkänt så är det ju faktiskt mer känsligt. Och det är klart att de juristerna som sitter och jobbar med Ericsson och IKEA och Ericsson. De har ju nånting i storleksordningen på 30 % av sin omsättning bygger ju på royalties i samband med att de har patent och grejer. Alltså, det är ju en grym intäktskälla för de. Och det är klart att sitta och jobba med att registrera varumärken och patent för Ericsson. Då kanske inte ska sitta och skriva de dokumenten eller har de telefonsamtal när du sitter på en flygplats så den typen av information och briefing har vi. Men vi har inte jättemycket policys. Det är inte jättehårt. Det är väldigt individberoende. Man har stor tillit till sina anställda på det företaget jag jobbar på.

25. TB
Är det något som sker kontinuerligt?

26. R4
Nej, det skulle jag inte säga. Det är i samband med anställning. Det är en eller två aktiviteter per år som rör medvetande och ja, informationssäkerhetsrelaterade. Någon gång skickar de ut sådana här bluffmejl. Men vi har haft någon sån här du vet, hela företaget samlas i på Malmö live då 2 dagar och det är klart att då har man ju tutat det i agendan såklart att man har någon awareness training. Det är inte så att det tickar på var tredje månad.

27. TB
Hur ser ut med det att policy ska efterföljas då? Görs det någonting för att säkerställa att dessa policys följs?

28. R4
Nej, tyvärr inte. Däremot gör våra kunder gör det, det vill säga de jag jobbar med. Där tvingar dem att införa rutiner för att säkerställa att de målen man försöker definiera, vilket är svårt. Men på något sätt måste man ju försöka mäta framgång. Alltså gör vi det vi tror att vi gör. Men internt så vitt jag vet görs det inte. Vi som bolag är nog som de flesta bolagen, att om går in och om du hade haft access till vårat intranät, dessa policydokumenten, så är det säkert hälften daterade 2016 eller nåt sånt där. Du vet någon plockar fram de här policy dokumenten dag ett så innehållet stämmer förvisso. Även om du hade gjort en review så hade du kanske sagt att ja, det här håller det här är fortfarande bra, och du hade ju i alla fall kunnat uppdatera datumet även om innehållet hade varit samma. Men nej, jag tror inte det inträffar i vårt bolag då. Däremot jobbar man med det jag brukar kalla då bottoms up. Alltså skulle du prata med vår teknikavdelning och våran IT gäng de sitter ju ständigt och övervakar sårbarheter och

tekniska brister och kolla vad vi har på våra datorer så det sker ju en från en teknisk synvinkel så sker ju en konstant... De har ju koll på grejerna och de vet vad de gör. Men det, det är ju när man pratar policys, då brukar man ju säga tvärtom, du vill ju styra din verksamhet. Det är därför du skriver en policy så när teknik avdelningen sitter och utför sårbarhets tester och när de scannar nätet. Koll på intrång och så vidare, så vill man ju att det ska följa någon form av företags plan, men det gör det ju inte utan det bygger ju från tekniksidan. Så jag menar mycket, mycket utav det man skulle vilja ha bättre koll på ur ett styr governance perspektiv. Det görs ju, men det görs inte med styrning utan det görs baserat på teknik och funktionalitet. Jag vet inte om ni hänger med på den. Men det är skillnad på att styra verksamhet och på bottoms up. Då går du ner och snackar med teknikavdelningen så visar det sig att de gör jävligt mycket utav det som man tror du att de gör, men det är ingen som vet det går jag upp och prata med någon chef eller någon i ledningsgruppen och så och så frågar, har ni koll på eran IT säkerhet? Och då är ofta svaret, jag vet inte, du får gå och snacka med IT chefen. Då får man det svaret. Då sker ju inte det här på ett organiserat sätt och då tappar man mycket effekt.

29. TB
Men Albin du kan ju fortsätta där på nästa fråga.

30. AO
Hur arbetar ni med säkerhetskultur i samband med distansarbetet. Är det utmanande, isåfall hur?

31. R4
Nej, därför att och jag tror det är drivet av att det är så får ju incidenter alltså. Det är många som läser i tidningen, det händer saker, ransomware, GDPR böter till vissa företag. Det är alltså det är en del grejer som hamnade på löpsedlarna. Men jag kan ju ärligt säga att jag har jobbat i 35 år och jag har inte jobbat med ett enda företag där det har varit en incident som faktiskt har haft effekten av att påverka det här företagets överlevnad eller att det skulle ha på något sätt hotat dem. Dels så sällan som det händer sådana grejer, det gör att det även om man nu läser för att Maersk drabbades och torskar en miljard kronor eller vad fan det var eller när du läser att Malmö kommunala bostäder det är någon som har glömt en portfölj på en busshållplats och så vidare alltså. Det är ju inte så att. De är inte så att företagen går omkull. Även om man i en riskanalys skulle komma fram till att konsekvensen faktiskt skulle kunna bli det, så är det. Det är svårt att få gehör för det här av den enkla anledningen att det händer inte tillräckligt mycket grejer som får de konsekvenserna så att du faktiskt skulle börja jobba med det här. De som skulle drabbas stenhårt av den här typen, det är ju banker, det är ju försvaret, det är ju myndigheter. Men de har ju koll på det. Det är de som jobbar bra med det här. Men tittar du på sjukhus om du tittar på Trafikverket om du tittar på som jag sa bostads... Alltså Trelleborg ab. De tillverkar gummislangar. Alltså de har ingen drivkraft att jobba med informationssäkerhet eller med IT eller med social engineering. Jag menar man kan skicka dit någon som knackar på dörren och alltså även om det skulle hända någonting så skulle du inte få sådana konsekvenser att de tycker är värt att lägga pengar och resurser på att göra det säkert på något sätt. Jag menar det blir krig i Ukraina. Ja helt plötsligt så alla alla som har finansiella.

Grejer med Sovjet ja nu är de helt plötsligt drabbade. De hade ju kunnat göra det här som en del i sitt risk management. Jag menar, när det blå vad heter det drar en orkan i Bahamas, varför det? Det är alla brevlådeföretag som håller till i Bahamas. Vad får vad får det för konsekvenser så att? Försäkringsbranschen jobbar ju aktivt idag med att. De måste ta med dig riskerna visar att det enligt lag eller vad man nu skulle säga att ta hänsyn till vatten höjning till klimatförändringar till krig till politiska. Det är en del i deras kravlistor. Det fall det fanns inte för 15 år sedan. Så det, det händer ju grejer hela tiden, men.

32. AO
Ja kan bli spännande alltså. Okej. Hur arbetar ni med säkerställda? Contains av policys gällande säkerhetskultur kanske det till just mycket på det men.

33. R4
Ja och om du tittar på Jag läste i den här punkter som på era frågor pratar vi människor så sker det ingenting. Då görs det inget däremot om du tittar på teknik leveransen och det alltså vi har ju policys vi har. Förväntat beteende hos användare och rent tekniskt så övervakas ju det här utav det gänget som sitter då i Indien. De är 40 länder som har stenkoll på vårt nätverk. Vem gör vad och så vidare? Men det sker ingen det... Det är inte så att någon kontaktar mig om jag går in på atg.se och lägger in en v 75 rad. Det är ingen som säger till mig, det är inte otillåtet i våran policy att besöka sajter som inte är företagsrelaterade. För de ser ju det, de skulle kunna agera på det. Men där sker ju ingen övervakning på det sättet.

34. TB
Hur är det mer riskmedvetenhet där? Finns det utbildning eller andra sätt kring risker

35. R4
Ja, det är ju det ingår ju i grund introduktionskursen där alla signar på ett avtal där man skriver på att man har läst och förstått end user guidelines. Sen att folk inte följer end user guidelines är ju någonting annat då, men. Ja som sagt, de räknar nog som jag sa tidigare, det tror jag att det av 500 anställda så är ju trehundrafemtio högskoleutbildade. Det är inte under folk som står och langar hamburgare på McDonalds utan det och då jag men alltså det man kan skratta lite åt det. På McDonalds så har de ju stenhårda processer rutiner du gör så här 1, 2, 3 4 5 annars får du sparken. Det finns ju inte i ett sånt här bolag och det här påverkar naturligtvis också alla som till exempel jobbar med cyber security. De måste ju ha local admin på sina datorer för att kunna ladda ner och hämta hem de programmen som behövs för att göra sitt jobb. De går ut hos kunder och så någon gång ska ju ganska någon kod och någon gång ska man ju titta på hur man har byggt ut säkerhets bubblor på Linux plattform och sen nästa gång så är det ju någon utvecklingsmiljö och webbaserade på bilindustrin då alltså det måste ju hela tiden avpassas till när de ska förstå vad de ska kontrollera helt enkelt och då kan man ju inte sitta med en låst dator. Men det är klart så de här är ju största risken. Därför att de jobbar med det här. De letar ju efter ransomware. De letar ju efter buggar och det är klart att då är ju risken stor att de drabbas själva så där, men där skulle man då snarare ha separera så att de som jobbar inom cybers security de ska ha egna datorer. De ska inte ha [***]-datorer då till exempel. Det skulle ju vara ett enklare sätt att hantera det. Jag har jobbat på många olika

företag. Det är svårt att hitta någon som jobbar med informationssäkerhet eller IT säkerhet på ett strukturerat och bra sätt. Det går emot människans natur. Jag vet inte.

36. AO
Men vilken roll skulle säga att ledningen har? Vi har i denna aspekt.

37. R4
Ja, den är enormt viktig skulle jag om du frågar mig. Alla de företagen där jag driver ett arbete som får drivkraft och där det faktiskt händer någonting har ledningens stöd. Om ledningen säger att det här ska vi göra och så är det någon som får en budget och så säger man att nu har jag, nu har vi ett år på oss. Jag jobbar ju mycket med att implementera det de här... Det här tänket, kulturen alltså att förankra det i ett bolag och då är man ju inne i alla delarna och då finns det. Jag brukar kalla det för en design fast alltså att du behöver ha de här dokumenten på plats. Du måste plocka fram de här policybeskrivningarna och de måste ju naturligtvis tas fram av företagsledningen jag menar om någon som sitter på ett kontor i Falköping skriver ett direktiv där det står det här måste vi göra, då är det ingen som tar på det. Men om VDN skickar ut att det här om du inte gör det här, då får du sparken ja då, då lyssnar ju folk ju men... Att genomföra förändringarna designfasen är dokument då kan du göra en pärm precis som att du gör en budget finansiell plan. Du kan ha en marknadsplan vi ska bearbeta för de här marknaderna. Du kan ha en logistik plan, alltså så här vi är vi ett bolag som levererar prylar till ICA, då måste vi ha en bra logistik och transporter och så vidare och då förväntar man sig ofta också att ta fram den pärmen som beskriver hur ni jobbar med IT och information. Hur hanteras det? Ja, det finns ju inte. Om inte den finns på samma nivå som en affärsplan eller finansiell plan eller logistik, ja, då är det med svårt. Svårt att genomföra ett förändringsuppdrag. Precis som jag beskrev då att då får man gå ner och snacka med IT-snubbarna som oftast sitter i något källarplan på många bolag och de har skiTBra koll på det de gör. Men om man då frågar, har det här, finns det någon återkoppling? Alltså vet ni om det här hjälper företaget? Vet ni om att ni har byggt en alltså, den tar en sån här sak som backuper. Jag jobbar på ett outsourcing företag så de har 40 kunder med typ trettiotusen anställda sammanlagt och de tog betalt per gigabyte som backades. Alltså så här företaget hade 4TB data som backades så betalar de 300 000 kronor i månaden. För backup leveransen som då var byggd på gigabyte och så frågar jag kunden. Vet ni vad det är ni backar behöver ni backa 4 back och de har ingen aning. Och så går man igenom det och så tittar man på ja, då visar det sig att. 2TB det var ju privata MP3or MP4or. Det var ju videos och musik och bilder som de anställda hade tankat över från sina mobiltelefoner och sådär eller laddat hem via internet då. 300 000 spänn i månaden betalar de för att personer på företag hade laddat hem privata grejer. Då styrs det ju inte, då är det ju bara bottoms up. Det är någon som har installerat ett teknisk plattform för att ta backup, men det är ingen som talar om vad man ska backa eller varför man ska backa eller på vilket sätt då och det här. Det var det bästa med grejer GDPR. Det skapar ju attention. Det var ju det som var bra. Jag menar GDPR säger, det finns ju ingen jävel som kan hantera eller kontrollera personuppgifter på det sättet som den lagen och speciellt inte om man nu tittar på Facebook och Yahoo och Amazon och de som faktiskt var målen för. Men det skapar ju medvetande. Alla har ju sprungit här i 4 år för att ha koll på saker och ting så det var ju bra ju men.

38. AO
Men hur är det i den verksamhet de jobbar i? Känner att du har stöd från ledningen i säkerhetsaspekter eller informationssäkerhetsaspekter?

39. R4
Frågan är vad? Konkretisera lite.

40. AO
Ja men alltså i det i din verksamhet. Vilken roll ser du att ledningen har alltså. Får ni mycket stöd av dom?

41. R4
De som är chefer och i ledande positioner inom cyber security området, alltså de här indierna vi när jag säger lite löst, 50 stycken som jobbar med cyber security och så där då. Där finns det ju bra kunskap och där finns ju ett medvetande men inte om du tar ledningen.

42. R4
För bolaget som sådant alltså tar väl skulle jag säga här ekonomichef och vd och de som ansvarar för de här patent och varumärke för de har ju ingen koll på. På vad det innebär att jag jobbar med informationssäkerhet och det är de som borde sätta sig in och styra den verksamheten lite bättre och så.

43. AO
Ja, vill du gå vidare TB?

44. TB
Absolut, hur jobbar ni med rätt tillgänglighet, och obehindrad tillgänglig på data?

45. R4
Där tekniskt stöd finns, ja, vi jobbar med Office 365. Vi har också äldre, one drive och lite sånt och det sätts upp efter, vad ska man säga, efter specifikationer. Så är det någon som vill ha kontrollerad åtkomst, dom vill veta vem som gör vad det här med att kunna ladda hem dokument eller inte kunna ladda hem dokument, dela dokument eller inte dela och så vidare. Där finns stöd för det, men du måste veta om det. Alltså om jag ringer till en it-avdelning och säga nu ska jag gå in och jobba med den här biltillverkaren i Göteborg och då vill jag ha en sajt där jag kan dela dokument med någon som ingen annan kommer åt så finns det en lösning på det då. Då får jag det naturligtvis då där våran IT avdelningar, då kommer den ha tillgång, alltså de som är administratörer, de som sätter upp den här lösningen. De kommer ju ha tillgång till det också och det är väl där man det är väl där man ibland brister tycker jag rent tankemässigt. Alltså man litar på sin egen it-avdelning, men de är ju dom som har access till allting. Det är ju som den här outsourcing operatören. Tittar man på de som driftar 40 kunder med 4... Alltså de har ju tillgång till allt. Där har det ju den största risken jag menar, skulle jag vilja åsamka skada, då skulle jag ju gå och prata med de här outsourcing bolaget och försöka

fiska upp någon som sitter med databashatten på sig. Därför att där vet jag. Den personen kommer ju ha åtkomst till precis allt till de här 40 kunderna och så ge honom en miljon kronor och beställa du det man vill ha dem. Det är ju den enklaste vägen in. Men ur ett kundanseense, igen då, nu jobbar jag som konsult, så min fråga är ju nästan uteslutande till kunderna, hur vill ni att vi delar information? Vill ni sätta upp något system som ni hanterar och där vi delar information? Eller vill ni att jag ska skapa någonting och det vanligaste svaret, det är ju att kunderna har färdiga rutiner för. Hur man delar, bjuder in till domäner och så vidare, då så.

46. TB
Brukar tillhörigheten var begränsad då eller får du det du behöver eller hur funkar det?

47. R4
Nej, jag skulle säga jag får det behöver, men jag får ju ingenting annat, vilket du i någon mening skulle kunna säga att det är en begränsning för ofta sitter man ju och så får du ta del utav ja, säger 2 projektsajter och 100 dokument.

Men sen när man sitter i möten med kunder, då började de prata om någonting annat och så har ju inte jag en aning om vad det är då för att det har inte jag tillgång till och det ska jag inte ha tillgång till. Men de vet ju inte om det, alltså då jag sitter och pratar med då utan projektet som jag själv är med i. De har ju delat ut rättigheterna, så de vet ju vilka sajter jag kommer åt. Men sen när man då sitter och börjar jobba med verksamheten då den verksamheten den tror jag att man har access till allt och det har man inte så.

48. TB
Och det är ju lite digitala skydd kan man säga rättigheter och så där. Men hur är det med fysiska, jobbas det med skyddet mot fysiska attacker, alltså shoulder surfing, eller dumpster diving, eller såna här saker.

49. R4
Vet inte. Om vi pratar om vårt eget bolag så vet jag inte hur det sköts faktiskt.

50. TB
Har du fått instruering eller information om att göra saker på ett visst sätt?

51. R4
Jag har aldrig fått mer än att det för det starkaste skyddet jag har sett är att du måste ha en bricka. En anställningsbricka som bärs synligt och om du ser någon människa som inte har en sådan bricka då och som inte går tillsammans med någon som har en bricka då ska man ifrågasätta, så du ska alltid ltid . Men det är det starkaste skyddet då så.

52. TB
Och för det försvinner lite med distansarbetet där. Hur är det med att begränsa anställda i form av vilken plats om man sitter på caféer och sådana saker? Är det något som jobbas med?

53. R4
Inte mer än att om du sitter på publika ställen så finns det ju inskrivet i våra end user guidelines så att lite beroende på vad det är för information du hanterar det så kanske du ska fundera på om du sitter på ett café eller om du sitter på flygplanet eller om du sitter på bussen alltså. Vissa telefonsamtal kanske man inte ska ta på bussen. Men nej, det är ingen som kontrollerar eller följer upp. Det är inte så lätt.

54. TB
Så det formella på det planet är ju egentligen vid anställning i dessa end user guidelines, har jag fattat det korrekt då?

55. R4
Man förväntar sig att folk ska göra det. Det sker i samband med introduktion och utbildning i samband med anställning. Sen sker det inte mycket uppföljning på det.

56. TB
Nej just det. För hur länge har du jobbat på verksamheten nu då?

57. R4
Ja, i det här företaget har suttit i 3 år nu.

58. TB
Så efter det första tillfället så har inte gjorts så mycket uppdatering eller uppföljningar eller vidareutbildningen och så?

59. R4
Nej, men jag skulle mer koppla det till när det här indiska bolaget signades. Ja då skedde det ju en massa introduktion och utbildning och information om vad de jobbar med så som sagt, vi hade en sån här dag när alla samlades i Malmö under 2-3 dagar och så hade vi så här workshops och så vidare. Där var det väldigt mycket utbildning och information. Vi har ju haft det. Det finns månadsmöten på företaget som alla är inbjudna till där det någon gång per år, så sitter ju då. Våran CISO alltså vår informationssäkerhetsnubbe och pratar om när det har hänt någonting eller hur vi ska agera så det sker ju en kontinuitet, men det är ingen som är tvingad att gå på de här månadsmötena. Jag menar det, det är en gång per månad de spelas in. De finns tillgängliga, men det är ingen de är ingen som kontrollerar att alla har lyssnat eller att alla har gått på de här utbildningarna. Så ja, så det finns där och sker där. Men nej, det följs inte upp och det mäts inte så.

60. TB
Ja, jag förstår.

61. TB
Ja, jag tycker faktiskt som man på det tycker jag nästan att vi har fått med det mesta Albin, eller vad tycker du?

62. AO
Jag tycker det också.

63. TB
Men då tror jag att vi i alla fall rundar av all inspelningen här.

7.3.5 Uppföljningsintervju 1

Intervjuns längd
33 minuter, 11 sekunder

Datum och tid
14/5/22, 10:00

Förkortningar
AO = Albin Olsson
TB = Tarek Bermalm
R1 = Respondent 1

1. AO
Så där.

2. TB
Men jag kan ju ta första frågan här då vi undrar ifall ni har policys som är specifikt utformade för social engineering och eventuellt vid distansarbete då i så fall vilka?

3. R1
Men nej inte speciellt utformade för, men det är punkter i policyn, alltså i punktform så ingår de delarna. Nu ska vi se om vi ska säga rätt förresten i alla fall vad gäller remote-arbete den den är jag betydligt mer säker på. Ja.

4. TB
Och kan du utveckla den delen? Vid remote-arbete då, vad gäller där?

5. R1
Ja, men det är ju så att säga. Det är alltså policyn anger högsta nivån på ledningens målsättning med arbetet och det finns ju en möjlighet att alltså det är möjliggjort genom policyn att man ska kunna jobba hemma då. Det finns ju en del att ansvarsutpekande vad som gäller så att säga då, men det är uttryckta i målsättning kan man säga sen kommer ju regler som ligger under policy och det är där vi är mer i detaljerade och det och där finns ju regler för både social engineering och för för remote arbete och då handlar det mer om så att säga. Vad alltså är det mer i detalj vad man får göra och inte göra? Vilka typer av aktiviteter man kan ta sig till och inte så att.

6. TB
Säga då just det. Och då är de kanske i distansarbetet där i det saker som säkerhetsmässiga åtgärder eller kan det vara ergonomiska och miljö och trivsamhet och sånt?

7. R1

Ja, det är både och det. Är arbetsmiljö är en. Del men sen så är det säkerhetsmässiga, en annan del också då. Sen är det så att det här är ju reglerat med med dels policyn så har vi reglerna. Sen är det så vid distansavtal så har vi dessutom ett avtal som ska följas. Och just när det gäller just mot remote-arbete, det där distansavtal som som vi och det här regleras ytterligare så att säga vad som gäller och där kommer det med arbetsmiljö är en mycket mer också.

8. TB
Just det har ni kunnat möta och se vad dessa social engineering eller distansarbete, dessa policys vad det ger för effekt?

9. R1
Jag, vi mäter absolut på hur hur det fungerar med remote access. Där mäter vi vilka som sitter hemma och vad de gör och så vidare så att det det har vi ju nyckeltal och KPIer på då.
Och social engineering gör vi inte kontinuerligt, utan det utsätter vi ju dem för tester helt enkelt ja. Och vet inte hur mycket kan gå in på det, men vill testa så är det alltså phishing och den typen av av angrepp då.

10. TB
Har ni kunnat se någon någon utveckling eller positiv effekt eller liknande?

11. R1
Men nej, jag törs inte svara riktigt på det för att jag har bara varit med om en operation så jag törs inte säga om det blivit bättre eller sämre och tyvärr är det så att jag har inte fått till det som har gjorts innan, och jag vet inte om det jämförbart heller, så att jag har bara sett en.

12. TB
Ja okej ja men vi går vidare till nästa fråga här då Albin, du kanske kan ta den.

13. AO
Yes hur, arbetar ni med att skydda er verksamhet mot social engineering-attacker vid distansarbete? Vad skulle ni säga utmaningar är i detta?

14. R1
Ja utmaningen är ju många, men alltså det det vi gör så att. Den som som vi arbetar med det så det. Det är ju väldigt mycket med utbildning. information. Och det är både så att säga introduktionsutbildning. Där ingår ju det som ett moment då, men sen så är det ju då löpande också då. Exempelvis när allt har utvecklats som det gjort, geopolitiskt, så är vi ganska intensiva med information på intranät och så vidare också. Och om riskhöjningar och beakta det och var försiktiga med det nu senast gick ut med och pekade ut [***] utbildningspaket för källkritik för det eftersom vi mycket påverkanskampanjer nu tror jag. Så nyttjar vi ju att andra [***] erbjuder saker också så vi behöver inte göra alla paket själva, utan då pekar vi ut att ni som har de här tjänsterna ni ska gå och [***] utbildning i källkritik tycker vi. Så att det är så vi jobbar och sista biten är ju mätningen egentligen då i den då, alltså när vi haft en mätning

och fått en resultat och då är det redovisade ju och det blir ju lite inlindat och för de här mätningarna går vi inte ut med till de anställda rakt av så att säga.

15. AO
Men hur anser ni att distansarbete påverkar i ett arbete mot social engineering?

16. R1
Jag tror inte det påverkar jättemycket i och med att man sitter hemma och gör samma saker där vi inte kan och det är väl lite oroliga. För naturligtvis de inte kan veta, det är ju det faktiskt ser ut i hemmamiljön. Vi vet ju inte om om någon sitter i rövarhåla och jobbar över det hur ser det ut hemma hos folk? Det just den pusselbiten saknas, det kan man säga det jag menar där vet vi hur det ser ut hemma på riksdag. Där det ser ut som det gör, jag menar. Vi då har. Vi kontroll över den fysiska miljön hemma hos folk kan ju folk springa fram och tillbaka även om vi liksom. Ja vi poängterar ju absolut hur miljön ska se ut då, men det vi vet ju. Inte och vi har ju inga metoder att gå hem till folk heller. Vi har ju inte dem den rätten helt enkelt.

17. TB
Har ni någon någon approach för att jobba kring det där och har gjort något för att hantera det?

18. R1
Nej, alltså det. Det vi har gjort är att när det gäller vad man kan göra hemma och inte så har vi skurit in på på en hel del saker det. Det är ju långt ifrån allting du får göra hemma och sen så det är ännu strängare i att det är ännu längre ifrån vår kan göra hemma. Det är en hel del som är spärrat helt enkelt. Du kan inte köra över remote. Och vilka servrar? Jag ska inte gå in på dem, men det är det som är vår mest känsliga verksamheter. Det kan du helt enkelt inte komma åt hemifrån eller ens utanför [***].

19. TB
Ja, ja, jag tror nästa fråga här då är. Vilka är de största utmaningarna i att skydda er mot phishing attacker för gör vid distansarbete?

20. R1
Ja alltså de största utmaningarna är att rent allmänt med phishing attacker är att de blir ju mer och mer sofistikerade det och man trodde väl, höll jag på att säga, det kanske man faktiskt inte gjorde, men det har kanske funnits någon bild att vi utbildar oss och sen så vi på något sätt rusta det.
Men jag tror inte du vill bli det utan... Vi måste hela tiden hänga med här och kanske utbilda oss och se bortom att. Och jag menar, det finns ju många nya tekniker som kommer också. Det är inte bara den gamla Nigeria-breven. Det kommer ju jag menar AI kommer ju spela in i det här också med fake videos och såna här saker. Och kanske plötsligt blir så att [***] dyker upp på i ett videosamtal om man luras och tro att det är han och så där jag menar. Men det, jag vet inte hur långt bort som kan ligga, men jag menar det. Det ligger definitivt i kortens riktning. Det är ju bara att kolla på den här Tom Cruise-videon för 2 år sedan eller vad det var.

Det var ganska övertygande. Utan att det var han? Då så att det där ligger på något sätt och gnager att det där kommer ju förr eller senare.

21. TB
Vad gör ni för att hantera de de utmaningar du nämnde där att de kan vara sofistikerade?

22. R1
Men alltså vi följer utvecklingen. Det gör vi absolut väldigt noga. Sen vet inte jag om vi har alla motmedel idag för det som komma skall det. Det skulle jag nog svara nej på att. Nej, det har vi inte, för vi vet inte riktigt hur det kommer att se ut och vilka motståndare. Vi kan skaffa oss heller, då? Sen har vi ju alltså. Vi är inte ensamma. Heller utan vi sitter ju ganska många, branschforum vi har köper externa intelligens och såna saker så att vi har definitivt en omvärldsbevakning. Den har vi.

23. AO
Bara med intelligens, vad syftas på där lite?

24. R1
Ja, det är ganska ofta som de här SOC-servicarna, Security Operations Center. Det är ofta externa parter, de där kan man ju ge dem i uppdrag att titta på våran risk-posture och titta på vad som händer på marknaden och det kan man köpa intelligence om vad som försiggår på darknet eller i andra kanaler också då. Och det gör vi och det gör ganska många faktiskt. Man köper den från sin SOC helt enkelt. Och det är ett gäng företag i Sverige som kan göra sånt här. Det är center och combitech och det truesec och några till då som är lite kända för det här då. Och då får vi en rapport helt enkelt som är custom made för oss då. Dels får vi generella delar i den också. Men sen tittar de på vad ser de som störst risker eller vad störst förekomsten av saker och ting mot mot just oss då.

25. TB
Jag tar nästa fråga här då? Vad är anställdas förhållningssätt till risker vid risker med social engineering, distansarbete? Vad är upplevelsen till det, inställningen?

26. R1
Jag tycker och det bygger både på på fakta, men också på känsla faktiskt. Jag tycker att de är mogna det stora flertalet. Det är väldigt mogna i vår verksamhet. Vi har ju. Förutom att vi har det var det surrat på en marknad så har vi också [***]. Vi är [***] och vi har ett gäng [***] som är ganska stränga som gör att medarbetarna blir väl utbildade i säkerhet rent allmänt då. Så jag tycker de är ganska kritiska och det visar även våra tester att ja, de är ganska kritiska. Men men ja, det stora flertalet det räcker att det är en där.

27. TB
Ja just det, vad är det som det lett till det, skulle ni säga, att det finns en högre mognadsgrad?

28. AO

Så att ja.

29. R1
Nej, men det är så, så är de här mätningarna. Vi kan väl se som sagt nu som jag sa nu har inte jag kunnat följa jag inte kunna. Fullgöra utvecklat sig. På [***], men däremot vet jag hur det ser ut på många andra platser så att jag menar vi har. Vi har viss benchmarking. Att vi är bättre än andra så att säga, men återigen, det hjälper ju föga om om säg att du har 10% som är fortfarande som vi bedömer lite omogna då? Det tog ju bara en siffra, något sätt skulle vara så ändå 10% så att det duger ändå inte riktigt. Men det är alltid sämre säkerhet. Man spelar lite grann med med lök principer att ja då har man liksom. Människan är en del och sen så kommer tekniken in och även tekniken och i olika skikt. Jag menar, vi tittar ju på olika. Vi har ju olika tekniska skydd, naturligtvis också då vi har det är brandväggar, vi har det i praxis och vi. Har det i. Ja på på många olika platser i nätverk och på på end point och så också då så att så man hoppas ju på att vi ändå har en helhet som håller ihop och som skyddar oss väl då.

30. AO
Okej

31. TB
Ja spännande.

32. AO
Bara en snabb fråga. Hur ser det ut med tid? För vi har några kvar och vi ser att det är knappt här.

33. R1
Men det är inga problem. Vi kör så länge de blir.

34. AO
Tack så mycket.

35. TB
Ja stort tack. Ja, jag kan ta följdfråga till den, man kan ju du ta nästa huvudfråga där. Jag undrade i att skapa den här medvetenheten och insikten i risker vid distansarbete. Vad är utmaningarna i det? Vad är problematiken?

36. R1
Alltså det. Det är en utbildningssaktivitet och man ska inte bara att man ska inte underskatta det det. Att det det här handlar om om lärande och det är en del i mitt jobb för visst, så du menar att det är vi ändå? Det är en sak att form av säkerhet i tillsammans med tekniker och så vidare, men här skulle det vara möta alla användare och i en utbildningssituation ska man ju. Då ska man nog göra sig vinn om att vara lite professionell pedagog också. För det är inte bara säga det här och sen tro att ja, men nu har ju alla fått det här och sen så är det klart utan det här. Det här måste ju verkligen läras ut och läras in hos samtliga.

37. TB
Är det på ett långsiktigt plan som kan som kan hjälpa där eller hur funkar det? Hur funkar det faktiskt lära in?

38. R1
Ja, men jag tror det sker på ett långsiktigt plan att man har en strategi för det så att det är lätt att bara bocka av och säga att ja, men jag har gått ut på intranätet och informerat om det här. Då är det klart. Men så ska ju ändå i mitt fall 150 pers förstått det här och förstått vad mitt budskap och allting då och det ska man ha varit ödmjuk inför hur man hur man tar ut till folk så att vi jobbar ju med lite olika metoder om jag visst jag går ut på intranätet och skjuter information ibland. Och om vi har lite flaggningar för hur viktigt det är och så. Där då. Men man kan inte bara jobba så, utan ibland måste man sätta in lektionssalar lära ut då där man har kontakt med med eleverna och kan på något sätt få en intryck av… Jag menar gå med ett budskap fram eller inte då, men det är lite olika beroende på budskapet. Har vi en phishing, Alltså har vi fick phishing-angrepp som träffar oss och vi vill gå ut på det här snabbt. Men då säger vi där på intranätet och och försöker trycka på att det här är faktiskt viktigt. Det händer just nu då. Men sen är det långsiktiga arbetet. Det handlar kanske mer om att hur utvecklar vi vårt kritiska tänkande och så? Här och ja då… Och då kanske… Man har en dialog med medarbetarna istället för monolog.

39. AO
Hur ofta har ni utbildningen?

40. R1
Inom, vi har ett gäng obligatoriska så att vi vi samlar gör personalen som har börjat på på [***]. Det gör vi 2 eller 3 gånger per år då. Och då är ju lektionssalen. Har det varit teams på under covid då men då annars så är det lektionssal då och då är det intro utbildning så att då får man en väldigt breda paletten vad gäller på den här [***]. Men vi har ju informationssäkerhet delar med där också. Där ingår ju remote och social engineering-bitar också förstås. Så att det det grundplåten och sen så sen har vi haft lite beroende på behov också. Vi har nyligen kört en kampanj på hanteringsregler, till exempel har ju hanteringsregler för alla vår all vår dokumentation. Då och då har vi känt för något halvår sedan jag kände att nej, men det här börjar börjar folk inte förstår det här eller om det kanske är för mycket nya människor som kommer med fel med uppfattning om hur hur vi jobbar på på just den punkten då, så då kör vi en kampanj. Då gick runt på alla avdelningar då vi 6 avdelningar så att då egentligen 6 avdelningar som vi gjorde på just hanteringsregler då.

41. TB
Hur funkar det då?

42. R1
Men det funkade bra. Såna saker gör ju inte jätteofta så att det jag tror ändå att då håller man intresset uppe lite grann då. Men det, det är inte en del i en strategi utan det kommer mer från

ett behov att det finns ja, men här behövs det så att strategier är en sak. Men sen får man ja anpassa sig vid behov helt enkelt. Vi har haft samma sak med mot arbete tidigare i covid till exempel. Att nu sitter folk hemma, de behöver de ha utbildning så har vi kört utbildningar.

43. TB
För säkerheten alltså?

44. R1
Ja precis ja ja, det har varit en kombo till det varit både användbarhet och säkerhet då.

45. TB
Ja ska vi gå vidare till nästa då… Ja hur väl insatta är det ledningen i social engineering.

46. R1
De är nog ungefär lika insatta som medarbetarna, skulle jag säga i att identifiera och förstå vad det handlar om. Sen får ju ledningen lite mera, då får ju lite mer statistik och vi har ju en lite annan dialog med dem också, för de har ju ett ansvar som de ändå måste uppfylla att förstå saker och ting runt cybersäkerhet så att. Dom var väl snäppet mer upplysta av oss så att säga sen som användare skulle jag säga att de är ungefär som snittet användaren.

47. TB
Skulle du säga att det finns ett ledningsstöd för skyddet mot resursanvändning?

48. R1
Alltså, vi har ett ledningssystem för informationssäkerhet. Det har vi och den bygger på ISO-27000. Så att och den den har använder vi rakt av så att den den är ju som standard, så att säga. Men den är ju till för bara att styra arbetet kan man säga och se vad man lägger i arbetet det det är ju ja. Är lite annat då, men den styr de mäter så det.

49. TB
Är bara förtydliga att fråga här är typ som som sägs och vilken sitter du i ledningsgruppen eller vilken hur ser det ut där?

50. R1
Ja nej, jag sitter i den extended vad heter den den större ledningsgruppen vi har. Vi har en kärna något sen så har vi en yttre ring runt den så att säga då, så att när när det är extended. Så så sitter jag i den. Yes, ja.

51. AO
Tycker du att det skulle du föredra att att sitta i kärnan?

52. R1
Nej, det behövs inte därför att om om någonting blir akut då kommer jag in till kärnan på nolltid så att det och så har vi gjort att exempelvis det där när det här bröt ut nu österut då så

så ville folk ha mig där helt enkelt direkt då så att och jag har full access till så att jag vill komma dit så kommer jag dit då? Så får vi hantera det där med lite. Med lite omdöme då. Jag kan inte springa dit med vad som helst men eller allvar då kommer dit.

53. TB
Jag undrar också förut, så pratade vi om ledningsstöd. Och det är det sätt att ett system, liksom. Men hur är det med förhållningssättet eller eller inställningen eller medvetenheten? Finns det, hur upplever du att det ser ut i ledningen? Till social engineering, alltså?

54. R1
Nä men alltså. De träffas ju precis som alla andra användare av något spam mejl då och då och så där så att de hålls. De ibland så blir det ledningen. Ibland sitter ledningen ganska isolerad från från verkligheten, men här gör man inte det, utan det här träffas man av samma saker som alla andra, så att de är noga just den frågan, så jag skulle nog säga att de är ganska… Jo, men de var medvetna där de absolut. Jag hade något exempel för ett par 3 veckor sedan då jag just en ledningsperson drog in mig i ett rum och visa det på att ja. Men kolla. Här har jag fått saker och ting, så att det jag. Vet att det händer. Då det träffar de också?

55. TB
Hur skulle du säga att distansarbetet här? Då skulle du säga att jag också har en roll eller mindre känt, eller hur ligger det till?

56. R1
Nej, men det är lika känt skulle jag säga ja till. Det är till och med så att ledningen är nog. Dom har traditionellt sett varit mer ute och rört på sig än kanske de anställda så att de har större. De är i alla fall används emot arbete mycket mera än än andra. De är ofta ute på tjänsteresor och de är ute och föreläser mycket så att vi har en ganska speciell ledning i och med att det är en direktion då. Så de är ute mycket och rör på sig så att de har verkligen. De har mycket emot arbete i sin vardag så de vet vad det handlar om, så så här.

57. TB
Ska vi se vad vi vill ta härnäst. Ja, jag tar denna då från ett proaktivt perspektiv. Hur jobbar ni med att mitt mitigera eller mildra eller lindra skadan av en social engineering-attack ifall det skulle ske?

58. R1
Om vi tänker på proaktivt. Alltså, det är många frågor, va delar i det beror på som den sociala näring skadan skulle resultera i men alltså all proaktiv. Allt proaktivt arbete vi gör, det är jag arbetar med med att se till att vi har skyddsnivåer på. På nätverkstrafik och på vår på alltså all analys på det som kommer in helt enkelt tillsammans med vissa skydd som det är ju parat med vissa skydd också då så att. Och mellan nuförtiden så är ju dagens hanteringssystem. Det är ju så mycket mer än bara antivirus utan det det ligger ju ofta liksom. Du, vad heter system och sånt här bubblat med med det här också så att det är många skyddsmekanismer i i de tekniska skydd som vi köper så är det ju och som jag var inne på tidigare vi lägger ju tekniska skydd i

olika lager också. Det är inte så att ett mail passerar en kontroll och kommer in till banken och sen så går det igenom eller inte, utan vi kontrollerar dig på många olika platser också. Vi har också en strategi att jag använde olika produkter på olika platser. Man har olika brandväggar om. Man har och. Yttre och inre. Zoner såna här saker så att. Det proaktiva arbetet det är svårt att svara på en fråga så där, men får mera blir det resonemanget att vi i gör det på många olika platser och återigen lök principen gäller. Man kontrollerar på många platser om man man lägger många olika lager helt enkelt.

59. TB
Vad gör ni då? För att om det skulle ske, vad gör ni för att lindra just skadan den skadliga effekten?

60. R1
Ja nej, men alltså beroende på vad som händer. Det är lite olika om det kommer in ett social engineering-mail som vill få oss att betala ut pengar så den sak kommer resursplanering medel som vill få oss att installera ransomware-programvara så är det en annan så att det är. Lite olika beroende på. Vad som träffar oss så att säga idag.

61. TB
Ett vanligt scenario kan ju vara att uppgifter och lägger ut eller om än att den anställda tappat sina uppgifter så att säga. Och vad gör man då?

62. R1
Ja precis. Ja, det kan ju vara ett social engineering-email som vill få som vi lurar anställda att lämna ut uppgifter och. Ja, jag har. Jag har heller inga färdiga recept där. Däremot så skyddar vi informationen. Det är en proaktiv att delarna som vi skyddar informationen på olika sätt då så att all alltså den den känsliga informationen ligger inte så tillgängligt så som på många andra platser en sak som man kan svara på direkt. Det är att vi har ju också via policy så har vi ju rätten och det har ju många arbetsgivare. Vi har ju rätten att övervaka personalen, vilket vi uttrycker i policyn och det där har ju en. Sak som man arbetar ut med arbetsgivareorganisation, arbetsgivare, organis. Personer och arbetstagarorganisationer också. Man har inte transparens i att arbetstagarna är ju faktiskt övervakad, vilket ger så att säga är en proaktiv aktivitet. Att, ja, de vet att jag kan inte göra vad som helst, för då kan jag bli avslöjad och så vidare då så att. Och på samma sätt är det ju så att nu så sitter inte vi och titta på vad medarbetarna gör för det också liksom. Det har också styrt upp i de här policyn att vi det krävs en hel del för de-facto faktiskt titta på vad vi kan göra då. Men, men vi brottsmisstanke eller någonting. Sånt här händer ja, men då har vi ju forensik och gå in och gå in och titta i loggarna helt enkelt vara helt. Försvann den här informationen. Ja, men vilken medarbetare har knyckt den helt enkelt? Så att då är vi ju med, då ger jag efter arbetet.

63. TB
Det kan ju ofta vara en bara en tidspress på sånt här också. Om någonting har hänt speciellt vi kanske runt ransomware eller liknande saker. Är det någonting ni tagit i beräkning?

64. R1
Ja, ja absolut, det har vi och där har vi jobbat med våra förmågor att att. Att bli snabbare, och jag nämnde det. Tidigare den här externa SOCen och vi köper ju SOC tjänster, inte bara för intelligens utan vi köper också för respons. Så att vi har 24/7 på att kunna få respons aktiviteter också på väldigt kort varsel.

65. TB
Är, det är responsen mer utmanande på något sätt vid distansarbete?

66. R1
Nej, det skulle jag inte säga, men det beror nog. På hur vi har byggt upp det att vi. Jag ska inte säga att responsen påverkas av distansarbete utan vi är där är vi nog lika snabba skulle jag säga. Men vi behöver inte gå ut fysiskt till medarbetarna.

67. AO
Ja nej men alltså alla som jobbar med.

68. TB
Och hur är det med säkerhetskultur i hantering eller respons eller mitigering av ett intrång ifall det har skett? Säkerhetskultur, hur skulle du säga att det funkar här?

69. R1
Den här typen. Av incidenthantering och så där de de är ju de är dedikerade till.
Det så att. Säga så. De vet mycket väl om om vilka krav det är på integritet och på att man inte. Att man inte förstör bevis och sådana här saker så att det jag skulle säga att där är mognaden hög. Men det är för att det är professionella. Som jobbar med eller helt enkelt? Det de jobbar bara med med de delarna.

70. AO
Men hur är det med den vanliga anställda som inte är informationssäkerhetsarbetande?

71. R1
Ja, men de alltså i incidenter och så där. Då är de ganska handfallna skulle jag säga. Men de får hjälpen. Det är därför vi har vårt incidenter response team då. Men den vanliga användaren vid incidenter dem är nog inte särskilt alltså. De vet vad de ska göra det till att börja med, för det har de ju fått instruktioner om att vi vid konstigheter så ja, då kopplar man loss från nätverket, man låter datorn vara och så vidare. Sen gör man ingenting, men det är. det tar slut där. Och sen kommer vi åt responstid helt enkelt så att ja.

72. TB
Skulle du säga att det är med… Ska tänka här hur man vill formulera den här frågan. Alltså säkerhetskultur kan ju ha liksom, men om det finns en bättre säkerhetskultur så kanske man kan rapportera saker snabbare eller sådana effekter hos den man som medarbetare att det finns

större acceptans eller liknande saker har ni är det såna grejer? Är det något som ni tagit i beaktning?

73. R1
Just det här med transparens är ju alltid någonting man funderar på för det. Det funderar jag på. Jag tittar ju alltid på vilka incidenter som ramlar in då, men så kommer jag alltid frågan, ja, har vi några? Grå nån gråzon då? Vad är det som inte Kommer in och. Så vidare. Och jag tror att. Min känsla för rapporteringsviljan är att att alla vill rapportera och vi har inga såna här. Jag upplever inte att vi har några såna här jobbiga skuldbeläggande utan folk. Det är ganska högt i. Tak där vi. Springer tillbaka direkt att dra in lönen för dem bara för att den rapporterande incident om de skulle råka klanta att säga det finns en viss acceptans.
Det tar vi med oss som en utbildande sak då. Däremot tror jag det kan finnas dels att folk inte känner till att de måste rapportera. Det ska dom känna till, men det finns någon som kanske inte gör det eller de som helt. Enkelt är lata. Som struntar i de orkar inte rapportera, kanske inte hinner, så ska det vara också. Och de är ju, det är ju ett bekymmer, det är.
Alltid däremot tror jag att det det är nog mindre alltså mindre signifikanta incidenter som slinker igenom den vägen. Därför att dom större dom känner vi till på andra sätt än bara rapporteringen säger att vi har något någon stor störning i våra kärnsystem. Då vet vi om det så förväntar oss en incident och om det här inte kommer då det illa. Men den kommer nästan alltid så att. De större fångar vi helt enkelt, det är det vet vi.

74. TB
Men för hur är det med de här mest säkerhetskulturella frågorna, vid distansarbete kan det ju te sig lite annorlunda med vad man ens har möjligheter att etablera säkerhetskultur till exempel? Vilken roll skulle du säga att det har i mitigeringsaspekten?

75. R1
Ja, men det har nog ganska stor roll och man kan ju ta covid som exempel, för där har vi faktiskt haft ganska många medarbetare som har börjat till banken under covid tiden som alltså inte har traditionen av att sitta fysiskt på plats för när du är fysiskt på plats, då får du ju visst kultur genom väggarna. Eller bara umgänget med människor. Vi kan få apparaten och så där, men många har börjat, inklusive jag själv börjar faktiskt under covid och då ja, då kommer man in för en dags introduktion. Sen åker man hem igen och sen sitter man hemma ett år och där tror jag nog att förlorat en del. På det faktum att att folk inte har haft fysisk kontakt med sin arbetsplats.

76. AO
Okej.

77. R1
Jag törs inte säga hur mycket jag törs inte säga hur. Mycket, men jag är övertygad om.
Och jag tror många har spekulerat i. Jag spekulerar i. Det är ju i alla fall när vi pratar om det här. Att vi alltså de som har börjat under covid de har ju fått en sämre känsla för sin arbetsplats och i rent allmänna termer och det kan ju vara alltså rena utbildningsfrågor också.

Det, det har inte. Det har inte bara säkerhetsmässiga aspekter utan det det diskuterar vi medarbetarskapet. Hur ska vi få ihop familjen också då? Och det är ju säkert delar med en sak då. Det har ju drivits projektet runt det här i banken så att jag menar medvetenheten om om att det här att det är på det här viset blir ganska hög.
Vi har haft någon sån här framtidens arbetsplatsprojekt och så där då så att det vi tittar lite grann bortom covid. Hur ska vår hybrid miljö se ut, hur ska vi jobba hemma och på jobbet och så där så att det det har kommit mera från arbetsmiljöhåll så att säga och arbetskultur rent generellt då med säkerhet har ju varit en del. Och jag har ingått i det här projektet där.

78. TB
Det är något som kommer få i och med att det verkar som att distansarbete i någon utsträckning kommer finnas kvar. Är det något som tror får en större roll i framtiden?

79. R1
Ja, jag är helt övertygad om det. Det här är en arbetsmarknads fråga också att vara attraktiv arbetsgivare och så där. Man kan inte bara säga nej till allting och. Sen säger. Jag att nu nu. Nu är vi lite säkrare så att säga, utan vi måste ju. Hantera det här på något sätt? Sen har vi fortfarande vi som sagt, vi har strukits skyddslag så att det finns faktiskt en hel del vi inte få göra hemma så att men det får vi hantera på något sätt. Så att det. Genom genom ja hur vår organisation ser ut och hur vi jobbar helt enkelt. Det går att göra ganska mycket med arbetssätten också.

80. TB
Vad säger Albin ska vi ta de sista frågorna kanske?

81. AO
Ta den sista frågan ja.

82. TB
Vad skulle du säga det största problemet eller utmaningen i mitigering av att alltså att lindra skada när det har skett?

83. R1
Ja alltså, det är ju att fortfarande har vi en tidskritisk verksamhet så vi måste ju. Vi måste ju alltid fungera så att och det är klart får ett intrång, då kommer det gå åt resurser till intrånget, men de får ju inte. Man måste ju fortsätta med sin ordinarie verksamhet också, så att säga. Så att vi och vi är ganska slimmade som organisation så att det blir ju väldigt ansträngt. Det blir det och inte bara vid intrånget då utanför det kan man också tänka sig att visst du kan få ett intrång. Du kanske hanterar det, men det sliter ju samtidigt ganska hårt på.
Personalen då? Och frågan är bortom det intrånget på, alltså när man kanske har klarat av det klarar man av ett till då det är lite långsiktighet i säkerheten också. Och den kan alltid vara äventyrad om man så att säga är hårt slimmad som organisationer då.

84. TB

Får jag bara be dig kort, med en mening eller så utveckla vad du menar med tidskritisk där?

85. R1
Nej, men vi, vi måste ju vara uppe helt enkelt så. Vi, vi är en aktör på finansmarknaden så att folk förväntar sig att [***] svarar med våra finansiella tjänster. När det behövs.
Helt enkelt så att och då är tidskritisk i den meningen att vi vi måste ju kunna göra våra marknadsaktiviteter där när när vi förväntas göra dem helt enkelt.

86. TB
Ja, men då tror jag nog faktiskt, vi har fått alla frågor och. Lite till egentligen.

87. R1
Ja men vad bra. Det som sagt, det var tråkigt att det blev som det blev igår, så att det var bra att det i alla fall blev av idag

88. AO
Jag pausar eller stänger av inspelningen här, ja.

7.3.6 Uppföljningsintervju 2

Intervjuns längd
17 minuter, 57 sekunder

Datum och tid
11/5/22, 08:10

Förkortningar
AO = Albin Olsson
TB = Tarek Bermalm
R2 = Respondent 2

1. TB
Jo, vi kommer spela in mötet godkänner du det.

2. R2
Ja, det gör jag.

3. TB
Och då gäller samma saker som sist, att vi kommer ta bort efter 30 dagar och deltagandet är frivilligt och du kan när som helst också återkalla ditt deltagande. Och du kommer få tillgång till transkriberingen, så ifall det något som du tycker inte stämmer så kan det korrigeras.

4. AO
Och vi analyserar namn och verksamhet just det.

5. TB
Ja tack. Men, då tar jag första frågan här då i ja. Vi undrar om ni har några policys som är specifikt utformade för social engineering och eventuellt vid distansarbete då. Och då är en följdfråga, varför inte.

6. R2
De sluts upp i andra policys. Så att vi har vi redan rätt så rigida policy sig om vad man får göra och inte och sätta en policy just för social engineering, vad ska man säga, var inte dum. Det är en väldigt svår policy att sätta. Det finns till exempel inget [xxx] framework som säger du ska ha en social engineering policy. Det är en helt annan sak när man snackar: du ska access network, alltså. De andra policys är väldigt tydliga klara. Social engineering handlar väldigt mycket om medvetenhet istället.

7. TB
Så har ni policy som är mer utformad enligt medvetenhet och liknande saker.

8. R2

Den är utformad efter att man behöver ta vissa träningar. Ja. så att man behöver ta träningar, alltså att man tar träningar inom awareness att man tar.

9. TB
Okej.

10. R2
Sen kan man arbeta, men när jag ska ta typ en säkerhet hur man får bete sig både på nätet och på kontoret, vad som är tillåtet och inte.

11. TB
Okej, hur arbetar ni med att skydda er verksamhet mot social engineering i distansarbete.

12. R2
Det är awareness mycket. Det handlar om. Det hade en testat, jag tror vi gick in på det förra gången. Vi har även gjort tester där vi sätter dit eller där vi testar, går folk på det.
Nu jag är främst är det träning och att lyfta när vi har haft problem, till exempel när vi har personer som kommer in alltså, fysiskt på platser. Så förklarar vi vad som har hänt, att det har hänt och vad man inte ska göra i framtiden för resten av coworkers som är på den platsen.

13. TB
Just det. Har ni kunnat se vilken effekt awareness träning har haft.

14. R2
Ja, det är. det är svårt att säga, för jag har sett det man kan säga att.
När det får inte säga inte vänta… Man kan säga att det finns både litteratur som stöttar det och vi som arbetar inom säkerhet har sett att awareness är en av de mest effektiva sätten att förhindra social engineering.

15. TB
Vad skulle du säga är det utmaningar i detta?

16. R2
Ett otroligt informationsflöde. Om man säger i hemma miljön så sitter man och man får mejl, man får slack, man får andra som ska till exempel klicka på. Och skulle man då utföra alltså utsättas för social engineering antingen via telefon, email eller liknande så är det lätt att man multitaskar så mycket. Att man inte identifierar de här riskfaktorerna. Det som man istället här ifrågasatt det vanliga fall. När man sitter i en hemma miljö, så tenderar till att bli lite mer multitasking som gör att man missar.

17. TB
Kan det vara en alltså… Det blir väl kanske en moteffekt mot awareness, så även om awareness finns så kan det bli att man inte gör det man kanske borde göra.

18. R2
Precis, det är definitivt för att jag, även om man då har gått igenom de här träningarna så glömmer man bort de här riskfaktorerna man ska titta efter eller den här de här frågetecknet man ska klargöra innan man klickar på någonting just för det stressas fram och de som ofta använder social engineering är ju oftast duktiga på att veta att man ska framkalla den här stressen. Man ska gärna säga att det är tidsbegränsat att det är alltså då vet jag precis när de ska få fram detta.

19. TB
Ja, vill du fortsätta Albin.

20. AO
Ja men anser ni att att era anställda, i verksamheten är medvetna om att distansarbete medför större risker för social engineering attacker.

21. R2
Det kan jag ju inte riktigt veta. Då gissar jag åt andra.

22. TB
Det är inget som ni, det är inget som ni kanske också har ni utbildat i de större riskerna till exempel.

23. R2
Vad menar du. Förlåt.

24. TB
Att man kan genomföra utbildningar till exempel där man redogör för att det kan vara större risker vid distansarbete. Är det något som funnits till exempel.

25. R2
Nej inte under pandemin, utan vi har redan de awareness training och liknande finns redan. Vi, jag nämnde zero Trust förra gången vi pratar just om det här att inget nätverk är säkert egentligen så oavsett om du sitter hemifrån eller om du sitter på företagsnätverket så behöver man ta vissa. Alltså, man måste ha en viss awareness redan där. Vilket gör att vi har inte behandlat det annorlunda. Det istället om man säger så om vi tar bort det från awareness biten. Vi har inte handlat behandlat det annorlunda. Vi har haft mycket av deras, men det hade vi haft ändå. Däremot har vi haft en annan detektion. Vi har varit mycket mer redo från säkerhet att svara på när problem uppstår för vi vet att antagligen kommer incidenterna öka av just social engineering

26. TB
Ledningen. Hur väl insatta är er ledning i social engineering och dess effekter.

27. R2

[***]

28. TB
[***]

29. R2
[***]

30. TB
[***]

31. R2
[***]

32. TB
Vi kan stryka det här.

33. R2
[***]

34. TB
[***]

35. R2
Okej då, så då kan vi gå tillbaka, vi stryker allting vi pratade om.

36. AO
Okej

37. R2
Jag skulle säga så här ledningen, detta uttalar jag mig som en enskild medarbetare och min uppfattning och jag tror att nej, det har inte varit största orosmolnen, att vi sätter anställda att jobba hemifrån. Och därför kommer ske mer social engineering. Jag tror istället större frågetecken som varit. Här, hur ser vi till att medarbetare har det bra I hemmet har alla. möjlighet att jobba hemifrån alltså har de ett skrivbord, har de nätverk, har de etcetera. Social engineering har nog hamnat väldigt långt ner på listan och det har inte varit någonting som har uppmärksammats.

38. TB
Då en följdfråga också. Finns det ledningsstöd för skyddet mot social engineering?

39. R2
Ja, det finns det. Just nu så har det satsat väldigt mycket på cybersecurity har sett att under pandemin där många har fått strama åt budgetar eller liknande alltså ut alltså utanför vår verksamhet så har vi istället sett att vi har investerat mycket tid i att säkra upp vad vi har.

Så att vi har spenderat den tiden eller så kanske vissa saker har suttit på vänt under pandemin. Så att vi har istället jobbat på att säkra upp vår cyber security funktion.
Vilket för mig tyder på att vi har stöttning i social engineering, men de kanske inte sätter det specifikt till det utan de tittar mer på till exempel gartner och liknande som sagt att cyber threats är en av de största hoten för varje verksamhet. Och därmed har de då ger alltså gett oss möjlighet att börja jobba med contractions.

40. TB
Så skulle du säga då att ledningen är medveten om den ökade risken vid distansarbete?

41. R2
Nej, jag tror inte det handlar om distansarbetet. Det handlar om tiden just nu. Att det är alltså andra hot, det har inte varit, det är inte... Det har inte varit det som är på topp. Det finns mycket värre hot just nu, en del.

42. AO
Men då går vi vidare och tar den de sista frågorna här, bara från ett proaktivt perspektiv då. Hur arbetar ni med att mitigera alltså mildra eller lindra skada av en social engineering-attack. Ifall det skulle ske.

43. R2
Jo, jag försöker tänka hur, hur generell, hur vill ni ha det. Vill ni helst ha ett exempel eller hade ni velat ha generellt hur vi arbetar.

44. TB
Alltså exempel är ju bra om det kan ges om det kan ge sig och generellt helt okej. Håller du med Albin.

45. R2
Det är därifrån ett exempel. Ett exempel är att.
Vi får in någon som säger hej du, ja, du skulle klickat in dina eller vad heter det din emailadress och ditt password alltså [***]-identiteten de klickar skriver in allting, trycker “send” och plötsligt har de skickat ut sina inloggningsuppgifter. Oftast där har vi redan att vi detekterar sånt i våra mejlklienter där vi har en protection funktion så vi har sköter det via en detection funktionalitet och stoppar och har då en automatisk process som låser den personens account. Byter lösenord, och så är de uppe och rullar igen efter ett tag.
Vi kanske förlorat den personen förlorar en halv dags arbete, men samtidigt sprider sig inte det för oftast den spridning det har är ju att den fortsätter skicka ut det till alla den har mejlat och sen fortsätter den till alla den har mejlat och så vandrar runt hela företaget och och där har vi ju sett en mycket mer för bättre detection funktionalitet både inbyggt i verktyg vi använder, men även då vi har en detection avdelning. In-house. Som man om man då generaliserar det så handlar detta om att vi kör en detection funktionalitet som är väldigt stark. Vi kör playbooks, vilket betyder att när man identifierar det här mönstret har skett. Vi ser att normal användning på vårt nätverk eller via normal användning någonstans. Då kickar man igång en

playbook som säger. Låser accountet och så fortsättning. Det beror på lite beroende på om det är telefon, uppringning eller om du går in i byggnad också, men. Det sköts via en playbook. Vilket gör att det finns en process för att hantera olika sociala engeering-scenarion. Detta är ett rätt så använt sätt att göra detta på i branschen. Men för oss har det funkat väldigt bra.

46. AO
OK, skulle du säga att det blir svårare vid distansarbete. Alltså försöka arbeta med mitigering men du sa ju att det har fungerat.

47. R2
Nej, faktiskt det. Det tror jag nog inte spelar ingen roll. Jag tror att vid hemarbete och liknande. Det svåra är väl lite att det inte är på vårt nätverk, så vi har vi viss del av hur vi detekterade förr har försvunnit, för vi äger inte allas nätverk utan vi äger bara, alltså vår del av de inne på kontoret. Men det har gjort att jag fått vara lite kreativa. Och hitta andra sätt för att få den här detection funktionaliteten.

48. AO
Om vi går in lite mer på det mänskliga så skulle du ser ni att säkerhetskultur har en roll en mitigering och lindrandet, och isåfall hur?

49. R2
Det är väl också att de anmäler sig själva. Oftast så kanske… Nej, jag vill inte säga oftast, men man kan själv ibland inse. O shit skulle jag klickat här. Var detta fejk var detta någonting jag gjorde felaktigt. Skulle jag gett uppgiften på telefonen. Och att de rapporterar för vi får ju inte alla fall. Vi kanske alltså. Jag kan inte säga siffror, men vi får väl säga att vi fångar en majoritet. Men vi har ändå fall alltså dom här. Corner case, som vi inte identifierar. Vi har inte playbooks på dom. Dom kan ju identifieras om en användare har awareness och därmed rapporterar för att vi har ett rapporteringsverktyg som säger, har du utsatts för en säkerhetsläcka eller säkerhetsbreach. Och då kan du anmäla dig själv och där jobbar vi ju otroligt mycket med att få användare att förstå att detta är inte någonting…. Alltså… Detta är något som ska användas.

50. AO
Jag blir lite så här, när du sa playbooks, är det färdiga processer ni har för ifall det sker någonting.

51. R2
Precis vissa är automatiserade så vissa delar är skript, men vissa delar är också typ ring den här sätt igång det här flödet. Detta ska eskaleras liknande för vid till exempel. Det är också en lite annan får de access på ett admin account, då är det en högre säkerhetsbreach än om de tar en vanlig coworker. Nu ser jag här, jag har en minut kvar innan mitt andra möte, så om ni kan ta viktigaste frågan och liknande.

52. TB

Det är faktiskt sista frågan, så det passar bra. Ja, vad är ert största problem eller utmaning i mitigering av intrång. Vad är största utmaningen.

53. R2
Ingen aning, förlåt jag är helt fast i vad det skulle kunna vara...

54. AO
Nej det är lugnt.

55. R2
Men jag skulle tipsa det här med playbooks. Läs om det på nätet. Det är en otroligt häftig process eller hantering, det är där ni kan bygga upp väldigt mycket.

56. AO
Ja, men supersnällt, vi ska inte hålla er längre nu men en supersnällt att du ställer upp igen. Verkligen.

57. R2
Inga problem och är det någonting ni kan ju maila också så är det någonting jag frågar på, till exempel om ni fattas litteratur eller liknande på några frågor skicka.

58. AO
Just det.

59. R2
Ha det så bra, hejdå.

60. TB
Tack så jättemycket.

7.3.7 Uppföljningsintervju 3

Intervjuns längd
25 minuter, 25 sekunder

Datum och tid
14/5/22, 10:00

Förkortningar
AO = Albin Olsson
TB = Tarek Bermalm
R4 = Respondent 3

1. TB
Jag tittar första frågan här då. Nu ska vi se. Jo har ni policy som är specifikt utformade för social engineering och eventuellt vid distansarbete också då.

2. R3
Alltså man jag skulle säga så här när man skriver en policy så tar man ju hänsyn till att det finns social engineering och olika typer av tekniker. Inom social engineering-spektrat, kan man säga. Men jag skulle inte säga att vi har en speciell policy som adresserar det på det sättet utan myckets social engineering-grejerna hänger ihop med awareness. Alltså. Hur ser du till att medarbetarna är medvetna om det här. För det är ju mycket utbildning skulle jag säga så att jag skulle säga att det är det är mer utbildningsdelen än på policydelen här.

3. TB
Ja just det, men finns det... Hade du något mer att där..

4. R3
Nej nej men det. Jag tänkte säga var ju att det är klart att i vissa policy delar så att säga adresserar ut som man har saker. Alltså det här att man inte ska lämna ut information till vem som helst och sådana saker det. Det har vi ju lite luddigt beskrivet i policyn så att säga, det är ju standardgrejer att vi inte lämnar ut information till någon obehörig och så vidare.
Men sen så det var lite övriga, vilket delar inom social engineering och som vi vill pratar om, skulle jag säga. Men, det mesta adresseras genom antingen att att det delar av någon annan policy eller eller utbildning helt enkelt av medarbetare.

5. TB
Just det sen lägger större vikt vid utbildning för för att skydda mot just social engineering då.

6. R3
Ja sen är det också, så om man ska vara helt krass. Det är inte jättemånga medarbetare som ens läser policy, att att tro att bara för man skrivit 10 policys att det kommer att förändra någonting, det är ganska naivt så att.. policys i alla ära och det är jag använder policys

mycket. Det är för att stänga diskussioner. Jag använder det mycket som ett verktyg för att många gånger så kommer man säga, men kan vi inte göra så här. Och då och då tar jag fram på och säger nej, tyvärr eftersom management, vi har en policy här. Vi har gjort det så här, man har godkänt det. Har du problem ta upp det med management- Och då kan man stänga diskussionen och så och de flesta gångerna så blir det inte så mycket diskussion utan då. Då tystnar folk liksom, så det är mer så jag använder mina policys och sen givetvis så säger vi ju till våra anställda att de ska läsa dem och så vidare. Men vi vet ju av erfarenhet att det gör väldigt få personer. Läser alla policys.

7. TB
Skulle du säga att att era policys så är lättillgängliga, och nu menar jag inte att hitta dem utan mer innehållet.

8. R3
Ja, det tycker jag där vi försöker alltid skriva policys på ett sätt som gör att de går att läsa ganska lätt och så det finns ju företag som jobbar med policys på hundratrettio sidor. Vem kommer ta sig tid att läsa 100 sidor policy. Det finns inte. Det finns inte för det jag tycker desto kortare desto bättre skulle jag säga.

9. TB
Men du nämnde att ni med awareness jobbar med social engineering. Har ni mätt effekten av det, vilken påverkan det har?

10. R3
Ja vi gör det vi mäter är ju mycket. Det är svårt att mäta de andra, men det där är ju en sak som vi mäter. Det är ju hur många som klickar på phishing mail till exempel så vi skickar ut egna phishing, mejl och sen. Vilket jag faktiskt gjorde i år här till vår organisation och sen följer vi upp hur många som klickar i de mailen.

11. AO
Alright.

12. R3
Och sen låter man klickar, de får ju de får lite extra uppsträckning och då får dessutom extrakurser i förhållande till alla andra så att man får. Klickar man på saker som så blir man tyvärr tvungen att gå extra utbildningar så att det är så det funkar också.

13. AO
Yes ja, men då det går in lite på vår nästa fråga. Arbetar ni med att skydda er verksamhet mot social engineering attacker vid eller… Hur arbetar ni med att skydda er verksamhet mot social engineering-attacker vid distansarbete?

14. R3

Skulle säga att det inte är det skiljer sig inte jättemycket. Det möjligtvis den aspekten att när man sitter hemma kanske är det svårare att fråga någon om om någon ringer till en så om man är på kontoret så kanske man har lättare att höra. Men känner du det här och känner du till det här. Vet du det här. Ja man sitter ensam hemma så kanske man är mer mottaglig skulle jag säga, kanske eftersom man inte har några kollegor att fråga. Så ur det perspektivet tror jag kanske man är mer med mer tillgänglig mot attacker så att säga men men men nej. Alltså den utbildningen som vi utformar. Den är ju utformad så att. Säga är ju. I den är inte bunden till den lokation eller en fysisk plats på det sättet. Att så här, gör du kontoret och så här gör du hemma, utan det är ju generell utbildningen. Så här gör vi alltid .Så det är ingen skillnad på det kontoret eller hemma på det sättet, men det är klart att det är ju så att om du sitter hemma så kanske det är lite mer isolerad. Då kanske inte kollar upp saker på samma sätt eftersom det är svårt att få tag på en kollega och sådana saker så ur det perspektivet så så skulle det i teorin kunna finnas en ökad möjlighet att att folk som sitter hemma är mer mottagliga mot saker.

15. AO
Ja absolut. Ja, anser du att det som distansarbetet påverkar ert arbete mot social engineering?

16. R3
Nej inte jättemycket så. Det skulle jag inte säga, nej. Men för att för att de här teknikerna som man använder dem är ju så att säga applicerbara oavsett var man sitter. Det enda möjligtvis om man skulle kunna säga någonting, det är klart att ta sig in för ett kontor där folk sitter hemma och jobbar det kanske lättare för att det är mindre folk på kontoret. Men samtidigt är det också mindre folk som släpper in dig så att. Det går åt 2 håll där, men det är klart att om jag skulle jag skulle vara en sån under pandemitider så har jag. Så har det varit mycket mindre folk på kontoret och givetvis och det är klart det skulle jag då lyckas ta mig in på ett kontor så är det ju mindre personer som kommer ställa frågor. Till mig. Vad gör jag där. Men sen samtidigt, om det är mycket folk kom till kontoret så kanske det är lättare att komma in på ett kontor någonstans för att man bara hänger på att folk in. Så det är både och, skulle jag säga.

17. TB
Jag går vidare med nästa här då. Ja anser ni att alltså anställda i den verksamhet är medvetna om att distansarbete kan medföra större risker social engineering attacker är det något som ni som jobbat med kanske.

18. R3
Det skulle jag inte säga. Jag tror att medvetenheten sitter på ett annat ställe. Jag tror inte att den är förknippad med exakt var du jobbar. Utan att den sitter på det det på ett annat plan i huvudet att man tänker innan man gör saker. Man kanske inte ger ut information till folk som ringer till en och mailar, alltså det jag skulle säga att det är medvetenhet som är på ett annat plan än just vad man sitter och arbetar. Jag tror inte att jag tror att också, men man tänker idag att.
Förr i tiden skulle det vara mycket mer också att man skrev ut dokument och hade liggande på sitt skrivbord och så vidare. Och då är det ju en säkerhetsaspekt givetvis att det sitter man hemma så kanske man inte har samma säkerhet som fysiska säkerhet som man har på ett

kontor för att vi har större möjligheter att köpa kamerasystem och larm och allt sånt där är på ett kontor, men. Det är ju att det är väldigt lite utskrifter nu för tiden. Vi går mot en utveckling där vi inte skriver ut speciellt mycket längre på det sättet och då finns aldrig i datorn och då spelar det ingen roll vad du sitter på ur det. Perspektivet, skulle jag säga.

19. TB
Ja hur väl hur väl insatt är er ledning i social engineering.

20. R3
Det är de ganska väl insatta skulle jag säga. Det, de är också mer utsatta för saker så att de alltså. Vi har ju hela det här med man brukar ju kalla CEO fraud och CFO fraud så vidare. Då får ju väldigt mycket konstiga mejl och såna saker att de ska godkänna transaktioner och andra sådana saker och därför är det ju kanske lite mer på tårna skulle jag säga än gemene man i bolaget. För att dom är utsatta.

21. AO
Absolut, snart får jag bara. Sitter du i ledningsgruppen du som CISO. Tror du att det är ett problem, eller skulle det bli bättre om du satt i den gruppen också. Hur skulle detta påverka medvetenhet?

22. R3
Nej. Det gör jag inte inte. Det skulle bli bättre. Det är ju en utveckling vi ser inom många olika branscher att CISO flyttar in i ledningsgruppen och jag skulle säga att det beror lite på vad det är för typ av bolag också för att det beror lite på om det. Om den här säkerhetskulturen finns i bolaget så vill du nog ha CISOn i ledningsgruppen, men finns inte säkerhetskulturen i bolaget. Så tycker du inte att det är så viktigt, så det handlar nog om hur mogen man är som organisation och hur mycket man tycker att IT säkerhet… Hur viktigt det är för ens kärnverksamhet liksom.

23. TB
Just det får jag bara kolla med dig, [***], för vår del så har vi öppet schemat det är ingen stress från vår sida. Men vi har 2 huvudsakliga frågor. Ska du vidare till ett möte eller sådär?

24. R3
Nej, det är okej. Jag har nästa möte kl. 10 så.

25. TB
Ja, men jag var nyfiken på och följdfråga, för du nämnde att det skulle antagligen… Det skulle vara en bra sak att CISO satt i ledningsgruppen. Vad är det som saktar ner den processen. Den här ändringen.

26. R3
Ja, jag tror att det handlar om mognadsgraden i den nuvarande ledningsgruppen, att man förstår hur stort ett. Jag tror att många ledningsgrupper lever i en liten bubbla av att man inte

riktigt har varit med om ett större angrepp och jag tror att de om ni om ni skulle titta på bolag som har utsatts för större angrepp versus som inte har varit det, så skulle ni säkert se en trend där att CISOn tenderar nog mer att vara med i ledningsgruppen i ett bolag som har varit utsatt för någonting. För det hänger ihop, alltså det. Det här är ju liksom, om du sitter i ledningsgruppen eller inte det. Jag skulle säga att det är kanske inte det absolut viktigaste. Det viktigaste är att det finns pengar till området att allokera en budget och så vidare. Det är ju det absolut viktigaste sen om man sitter i ledningsgruppen is sig, så länge man har en god relation till ledningen så tror jag inte det är avgörande att man sitter med. Men det är klart att har man en dålig relation om du sitter utanför. Ja. Då kommer det förmodligen inte så prioriterat ditt område.

27. TB
Just det ja.

28. R3
Och det kommer också kraven. Det kan ju titta på man börjar titta på krav i amerikanska bolag, alltså typ, jag har läst det väldigt snabbt jag inte kan minnas den googla på det, men där börjar man införa ett krav om att du skulle ha man säger man ska ha lite säkerhets kompetens i en styrelse till exempel. Som anställer i bolagsstyrelserna eller som ett krav från jag tror det är. Nu vet du vad jag vet, men jag tror det s kan det vara SIC alltså amerikanska finans in. Inspektionen då som som har satt upp sådana regler. Jag vet inte om det gäller alla bolag, men det har kommit som ett förslag att man ska innan införa detta och detta kommer ju förstås ganska stora impact så att säga för det innebär då att du måste ha någon i din styrelse som har den här kompetensen och. Och det blir ju intressant att se vad det ska bli av dig, för det kommer ju verkligen tror jag när det blir regulatoriskt så att du måste ha någon så kan du inte längre bara så här vifta undan det växer upp.

29. TB
Ja, det är mycket drivmedel liksom.

30. R3
Okej, ja, det tror jag kommer att göra jättestor skillnad och det kan jag tänka mig. Att USA om man tittar man är väldigt såhär. Europa tittar ju många gånger på USA, så att jag tror inte Europa är långt efter med att tänka på det sättet. Jag tror i USA kanske är det lite längre fram här för de har varit utsatta och du vet, de har väldigt mycket. Det har varit mycket fokus på it säkerhet på ett annat sätt. Och då d. Det de är. Men om jag vet inte man märker när man. Jobbar med amerikanska inte säkerhetsstandard och så att det kan vara ganska tungt. Det kan vara såna här regler som att du ska. Ha ett staket. På en viss höjd då alltså att du ska ha visst antal kameror per kvadratmeter så de de de de går när man tagit säkerhetskoncept. Så det är lite speciellt, så jag tror att USA Europa kommer få hänga på det tror jag det är bara. En tidsfråga skulle jag säga.

31. AO
Men, tror du att det skakiga säkerhetsläget i Europa påskyndar det här.

32. R3
Ja, det gör de utan tvekan utan tvekan. Jag kan bara ta ett exempel från vårt bolag vår VD då han har ju suttit och pratat andra. Han har lite andra VD kompisar som han har någon slags nätverk med och de har väl pratat om ransomware, vad är det, i den här VD gruppen då. Om att det varit något bolag som varit drabbat och så. Så han kommer ju att fråga mig om de här grejerna, det vill säga, det är inte jag som driver och och slänger det i ansiktet på honom, utan nu är det han som kommer och frågar då. Det gör ju jättestor skillnad för det innebär ju att det har kommit upp på VDns agenda och det gör ju jättestor skillnad för plötsligt när det kommer upp på den nivån så får det fokus. Det får bli för pengar, du får tid och så vidare och sen. Det gör jättestor skillnad medvetenheten i ledningsgruppen skulle jag säga framförallt VD och skulle jag säga att man har VDn alltså VDn förstår det för att gör inte VDn DET så är det problematiskt, skulle jag säga.

33. TB
Ja, men då tar vi nästa fråga här då. Så från att proaktivt perspektiv hur jobbar ni med att mitigera eller då mildra eller förminska skadan av en social engineering-attack, ifall det skulle ske.

34. R3
Hur vi jobbar med att förminska skadan. Hm Okej… Ja, men det är ju det är jättemånga olika sätt, för det är det, det är ju. Det, det är lite det som vi jobbar i alla fall mycket med säkerhetslager att det inte. Det är inte ett system som ska detektera eller förhindra angrepp, utan du ska ha olika typer av system på olika lager som hjälper till att detektera angrepp och förhindra det. Jag tror på att det finns många säkerhetsleverantör pratar ju om att det man "köper ni bara vårt system så kan ni luta er tillbaka och dricka piña coladas" så funkar det ju inte. Det finns inte en lösning som löser alla hittills säkerhetsproblem. Det finns inte. Däremot så staplar man kanske flera lösningar på varandra för att skapa olika säkerhetslager och bygga in säkerhet på olika nivåer. Och det är så vi jobbar mycket med saker, att vi tittar på, vad kan vi. Kan vi ha säkerheten inne i systemet och så kan vi ha ute utanför systemet och sen kan vi ha det på nätverket och sen kan vi ha det på… På firewall, alltså vi jobbar med många olika säkerhetslager hela tiden, så det skulle jag säga är ett sätt. Annars kan man ju inte säga det. Vi har ju många it-säkerhets-initiativ. Och de flesta där är ju relaterade till det. Visst, många av dem är relaterade till olika typer av social engineering… och som jag. Jag tror jag nämnde det förra gången också. En av de största problemen idag när det kommer till social engineering är ju phishing. Ja det här med att folk skulle sitta och ringa till folk och försöka extrahera information. Absolut, det kan hända, men det är inte vanligt. Och det är ju bara viss typ av människor som är ganska duktiga på det. Jag märker ju alltså. Jag jobbar med många som har jobbat med penetrationstester, så det är bara för att man är en god penetrationstestare och är har väldigt god förståelse för tekniska innebär det ju inte att du är bra social engineer-er. Det är andra typer av saker att man är nästan att man ska hålla skådespelartalang liksom. Och du skulle kunna lura någon att vara snabbtänkt att det är en viss typ av talang liksom. Ja, det är inte alls säkert att en pentestare är speciellt bra på att ringa till någon och extrahera information till exempel många av de. pentestare jag har är ju kanske inte väldigt sociala. Så

de tycker det är jättesvårt att ringa till folk och extrahera saker som man faktiskt så att men jag skulle säga att phishing är det är det viktigaste eller största problemet när det kommer till social engineering, att man lurar folk på mejl, det är det vanligaste och mest problematiska, skulle jag säga.

35. TB
Just det. Skulle du säga att säkerhetskultur har en roll i mitigering av intrång.

36. R3
Ja utan detta utan en säkerhetskultur, så har du ingen säkerhet, alltså. Det är det som vi har pratat om innan kanske, men där jag kan köpa hur många lösningar som helst för detektering och allting liksom. Men det spelar ingen roll om någon ändå sitter och typ gör dumma saker och inte tänker sig för och klicka på saker så så kanske vi kan ha vissa system som kan rädda oss. Från den typen av saker, men. Men det är ju medvetenheten som gör att säkerhetskulturen som gör väldigt stor skillnad och det är många bolag som under estimerar impacten av medvetenhet så att säga och säkerhetskultur man tänker, men vi köper bara massa firewalls vi köper massa fancy application gateways och så vi så har vi löst allting. Men det. Är inte riktigt. Du kan ju ha hur mycket grejer som helst. Men om någon sitter och lämnar ut information eller. Laddar ner ett dokument som dom inte ska ladda ner och klicka på det och såna saker, så det är ju liksom. Ja då kan du hoppas att du har system som hjälper dig när någon gör någonting dumt men fortfarande vi vet till exempel att. Ja end point protection, alltså typ antivirus lösningar på datorerna. Ja, de kan ju fånga kända saker. Men nya saker ja då, då är det svårt.

37. TB
Ja, anser ni att det är svårare vid distansarbete på något sätt jobba med det här. I så fall hur och hur kan detta hanteras.

38. R3
Men du menar att skapa en säkerhetskultur.

39. TB
Ja till exempel.

40. R3
Ja, jag skulle vilja påstå faktiskt att ja, det är lite svårare för att jag märker att de gångerna jag går ut, jag har haft en del såna town-hall möten och såna saker får låna lite talartid hos olika chefer och sånt i organisationen. Då märker jag ju att folk blir mer engagerad när jag kommer ut och pratar med dem in personen. För då kommer de till mig efteråt och fråga om massa saker och du vet fler blir engagerade. Så jag skulle säga att det är lättare för mig att få ut mitt budskap och jag får träffa personalen. Mycket lättare. Det påverkar, det gör det.

41. TB

Hur kan man hantera det då ifall ifall det inte är tillgängligt så att säga om det är distans som gäller, vad kan man göra åt det.

42. R3
Det klart. Jag tycker att den är den är svår för att då handlar det kanske om att utbilda cheferna till att ha medvetenheten om it-säkerhet så att de får utbilda sin personal i sin tur så att man istället för att tänka att jag ska kunna ta mig runt till alla anställda och prata med dem, vilket jag inte kommer kunna göra, det är för många. Så kanske jag får gå till cheferna istället och så jag får ut mitt budskap till dem och hoppas på att cheferna sen meddelar det här vidare till sina organisationer och pushar för, [xxx] cheferna till det på det sättet också.

43. AO
Yes, men då tar vi sista frågan då. Då ska vi släppa iväg dig. Vad är det största problemet eller utmaning i mitigering av intrång.

44. R3
Intrången alltså som sker utifrån?

45. TB
Ifall det har skett redan vad är störst för utmaningen att mitigera skadan.

46. AO
Alltså förmildra den.

47. R3
Jag skulle svara även om det är ganska i min optik i alla fall att man man ser saker i tid och åtgärdar det i tid. För att vi har väldigt mycket detektering som möjligheter och så är det en sak, men sen så kanske det bygger på att en fysisk person då ska jag titta på detekteringen göra en analys. Vad är det som. Har hänt. Ta action och tyvärr är det ju så att vi vet att vissa av de här cyberangrepp man kan kan ske på 5 minuter. Så alltså vissa av de här stora ransomware-angreppen till exempel, där har ju. Många av datorerna blivit krypterad på typ 10-15 minuter. Så det jag skulle säga att det är svarstiden, alltså. Hur lång tid tar det för oss att hitta, se hotet. Förstå hotet och reagera på hotet. Det är det största problemet i min optik. För att. Om du har den mänskliga faktorn där liksom, det är ju den här. Det är inte så att allt som sitter och tittar på de här grejerna bara har en sak att titta på, utan det är ju ofta så kanske det kommer in ett alarm där och så kommer in någonting där och så händer det någonting där och så sitter de med att göra någonting annat så det är den svarstiden skulle jag säga att man hittar i tid och kan stoppa det.

48. AO
Yes ja. Men det var där vi hade superschysst att du ville ställa upp.

49. R3
Återigen inga barn.

50. AO
Så får du ha en superdag.

51. R3
Detsamma.

52. AO
Ha det.

7.3.8 Uppföljningsintervju 4

Intervjuns längd
25 minuter, 51 sekunder

Datum och tid
9/5/22, 18:00

Förkortningar
AO = Albin Olsson
TB = Tarek Bermalm
R1 = Respondent 4

1. TB
Så där. Ja, då kanske jag tar första frågan då. Vi undrar ifall ifall ni har policys och riktlinjer som är specifikt utformade för social engineering vid just distansarbete och i så fall, vilka är de.

2. R4
Nej, det har vi inte inte specifikt för distansarbete.

3. TB
Nej finns det sådana som är utformade för social engineering då.

4. R4
Ja det kan man. Det var som en. Jag kommer inte ihåg vad vi sa sist, men vi har ju en sån här introduktion alltså. Det finns ju en end user guideline på vårat företag och där finns ju fler avsnitt då som hanterar hur man ska agera och där ingår ju bland annat då när du jobbar med mobile devices och vad man bör tänka på alltså hela paketet där från när du sitter på flygplatser och vad du jobbar med för information. Till hur man ska agera. Men det och då inkluderar det även då även social engineering och egentligen, om du tänker att du sitter på kontoret också. Att besökare som har obehöriga som inte har besöksbricka och som inte ledsagas av någon anställd. Där ska man ju ställa frågan om vilka de är och så vidare och jag menar såna här allmänna formuleringar som att ifrågasätta alltid telefonsamtal och mejl om du inte vet vem avsändaren är. Om du inte kan bekräfta det, det finns ju då, men det är inget som är specifikt riktat då mot nu. Alltså om det. Jag vet inte om ni hade det här med pandemin som en liten inkörsport. Vi har inte haft några ökade detaljer eller att de har highlightat något i samband med det, utan det här de generella direktiven som finns.

5. TB
Just det, men för att förtydliga då så fanns där ju end user guidelines delar som som har att göra med vad du får säga och inte får säga och allmänna så är det ifrågasättande vid samtal och sådana.

6. R4
Ja, det finns det alltså det. Där är ju vi. Har ju jag skulle säga vi har klassificering av information, men vi jobbar inte med det på ett strukturerat sätt utan det är generella åtaganden, alltså vi gör definitioner på känslig information och konfidentiell och öppen publik då och där finns det ju då lite riktlinjer till hur man ska agera och hantera det när man delar information om man använder den och det är för att våra kunder ställer kraven. Men jag tror jag sa det sist också att det är vanligare.
Att kunden ställer krav. Eller de kunderna vi jobbar med att det är de som talar om hur vi ska dela information och så vidare. Det är inte så att det är inte så att vi kommer med det så.

7. TB
just det kan du, kan du uppleva att de här policys som finns oavsett om det är som kundens sida eller hos er sida att det ger effekt i så fall vilken.

8. R4
Det ger effekt hos dem som har ett medvetande som vet vad det handlar om. Det har inte effekt hos de som struntar i det som. Det det finns i alla verksamheter och där därför jag vill så jag brukar säga 80 20, alltså 80 % i människa, 20 % i teknik och om vi tittar på på risker och det speglar nog också ungefär.

9. TB
Just det.

10. R4
Vad heter det beteendet hos de anställda. Jag menar jag, men vi jag sa kanske det också att det är ju jurister alltså. De jobbar med patent och trademark och det är ju småpåvar alltså. Vi är 500 anställda varav trehundrafemtio har ju 200 högskolepoäng, alla vet bäst så jag menar det, de vet att det är mer värt än vad IT-avdelningen säger till dem i vissa sammanhang och prioriteringar med att kunden har rätt och jag måste kunna jobba och fakturera. Det är viktigare än alltså. Det tas beslut på olika grunder om man säger så.

11. TB
Så skulle du säga att i och med den där bakgrunden de har eller den kompetens och de här ska man säga att de har helt enkelt är det en högre medvetenhet kring social engineering.

12. R4
Jag skulle säga som så här de är medvetna om när de bryter mot. Jag tror alla vet när de gör någonting som de inte borde göra och då har då har de väl den tanken. Är det okej här och det är klart, jobbar du då med en befintlig kund som du har jobbat med i 5 år och blabla Då tror jag de tänker att vi har jobbat med det här i 5 år och agerat på det här sättet. Jag tror inte det är någon som utger sig för att vara någon annan, så det är väl ändå en sån där tanke och medvetenhet, men då kan man ju vända på det så här. Hur tror ni att en malicious intruder i sin tur agerar. Det är precis det som är social engineering, att utge sig för någon som man har

jobbat med i 5 år och skicka ungefär samma typ av meddelanden som har gjort så att just det här med locka till felaktigheter och så, det är väl det. Det är väl både på gott och ont.

13. TB
Just det.

14. R4
Men vi har ju ett rätt bra team, som jag sa i Indien då som övervakar all trafik och de om vi säger så fort det kommer upp någon ny trend där det där det skickas ut antingen mejl eller att det är folk som ringer eller så där.De är ju rätt snabbt på och lägga ut den typen av information då till företaget, men då är det ju det gamla barnet. Då lägger de ut det på vårat intranät. Jag menar hur många sitter och läser ett företags intranät dagligen.
Så så det ja. Det finns ingenting som är så bra så att det inte går att göra bättre om jag summerar.

15. TB
Jag förstår, ja, hur arbetar ni att skydda er verksamhet mot social engineering-attacker och då just vid distansarbete.

16. R4
Ja, det är ingen ingen aktiv handling vid distansarbete. Vi har ju ett gäng en tjänst som vi levererar till kunder. Det är ju så här med red teaming och blue teaming då så och det görs ju internt också men jag skulle säga att det är väl lite mer. Ja det. Det är också det görs för att visa att vi egentligen håller på med det och så. Men ja.

17. TB
Och detta är för social engineering men inte distansarbete? Är det korrekt eller hur ligger det till?

18. R4
Ja, det alltså distansarbete, det kan du sätta ett streck över. Det har ju inte gått ut något specifikt. Utan var du än jobbar. Det gjorde vi innan också jag menar, folk satt ju hemma och folk sitter ute hos kunder och kopplar upp sig via nätverk och så där så.
Så det har det har inte gjorts något extra inlägg för det. Det red teaming och blue teaming är att man går ut och försöker infiltrera sig på kontor och utge sig för någon och ställa frågor kring vem som är chef och så vidare.

19. TB
Nej, precis.

20. R4
Det är ju inte heller något nytt, men det har ju införts de sista två åren på vårt bolag då, så det är ju relativt nytt för organisationen och då får man ju lägga upp en flerårsplan så att säga man får göra det en gång och redovisa resultatet innan man kan tala om för folket. Ja, det var ni vet

20 stycken som gjorde något de inte borde ha gjort. Vad menar då man får ju köra det ett par vänd det är inte så att man löser det på en eftermiddag.

21. TB
Nej just det. Men en ytterligare fråga här då. Hur anser ni att distansarbete har påverkat ert arbete mot social engineering? Kan du uppleva någon effekt där?

22. R4
Nej, det är alltså. Vi har ju inte. Det har inte varit på agendan vi inte haft några incidenter har inte förupprätt att att agera på det har inte.

23. AO
Okej.

24. R4
Den typen av incidenter, och det har inte ja.

25. TB
Jag förstår. Albin vill du fortsätta.

26. AO
Ja absolut. Vilka är de största utmaningarna i att skydda er mot phishing attacker vid distansarbete?

27. R4
Alltså, ja, jag vet inte om det dubblar där så phishing attacker har väl ingenting med distansarbete att göra det. Det har ju mer koppling till att man får mejl eller att du surfar på sidor som du inte ska surfa på eller att du klickar på länkar och så vidare så det det ser jag ingen koppling till att det ser annorlunda ut när du jobbar på distans. Jag menar det, och det är ju ändå så att vi sitter och jobbar med våra företagsdatorer och kopplar upp sig, så vi har ju de här vad det nu heter där direct access och sådär så att det är ju bara de tjänsterna som publiceras av företaget som vi kan jobba med hemifrån och det är ju inte så att vi sitter och kopplar upp privata. Alltså, vi synkar mejlen med privata mejladresser och vi sitter ju inte att jobba från privata datorer mot vårt företags nät. För det går inte helt enkelt, så det där finns ju en viss styrning och där inkluderas ju phishing och den typen alltså det. Det tänker man ju in per automatik då.

28. TB
Men skulle ni det är ju en följdfråga där då, om skulle ni säga att det är an era anställda i verksamheten. Att anställda i eran verksamhet är medvetna, eller hur det ses på ifall distansarbete medför större risker för social engineering-attacker.

29. R4
Jag tror mognadsgraden alltså ni snackar social engineering det som rubrik område.

Vi, jag säger det, vi har inte drabbats, vi känner ingen som har drabbats. Vi har inte jobbat med några kunder som har drabbats. Vi har haft det på agendan när vi sitter med kunder, men vi har inte sett någon. De enda gångerna som jag kan redovisa att social engineering har fungerat. Det är när vi själva har gjort tester, men då är det ju medvetna planerade tester. Så jag, jag har ingen referens till kund eller någon eller så har de ju bara hållt truten. Det är aldrig någon som har. Jag har inte varit i kontakt med en enda, ett enda företag som ens vid ett tillfälle har drabbats av det det vi kallar social engineering, att någon utger sig för att vara någon annan. Jag menar phishing attacker och sånt där så svar ja, men det det bedömer ju inte jag som social engineering. Phishing attacker, det är ju. Det kan ju du och jag söka upp någonting och ladda ner på nätet och lägger in i ett mejl och sen hitta på någonting så.

30. TB
Ja alltså, det finns ju olika definitioner på social engineering och den vi använt till litteraturen och så där återigen, det kan skilja sig åt.

31. R4
Ja ja.

32. TB
Men det vi använt har täckt även social engineering och andra saker som vi säger social engineering inkluderar vi även phishing bland annat.

33. R4
Och då alltså Det jag inte känner mig bekant med, alltså social engineering, phishing och allt det här säkerhetsmedvetande. Ja, men att man skulle göra något specifikt kopplat till distansarbete. Det känner jag mig lite främmande för alltså det. Det finns ju ingenting som ändrar på det regelverket, alltså vi skulle vara precis lika noggranna och så när vi sitter på jobbet alltså. Det har ju ingenting med rubriken distansarbete att göra om du frågar mig.

34. TB
Nej förstår. Men tänkte nästa fråga där. Vi ska se vart vi var här.
Ja hur hur är ledningen hos er verksamhet insatta i social engineering, skulle du säga.

35. R4
Är det anonymiserat så skulle jag säga att vi har en omogen ledningsgrupp kopplat till allting som rör informationssäkerhet.

36. TB
Det är anonymiserat

37. R4
Det var som jag sa förra gången att jag själv är 56 år och har jobbat med det här i 30 år, men jag betraktar mig själv inte som någon guru eller expert, men jag menar 9 av 10 kunder som jag jobbar med där sitter ju andra som är 56 år och de är ekonomichefer och VD och så där

och det är klart, det är ganska logiskt att de kan ännu mindre än vad jag kan kring informationssäkerhet och vad det innebär. Så det är väl ungefär så man kan summera det. Sen kan du gå ut på lagret på ett logistikföretag och så ska du tala om för de som jobbar på lagret hur de ska jobba med mejl och social engineering och så där och då är det 25 åringar som har sitt andra jobb. De kan ju 10 gånger mer än vad företagsledningen kan så där.
De, som är 20 30 år. De har koll på det här. De har suttit och spelat spel och spelen funkar inte när det inte har uppdaterade säkerhets remisser och jag menar du sitter inte på samma nätverk som lillsyrran om du vill att din speldator ska fungera då lär man sig ju bygga upp det här och man lär sig att inte göra saker och ting och det har ju med sig även från skolgång och så. Jag menar vad fan. Det fanns inga paddor och datorer när jag gick i skolan. Då var det papper och penna som gällde. Men medans då de som är chefer och VD idag. Det var papper och penna för dem också så de har, det är väldigt låg mognadsgrad det gäller inte bara på det bolaget jag är anställd på.

38. TB
Ja skulle du skulle du beskriva det som en ovana, eller hur ser du på det.

39. R4
Omognad. De har aldrig satt sig in i den, de aldrig behövt. De har alltid frågat någon annan, vilket innebär att då vet de inte vad, hur det fungerar eller vad det handlar om och då är det ju ganska svårt att ta korrekta beslut.

40. TB
Hur kan detta hanteras då.

41. R4
För frågar du mig så hade jag, hade jag varit VD på ett bolag som är väldigt IT tungt eller intensivt där det ställer stora krav på att man har medvetenhet kring de prylarna man jobbar med. Då hade jag plockat in 2 stycken tjugofemåringar och så har jag talat om för dem vad jag vill att de ska göra. Så jag hade varit chef inte, jag hade inte talat om för dem vad de ska göra utan alltså rent tekniskt. Utan jag hade sagt till dem att det här och det här och det här ska vi göra och ni ska tänka på det här och det här, det här. Har ni en lösning på det.
Så hade de fått göra jobbet för då kan antagligen tekniken 10 gånger bättre än vad jag kan.

42. TB
Vad gör man med den den existerade ledningen då. För att hantera det ifall de fortfarande är i den [xxx].

43. R4
Ja, man kan väl säga som så här. Du kan inte sätta en 25 åring till att bli IT-chef och ansvarig för upphandlingar med partnerbolag, budgetar, återkoppling till verksamhet alltså. De har ju alldeles för dålig koll på vad det innebär att driva ett företag och det är ju det en företagsledning ska göra om de inte har kompetens inom IT. Då ska de driva företaget.

Traditionellt, men de ska ju inte lägga sig i och tala om för en IT-avdelning vad de ska göra och inte göra när de inte begriper vad det är de bestämmer om.

44. TB
Skulle en vinkel på det att vara att att låta det som är säkerhetsexpert inom företaget har en högre, en närhet till ledningen, alltså ha en högre sits, kanske vid bordet vid ledningen.

45. R4
Absolut ja, det är väldigt ovanligt även i stora bolag idag. Att IT eller vad ska vi säga, informationssäkerhet finns ju inte på agendan. Utan den som är IT-chef eller den som är då tillförordnad Chief information Security officer som det så snyggt heter. De rapporterar ju ofta till någon i inledningen. Det är inte så att de sitter med och är delaktiga i affärsutveckling eller strategier eller hur man ska jobba framåt, vilket är en väldigt. Det är ett väldigt stort. Vad ska man kalla det för. Det är ett aber när du ska driva det här på ett vettigt sätt. Och sen då, den dagen när Apple kommer och säger då att du har ni, ni får inte vara våran partner, ni får inte leverera tjänster till oss om ni inte garanterar att ni jobbar med informationssäkerhet på ett vettigt sätt visa oss. Då går ju samma ledningen och tror att man kan köpa det alltså. Plocka in en konsult och jobbar 2 veckor och så tror de att de har svaren på frågorna men det är inte det Apple frågade.De frågar ju efter hur man jobbar med det här på ett vettigt sätt.

46. TB
I det säkerhetsarbetet där att försöka etablera bra säkerhet för god säkerhet och en hög säkerhets mognad. Vad är utmaningen eller problemet är att få ledningen att lägga det högre.

47. R4
Pengar och så klart. De ser ju inte värdet av en investering.
De kopplar ju bara över de där de läser ju bara intäkter och utgifter och det är det kommer ju inte lösas innan jag dör höll jag på att säga, för det var ju för 20 år redan så. När jag pluggade 35 år sedan, bara en sån sak som interndebitering, ett företag med 7000 anställda och så ska man byta datorer på 35 orter. Då har vi en massa tekniker på plats och som sitter på servicedesken och såg ut som bolag och men då kostar det. Då ska de ha interndebitering 600 spänn i timmen så då säger vi att ja, men om vi går till IT-gården och IT-hantverkarna då kan vi köpa upp för 400 kr i timmen. Ja, men gör det då säger man ja, men vad fan 400 spänn i timmen om vi behöver 1000 timmar. Det är fyrahundratusen som går ut ur bolaget bara för att interndebitering i sexhundratusen och då går vi med förlust, alltså den som ska byta datorerna har ansvar för det uppdraget går ju back. Så istället anlitar man IT-hantverkarna och så försvinner det fyrahundratusen kronor ut ur bolaget. Det här var ju sån där interndebitering problem som jag pluggade 1990, men då har man. Alltså det hade man inte löst 2015 i alla fall så det är väl han Adam Smith eller vad han heter, han man får tacka. Det sa jag nog sist också va.

48. TB

Ja kanske det. Ja, det var en en till fråga jag tänkte på. Från ett proaktivt perspektiv. Hur arbetar ni med ett mitigerar eller mildra eller lindra skadan av en social engineering-attack ifall det skulle ske.

49. R4
Vi har egentligen bara standard. Vi har en IT-avdelning. Vi har rapporteringsvägar där alltså det, vi har övervakning, vi har hjälp post, vi har sån här rapport till närmsta chef och så vidare då så att vi har ju eskalering rutiner och är det så att man klassificerar en incident som vad heter det prioriterade eller att det kan få en stor inverkan. Då har vi ju ett gäng då så att säga som analyserar vad det är som har hänt och sen är det så att man misstänker att det här kan jag få stora ekonomiska konsekvenser. Ja, då kommer vi blanda in ekonomichefer och kundansvariga eller så att det kan bli stora tekniska problem. Ja du vet du får plocka in den kompetensen beroende på vad det är för incident och så får man försöka lindra det i sin skala då. Det är ju också lite svårt för vissa grejer då vill man ju traditionell, incidenthantering stoppa blödningen, återställ funktionalitet och sen analysera vad det var som hände. Men i dagsläget och framförallt nu när ni pratar social engineering, där man kanske tittar efter lite mer allvarliga grejer. Nu har vi forensik och grejer som ger helt andra möjligheter än vad de gjorde för 20 år sedan. Men nu kanske det är så att man vill att incidenten ska fortleva ett tag just för att du ska kunna samla bevis och identifiera vad det är som händer och sker här och det skapar ju lite andra förutsättningar.
Men det är ju väldigt beroende på vad det är för verksamhet man har och vad det är för typ av incident man tittar på. Men det har ju också ändrats lite med åren om man säger så. Men där, vi jobbar inte, vi har bara traditionell. Så se till att det funkar igen och sen analysera åtgärderna om det är någonting som går att åtgärda.

50. TB
Just det, hur är det med… oj här ramlade lite saker ursäkta. Jo, hur är säkerhetskultur i mitigeringen av social engineering-attacker som inträffar, säkerhetskultur. Vilken roll spelar detta i mitigeringen?

51. R4
Ja som sagt, vi har ju aldrig haft någon sådan incident, så det skulle jag säga du då får jag säga, jag vet inte inte om du pratar om vårt företag i alla fall.

52. TB
Nej precis utan jag det jag hoppas på att, de jag vill formulera det är ett proaktivt perspektiv så att i fallet en attack skulle ske har ni lagt upp något med säkerhetskultur.
Är det så att ni har jobbat med det på nåt sätt för att förebygga ifall det skulle hända.

53. R4
Nej, inte nej, alltså inte annat än det andra. Alltså säkerhetskultur. Det är väl det man bygger med awareness training och när du har planerade red team attacker eller när du skickar ut phishing mejl för att testa hur användarna beter sig men nej, vi har inte gått någon kurs i retorik, eller hur man är skådespelare eller så där då för att skapa någon kultur utan det här är

ju ett. I samband med att man anställd så har vi våra introduktionskurser och så när kultur är vad, hur ser din vardag ut, jag menar vi har regelbundna möten med utvecklings gänget nere i Malmö och vi träffas en gång i månaden. Det är varannan vecka har vi avstämningsmöten och de som jobbar inom, med teknisk säkerhet och har de lite dragningar där de går igenom, det är en form av kultur, men där är ju bara social engineering en punkt på, så det är inte så att det är något riktat just kopplat till det. Det är en del i det stora.

54. TB
Ja ska se ja och i mitigering. Vad är det. Vad är det största utmaningen i att ha en effektiv mitigering ifall skada ifall intrång sker?

55. R4
Ja, det är nog lite för brett områden. Håller vi oss till vårat företag. Som sagt, då har vi ju inte haft någon sån typ av incident eller som har lätt. Jag menar det värsta som har hänt med vårt bolag. Det är väl att någon e-postserver har gått ner medans vi hade en stor konferens så där de skulle använda e-posten för att kommunicera med deltagarna på konferensen. Så det var ju mer praktiskt, men det var ju inget säkerhet alltså. Det var ingen informationsäkerhetsgrej eller eller något sånt alltså, och som jag sa så har jag jobbat i 35 år med. Både stora och små kunder och ja, nej, jag hade jag har. Jag har ju inte något bra svar på det.

56. TB
Nej och det är okej.

57. R4
Då största problemet med mitigering av incidenter generellt är att om du tänker är att du har, om man räknar, jag kommer inte ihåg mitt lösenord som en incident, för det är det ju om du har tappat bort ditt lösenord och ringer upp till någon servicedesk och de ska sätta upp ett nytt lösenord, alltså att bli av med sitt lösenord är potentiellt att du skulle kunna breacha och när du ringer in där och vill ha ett nytt lösenord om du får ett för enkelt lösenord. Så är ju inte det bra. Samtidigt får du ett svårt lösenord så kommer användaren och jag menar om tiotusen användare i veckan som ringer om lösenord och då tröttnar man på desken att sätta starka lösenord och då litar man på att användarna ska byta lösenorden. Men den här typen av incidenter hanterar man ju. Det har fortfarande inte lett till några större inverkningar. Har man fyrtiotusen incidenter per månad på 30 bolag. Ja då har man ju. Man lägger ju jättemycket energi på att hantera de här 10 20 30 tusen som är hanterbar och som går att effektivisera som kostar mycket pengar men där risk och konsekvens egentligen är obefintlig. Det händer ju ingenting. Det är bara att man jobbar med dem riskerna sen så kanske du har. En ekonomichef som inte får ut sin rapport 2 timmar innan han ska redovisa det här för styrelsen eller för någon Investment grupp som ska in i bolaget. Ja, det kan ju få enorma konsekvenser i bolaget, men det är bara en incident på 40 tusen. Den försvinner ju och det är ingen som har en aning om det. Jag menar om du för statistik på vem som sitter i telefonen, då tittar man på genomsnittlig svarstid, ska vara en minut och 40 sekunder. Det är ju allting som kommer in när det och det och det har man koll på, men sen så är det någon som sitter där och väntar i 45 minuter. Men det är bara är en så den faller utanför [xxx] och sånt där jag personligen skulle

ju vara mer intresserad av vem fan fick sitta och vänta i 45 minuter och varför. Så det kan ju vara värt att följa upp medans då de här som får svar inom 30 sekunder. Det är väl totalt ointressant det, det funkar ju bara så så där. Det är lite styrnings effekter där så jag skulle säga, det är väl det som är största utmaningen med mitigeringar i allmänhet. Men det tog jag några enkla exempel. Det här med servicedesken, men alltså om du har incidenten som är svåra att felsöka, oavsett om det är människor som har varit involverad eller om det är tekniska problem. Alltså, hur fan hanterar man dem när man aldrig kommer fram till svaret eller när det sen efter 1,5 månad visade sig att man hade satt samma IP nummer på på 2 system och att det blir konflikter och då kunderna upplevt driftstörningar och system som har dykt i 1,5 månad. De haft inne konsulter för att analysera databaser och koder i applikationer och allting och så visar det sig att att man har IP nummer konflikt. Jag menar. Det är enkelt att lösa, men vad hur fan talar man om det för en kund.

58. TB
Men om du lämnar om det är en sån incident som är som har skett och som är svår att analysera efterhand, vad gör man då, vad är hanteringen.

59. R4
Nej alltså är det stora bolag så bygger du upp såna här återkommande alltså, då har man ju processer för alla incidenter som har föranlett, vad heter det, klassificering, högsta klassificeringen då. Om du klassar dem från 1 till 4 och 4 är det värsta, då har man ju rutiner. Så att det är ju inga klass 4 incidenter som man inte går igenom där man genomför en analys, man skriver en rapport man drar lärdom och man konstaterade om det här går att förebygga för nästa gång,
eller om man ska ändra på kommunikationsplattformen eller ja, det kan ju vara såna här enkla saker som har uppstått på grund av att kunden inte har uppdaterat sina system och då är ju det vad man får redovisas då. Men jobbar man med det här då då har man uppföljning på alla stora incidenter och då finns det speciella incidenthantering. Samt chefer eller vad man nu ska kalla det för som som har det på sitt bord. Så där. Men det är ju reaktivt. Det är ju efter att det hänt som man sitter och analyserar då så det det. Det är ju lite svårare att förutse, gissa vad som ska hända.

60. TB
Albin, tycker du vi fick med allt?

61. AO
Ja, jag tycker ändå bra. Har du något mer?

62. TB
Jag tror att jag tror att jag är nöjd.

63. AO
Då stänger jag av inspelningen.

Referenser

Andress, J. (2014). The Basics of Information Security: Understanding the Fundamentals of Infosec in Theory and Practice. *Syngress*.

Acar, A., Lu, L., Uluagac, A. S. & Kirda, E. (2019). An Analysis of Malware Trends in Enterprise Networks, pp.360–380.

Amankwa, E., Loock, M. & Kritzinger, E. (2018). Establishing Information Security Policy Compliance Culture in Organizations, *Information & Computer Security*, vol. 26, no. 4, pp.420–436

Ball, L., Ewan, G. & Coull, N. (2012). Undermining - Social Engineering Using Open Source Intelligence Gathering, KDIR 2012 Proceedings, Tillgänglig på: https://rke.abertay.ac.uk/en/publications/undermining-social-engineering-using-open-source-intelligence-gat [Hämtad 12 Maj 2022]

Barrero, J. M., Bloom, N. & Davis, S. (2021). Why Working from Home Will Stick, Cambridge, MA. Tillgänglig på: https://www.nber.org/papers/w28731 [Hämtad 11 Maj 2022]

Baruch, Y. (2000). Teleworking: Benefits and Pitfalls as Perceived by Professionals and Managers, *New Technology, Work and Employment*, vol. 15, no. 1, pp.34–49

Berg, A., Andersson, J. & Holmqvist, R. (2021). Informationssäkerhetsutmaningar vid storskaligt distansarbete. Tillgänglig på: https://lup.lub.lu.se/student-papers/search/publication/9052969 [Hämtad 26 April 2022]

Borkovich, D. & Skovira, R. J. (2019). CYBERSECURITY INERTIA AND SOCIAL ENGINEERING: WHO'S WORSE, EMPLOYEES OR HACKERS?, *Issues In Information Systems*, vol 20, pp.39-150

Borkovich, D. & Skovira, R. J. (2020). WORKING FROM HOME: CYBERSECURITY IN THE AGE OF COVID-19, *Issues In Information Systems*. Tillgänglig på: https://www.researchgate.net/publication/354694505_Working_From_Home_Cybersecurity_in_the_Age_of_Covid-19 [Hämtad 26 April 2022]

Brody, R., Luo, R., Seazzu, A., Burd, S. (2011). Social Engineering: The Neglected Human Factor for Information Security Management. Tillgänglig på: https://www.researchgate.net/publication/220121607_Social_Engineering_The_Neglected_Human_Factor_for_Information_Security_Management [Hämtad 23 april 2022]

Bulgurcu, Cavusoglu & Benbasat. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, *MIS Quarterly*, Tillgänglig på: https://www.jstor.org/stable/25750690?seq=8 [Hämtad 5 Maj 2022]

Ceraolo, J. P. (1996). Penetration Testing Through Social Engineering, *Information Systems Security*, vol. 4, no. 4, pp.37–48

Chapman, P. (2021). Defending against insider threats with network security's eighth layer, Computer Fraud & Security, vol. 2021, no. 3, pp. 8-13

CybSafe. (2020). Human error to blame for 9 in 10 UK cyber data breaches in 2019, Tillgänglig på: https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/ [Hämtad 5 Maj 2022]

da Veiga, A. (2018). An Approach to Information Security Culture Change Combining ADKAR and the ISCA Questionnaire to Aid Transition to the Desired Culture, *Information & Computer Security*, vol. 26, no. 5, pp.584–612

Dandurand, L. & Serrano, O. S. (2013). Towards Improved Cyber Security Information Sharing, CYCON 2013 Proceedings, Tillgänglig på: https://ieeexplore.ieee.org/document/6568369 [Hämtad 12 Maj 2022]

Eminağaoğlu, M., Uçar, E. & Eren, Ş. (2009). The Positive Outcomes of Information Security Awareness Training in Companies – A Case Study, *Information Security Technical Report*, vol. 14, no. 4, pp.223–229

Eurofound. (2020), Living, working and COVID-19, COVID-19 series, Publications Office of the European Union, Luxembourg. Tillgänglig på: https://www.eurofound.europa.eu/sites/default/files/ef_publication/field_ef_document/ef20059en.pdf [Hämtad 28 april 2022]

Eurostat. (2020). How usual is it to work from home?, Tillgänglig på: https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20200424-1 [Hämtad 28 April 2022]

Europakommissionen. (2020). Telework in the Eu before and after the Covid-19: Where We Were, Where We Head to Headlines

FBI. (2020). Internet Crime Report, Tillgänglig på: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf [Hämtad 9 Maj 2022]

Furnell, S. & Shah, J. N. (2020). Home Working and Cyber Security – an Outbreak of Unpreparedness?, *Computer Fraud & Security*, vol. 2020, no. 8, pp.6–12

Georgiadou, A., Mouzakitis, S. & Askounis, D. (2021). Working from Home during COVID-19 Crisis: A Cyber Security Culture Assessment Survey, *Security Journal*.

Goodhue, D. L. & Straub, D. W. (1991). Security Concerns of System Users, *Information & Management*, vol. 20, no. 1, pp.13–27

Gragg, D. (2003). A Multi-Level Defense Against Social Engineering. *ANS Institute*

Hight, S. D. (2005). The Importance of a Security, Education, Training and Awareness Program, *City of Raleigh*, no. 1-5

Hoffer, J. A. & Straub Jr, D. W. (1989). The 9 to 5 Underground: Are You Policing Computer Crimes?, *MIT Sloan Management Review*, vol. 30, no. 4, pp.35

Hove, L. (2020). Strategies Used to Mitigate Social Engineering Attacks. *Walden University*

Hughes-Lartey, K., Li, M., Botchey, F. E. & Qin, Z. (2021). Human Factor, a Critical Weak Point in the Information Security of an Organization's Internet of Things, *Heliyon*, vol. 7, no. 3

CybSafe. (2020). Human Error to Blame for 9 in 10 UK Cyber Data Breaches in 2019.

Höne, K. & Eloff, J. H. P. (2002). Information Security Policy — What Do International Information Security Standards Say?, *Computers & Security*, vol. 21, no. 5, pp.402–409

Ivaturi, K., & Janczewski, L. (2011). A taxonomy for social engineering attacks. International Conference on Information Resources Management. *Centre for Information Technology, Organizations, and People,* pp.1-12

Jacobsen, D. I. (2002). Vad, Hur Och Varför: Om Metodval I Företagsekonomi Och Andra Samhällsvetenskapliga Ämnen: Studentlitteratur AB.

Koohang, A., Anderson, J., Nord, J. H. & Paliszkiewicz, J. (2019). Building an Awareness-Centered Information Security Policy Compliance Model, *Industrial Management & Data Systems*, vol. 120, no. 1, pp.231–247

Kraemer, S. & Carayon, P. (2007). Human Errors and Violations in Computer and Information Security: The Viewpoint of Network Administrators and Security Specialists, *Applied Ergonomics*, vol. 38, no. 2, pp.143–154

Krombholz, K., Hobel, H., Huber, M. & Weippl, E. (2015). Advanced Social Engineering Attacks, *Journal of Information Security and Applications*, vol. 22, pp.113–122

Kruger, H. A. & Kearney, W. D. (2006). A Prototype for Assessing Information Security Awareness, *Computers & Security*, vol. 25, no. 4, pp.289–296

Lundgren, B. & Möller, N. (2019). Defining Information Security, *Science and Engineering Ethics*, vol. 25, no. 2, pp.419–441

Luo, X., Brody, R., Seazzu, A., & Burd, S. (2011). Social Engineering, *Information Resources Management Journal*, vol. 24, no. 3, pp.1–8

Mann, I. (2008). Hacking the Human: Social Engineering Techniques and Security Countermeasures. *I. Title, Hampshire: Gower publishing company*

Magnuson, S. (2017). Defending Networks Emerges as Top Battlefield Priority, National Defense, vol. 101, no. 758, pp.35-36

McKinsey & Company. (2021). What executives are saying about the future of hybrid work. *People and Organizational Performance*, Tillgänglig på: https://www.mckinsey.com/business-functions/people-and-organizational-performance/our-insights/what-executives-are-saying-about-the-future-of-hybrid-work [Hämtad 19 April 2022]

McKinsey & Company. (2021). What employees are saying about the future of remote work. *Organization Practice*, Tillgänlig på: https://fortcollinschamber.com/wp-content/uploads/2021/04/What-employees-are-saying-about-the-future-of-remote-work-Final.pdf [Hämtad 10 maj 2022]

Rao, U. H., & Nayak, U. (2014). The InfoSec handbook: An introduction to information security.

Peltier, T. (2006). Social Engineering: Concepts and Solutions. *Information System Security*, vol. 15, pp.13–21

Popovici, V. & Popovici, A.-L. (2020).Remote Work Revolution: Current Opportunities and Challenges for Organizations, *Ovidius Univ. Ann. Econ. Sci. Ser*, vol. 20, no. 468-472

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study, *MIS Quarterly,* Tillgänglig på: https://www.researchgate.net/publication/220260086_Improving_Employees'_Compliance_Through_Information_Systems_Security_Training_An_Action_Research_Study [Hämtad 4 Maj 2022]

Rahman, T., Rohan, R., Pal, D. & Kanthamanon, P. (2021). Human Factors in Cybersecurity: A Scoping Review, IAIT 2021 Proceedings, Tillgänglig på: https://dl.acm.org/doi/10.1145/3468784.3468789 [Hämtad 3 Maj 2022]

Salahdine, F. & Kaabouch, N. (2019). Social Engineering Attacks: A Survey, *Future Internet*, vol. 11, no. 4, p.89

Samonas, S. & Coss, D. (2014).The Cia Strikes Back: Redefining Confidentiality, Integrity and Availability in Security, *Journal of Information System Security*, vol. 10, no. 3

Sharton, B.R. (2020). Will Coronavirus Lead to More Cyber Attacks?, *Harvard Business Review*, Tillänglig på: https://hbr.org/2020/03/will-coronavirus-lead-to-more-cyber-attacks [Hämtad 28 April 2022]

Siponen, M.T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, vol. 8, pp.31-41

Siponen, M., Pahnila, S. & Mahmood, M. A. (2010). Compliance with Information Security Policies: An Empirical Investigation, *Computer*, vol. 43, no. 2, pp.64–71

Straub, D. W. (1990). Effective IS Security: An Empirical Study, *Information Systems Research*, vol. 1, no. 3, pp.255–276

Straub, D. W. & Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making, *MIS Quarterly*, Tillgänglig på: https://www.researchgate.net/publication/220260271_Coping_With_Systems_Risk_Security_Planning_Models_for_Management_Decision_Making [Hämtad 8 Maj 2022]

Talib, S., Clarke, N. L. & Furnell, S. M. (2010). An Analysis of Information Security Awareness within Home and Work Environments, in *2010 International Conference on Availability, Reliability and Security*, February 2010, IEEE, pp.196–203

Tessian. (2020). Research Shows Employees Are Less Likely to Follow Safe Data Practices at Home, Tillgänglig på: https://www.tessian.com/blog/employees-are-less-likely-to-follow-safe-data-practices-at-home/ [Hämtad 19 April]

Tessian. (2021). Back to Work Security Behaviours Report, Tillgänglig på: https://f.hubspotusercontent20.net/hubfs/1670277/%5BCollateral%5D%20Tessian%20Research/%5BTessian%20Research%5D%20Back%20to%20Work%20-%20Security%20Behaviors%20Report.pdf?utm_referrer=https%3A%2F%2Fwww.tessian.com%2F [Hämtad 19 April]

Thomson, K.-L., von Solms, R. & Louw, L. (2006). Cultivating an Organizational Information Security Culture, *Computer Fraud & Security*, vol. 2006, no. 10, pp.7–11

Trzupek, B. (2020). PKI Is Key to Securing a Post-Covid Remote Workforce, *Computer Fraud & Security*, vol. 2020, no. 10, pp.11–13

von Solms, R. & van Niekerk, J. (2013). From Information Security to Cyber Security, *Computers & Security*, vol. 38, pp.97–102

Wang, B., Liu, Y., Qian, J., & Parker, S.K. (2021). Achieving effective remote working during the COVID‐19 pandemic: A work design perspective. *Applied psychology*, vol. 70, no. 1, pp.16-59

Williams, C.M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity Risks in a Pan-demic, Journal of Medical Internet Research, vol. 22, no. 9, pp. 1-4, Tillgänglig på: https://www.jmir.org/2020/9/e23692/ [Hämtad 28 April 2022]

Wilcox, H. & Bhattacharya, M. (2020). A Human Dimension of Hacking: Social Engineering through Social Media, *IOP Conference Series: Materials Science and Engineering*, vol. 790, no. 1, p.012040

Wiley, A., McCormac, A. & Calic, D. (2020). More than the Individual: Examining the Relationship between Culture and Information Security Awareness, *Computers & Security*, vol. 88, p.101640

Whitman, M.E. & Mattord, H.J. (2008). Management of Information Security, *Boston: Course Technology*

Whitman, M.E. & Mattord, H.J. (2011). Principles of information security, 4th edn, *Boston: Course Technology*

Yang, L., Holtz, D., Jaffe, S., Suri, S., Sinha, S., Weston, J., Joyce, C., Shah, N., Sherman, K., Hecht, B. & Teevan, J. (2022). The Effects of Remote Work on Collaboration among Information Workers, *Nature human behaviour*, vol. 6, no. 1, pp.43–54

Zulkurnain, A. U., Hamidy, A. K. B. K., Husain, A. B., & Chizari, H. (2015). Social engineering attack mitigation. *International Journal of Mathematics and Computational Science*, vol. 1, no. 4, pp.188-198