Examensarbete

HÖGSKOLAN I SKÖVDE

SKILLNADER I ARBETET ENLIGT SÄKERHETSPOLICYN OCH ARBETET I VERKLIGHETEN

Examensarbete inom huvudområdet Datalogi
Grundnivå 15 högskolepoäng
Vårtermin 2013

Jimmy Andersson

Handledare: Birgitta Lindström
Examinator: Jonas Mellin

Sammanfattning

Information är en viktig tillgång för organisationer och därför är också informationssäkerhet viktigt för företag som vill skydda sin information. Företag inför informationssäkerhetspolicys som är en syn på hur företagets ledning vill att informationssäkerheten ska skötas. Det är ett problem att anställda väljer att inte följa vissa delar eller hela säkerhetspolicyn av olika anledningar. Detta arbete utför en fallstudie på ett företag för att se hur anställda efterlever den säkerhetspolicy som finns. Strategin för undersökningen är generell och den visar hur företag kan gå tillväga för att identifiera brister i efterlevnaden av säkerhetspolicyn. Resultat visar att flera av de anställda på företaget inte följer den policy som ledningen har tagit fram. I framtiden skulle det vara intressant att utföra en större undersökning som sträcker sig över flera företag.

Nyckelord: Informationssäkerhet, Informationssäkerhetspolicy, Strategi, Efterlevnad och Fallstudie.

Innehållsförteckning

1 Introduktion

Informationssäkerhet behandlar både datasäkerhet och säkerhet i allmänhet. Att skydda information är inte något beteende som har kommit nu på senare tid. Behovet att transportera information har funnits sedan länge. Som exempelvis en ridande budbärare som transporterade meddelanden mellan städer. Ibland blev de attackerade och informationen som meddelandet bestod av gick förlorad. Ett sätt att skydda budbäraren behövdes. Att transportera meddelanden idag sker för det mesta digitalt och det hittas nya tekniker för att skydda informationen på dem, som exempelvis kryptering av olika slag.

Det finns flera olika typer av hot mot information i dagens samhälle: Fysiska hot, logiska hot och mänskliga hot. Fysiska hot är hot som kan skada fysiska ting som exempelvis stöld och brand. Logiska hot är hot som kan skada verksamheten genom att en obehörig person fått tillgång till systemet. Mänskliga hot är hot som kan orsakas av användare som använder systemet, skadan kan ske genom att användare använder systemet på ett felaktigt sätt.

Detta arbete fokuserar främst på mänskliga hot. Ett exempel är att anställda av någon anledning inte gör det de är tillsagda att göra. Anledningen till varför de inte gör det de är tillsagda att göra kan vara att de helt enkelt inte vet hur de ska göra. Det kan också bero på att de själva valt att inte göra uppgiften av olika skäl, som exempelvis att de tycker att det är jobbigt att utföra uppgiften eller att de inte tror att de klarar av uppgiften och väljer därför att inte utsätta sig för den. Det är därför viktigt med en strategi för att studera efterlevnaden.

Denna undersökning genomförs med hjälp av en litteraturstudie för att ta fram en strategi för att studera efterlevnad samt en fallstudie för att validera strategin. I fallstudien görs först en kvalitativ intervjuundersökning för att ta reda på mer om företagets säkerhetspolicy och vad den innehåller. Efter det görs en enkätundersökning för att ta reda på hur de anställda på företag efterlever den policy som företaget har valt att använda för att skydda sin verksamhet.

I kapitel 2 beskrivs bakgrunden till arbetet, där tas centrala begrepp upp som är relaterat till ämnet som arbetet handlar om, nämligen informationssäkerhet. I detta kapitel beskrivs även olika hot mot företags information, samt ett scenario till varje hot för att läsaren lättare ska förstå hur attacken utförs och vilken skada den kan orsaka. I kapitel 3 beskrivs det problem som detta arbete presenterar. I kapitel 4 beskrivs metoden som används för att svara på de frågeställningar som arbetet består av. Genomförandet av undersökningen presenteras i kapitel 5 och resultatet presenteras i kapitel 6. Kapitel 7 består av relaterad forskning där liknande forskning beskrivs. I kapitel 8 presenteras en analys baserat på de resultat som presenterades i kapitel 6. Slutsatsen presenteras sist i kapitel 9.

2 Bakgrund

Detta kapitel är till för att skapa en bakgrund till det här arbetet. Ämnesområdet för detta arbete är säkerhet med inriktning främst på informationssäkerheten. Det ges även förklaringar till centrala begrepp inom ämnet.

2.1 Säkerhet

Ordet säkerhet används på olika sätt i det dagliga livet idag, säkerhet i hemmet i form av säkerhetssystem som skyddar våra hus när vi inte är hemma. Det finns också säkerhet i våra banker så att våra pengar som finns där är säkra, både internetbanker och vanliga banker har säkerhetssystem som skyddar våra ekonomiska tillgångar mot personer som saknar rättigheter att ta ut pengar från våra personliga bankkonton.

När det talas om datorsäkerhet så menar Pfleeger och Pfleeger (2006, S. 10) att det talas om tre viktiga aspekter: Sekretess, integritet och tillgänglighet.

2.1.1 Sekretess (*Confidentiality*)

Sekretess ser till att datoriserade tillgångar endast är tillgängliga för behöriga personer, med andra ord får endast behöriga personer tillgång till dem. Bendej (2006) skriver att känslig information inte får avslöjas till obehöriga som inte har rättigheter att se informationen. Sekretess kan även gälla oavsiktliga händelser där obehöriga personer råkar få syn på informationen, detta kan hända på arbetsplatsen när exempelvis en datorskärm är synlig för andra personer som inte har rättigheter att se informationen på skärmen. Det kan även ske vid en skrivare, personer som inte har rättigheter får syn på ett papper som nyss skrivits ut.

Att skapa sekretess skriver Pfleeger och Pfleeger (2006, S. 10) kan visa sig vara en svår uppgift, vem bestämmer vilka personer som ska ha behörighet till systemet? De som får rättigheter, ska de få tillgång till hela systemet eller ska de enbart få tillgång till delar av systemet?

2.1.2 Integritet (*Integrity*)

Pfleeger och Pfleeger (2006, S. 10) skriver att integritet försäkrar att de datoriserade tillgångarna endast kan modifieras av personer som har rättigheter till tillgångarna eller att de enbart kan modifieras på rätt sätt. Modifiering i detta sammanhang betyder skriva, ändra, ta bort eller skapa.

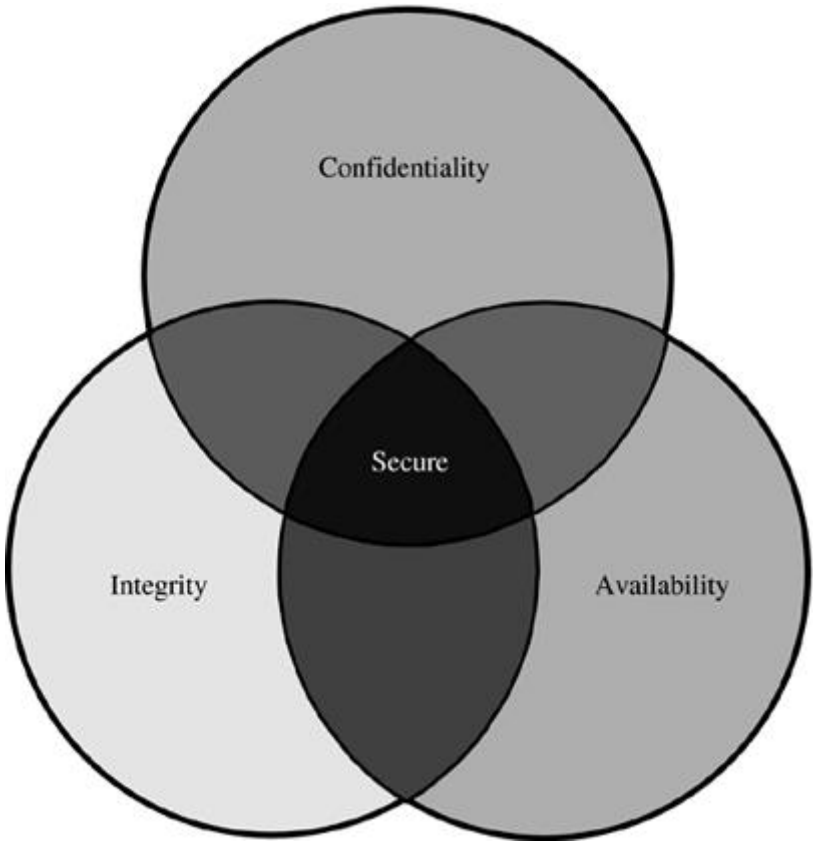
Att data är riktig innebär att informationen är korrekt, aktuell och presenteras rätt. Om integritet går förlorad kan det leda till att integriteten i användares data och andra IT-resurser försvinner. Förlorad integritet kan orsakas genom att data ändras, tas bort eller läggs till (Bendej, 2006).

2.1.3 Tillgänglighet (*Availability*)

Tillgänglighet gäller både data och tjänster och betyder att tillgångar (både information och resurser) ska vara åtkomligt för behöriga personer. Enligt Pfleeger och Pfleeger (2006, S. 10) är tillgänglighet att bara behöriga personer har åtkomst till tillgångar under en önskad tid. Ett exempel på förlust av tillgänglighet är driftavbrott.

Det är en känd attackmetod att neka någon tillgång till resurser, nämligen *denial of service* (DoS).

Dessa är enligt Pfleeger och Pfleeger (2006, S. 10) de tre målen som datorsäkerhet strävar efter, svårigheten med att skapa ett säkert system är att hitta den rätta balansen mellan dessa tre målen. Det är enkelt att bevara sekretessen av data i ett säkert system, helt enkelt genom att förhindra alla från att få tillgång till data. Problemet som följer då är att tillgängligheten går förlorad och ingen person har tillgång till den data som de ska ha tillgång till. Det vill till att hitta den rätta balansen mellan sekretess, integritet och tillgänglighet. Blir det för mycket av någon del så kan de andra två delarna förloras och blir det för lite av en del så förloras den delen. Blir det för lite av alla tre delarna så är inte systemet tillräckligt säkert. Figur 1 nedan visar relationen mellan de tre målen: Sekretess, integritet och tillgänglighet.



Figur 1: Relationen mellan Sekretess, Integritet och Tillgänglighet, från Pfleeger och Pfleeger (2006, sid. 11)

2.2 Informationssäkerhet

Information är en viktig tillgång för företag och andra verksamheter, det är viktigt att organisationer kan överföra information till samtliga parter som ska ha tillgång till informationen på ett säkert sätt. Det är även viktigt för företaget att de anställda inte förser utomstående med information som de inte har rättigheter till. Detta betyder att informationen måste skyddas mot olika hot.

Informationssäkerhet har länge ansetts vara endast kostnader för verksamheter. På senare tid när verksamheter blivit mer beroende av datorer och annan teknik för att utföra sina uppgifter blir informationssäkerhet en allt mer viktig faktor för att verksamheten ska fungera på ett bra sätt (Lundmark och Palm 2003).

Användares syn på säkerhet i arbetet är ofta att det är som ett hinder för dem (Lundmark och Palm 2003). Om deras kunskaper om säkerhet inte är tillräckligt bra och de inte vet hur de ska bete sig på ett säkert sätt så hjälper inga tekniska säkerhetslösningar för att göra systemet säkert, inte om de inte kan hantera dem på ett korrekt sätt. Detta får talesättet "En kedja är inte starkare än sin svagaste länk" att stämma väl.

Informationssäkerhet är en effekt av åtgärder som vidtagits för att förhindra att ett hot ska inträffa, ett hot kan exempelvis vara att information läcker ut, tappas bort, förstörs av misstag eller med avsikt, ändras samt se till att informationen är tillgänglig när den behövs. Ett hot mot ett datorsystem är enligt Pfleeger och Pfleeger (2006, S. 6) en händelse eller en rad händelser som kan orsaka förlust eller skada till systemet.

Informationen som ska skyddas kan vara tryckt på papper, vara lagrad elektroniskt, den kan överföras fysiskt (med post) eller med elektroniska medel (e-post), informationen kan även visas på film eller talas om i en konversation.

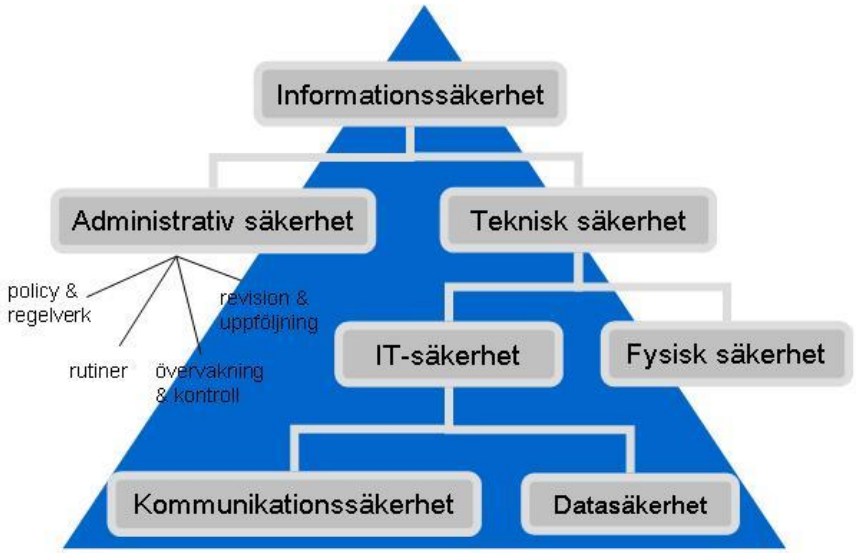
För ett företag kan det exempelvis handla om att skydda information mot att användare råkar tappa bort information eller råkar förstöra den. Det kan också handla om att användare med avsikt förstör eller ger ut information till exempelvis konkurrenter. Informationssäkerhet kan också handla om att skydda information mot mer tekniska och fysiska attacker till exempel stöld, intrång och förstörelse av tillgångar och information.

Informationssäkerhet kan delas upp i två kategorier: Administrativ säkerhet och teknisk säkerhet som figur 2 visar nedan.

Administrativ säkerhet
I sektionen administrativ säkerhet behandlas de administrativa delarna av informationssäkerheten så som policy och rutiner, hur arbetet ska göras och vilka regler som gäller. I den här sektionen ansvarar främst människor för att säkerheten i ett system ska vara intakt. Bryter en person mot en policy eller en rutin kan det leda till att systemet inte längre är säkert.

Teknisk säkerhet
I sektionen teknisk säkerhet handlar det om IT-säkerhet och fysisk säkerhet, de mer tekniska och fysiska delarna av informationssäkerheten. I sektionen fysisk säkerhet bestäms till exempel vilken autentiseringsmekanism som ska användas för att anställda eller användare ska kunna komma in på området eller till ett specifikt rum. I sektionen IT-säkerhet handlar

det om säkerheten som berör kommunikationen av data och datasäkerhet så som kryptering och säkra uppkopplingar.



Figur 2: Modell av Informationssäkerhet, från Landstinget Kronoberg (2012).

2.3 Typer av hot

Ett hot är som beskrivet tidigare en händelse eller en rad händelser som kan orsaka förlust eller skada för verksamheten. Bengtsson och Ollsson (2003) skriver i sin rapport om tre olika kategorier av hot som kan ge förluster eller skada för verksamheten.

2.3.1 Fysiska hot

Fysiska hot är möjliga skador på fysiska (synliga) ting, som exempelvis hårddiskar, hela datorer, skärmar, skrivare, CD-skivor eller USB-minnen. Händelserna kan vara allt från inbrott till brand, det kan vara översvämning eller avsiktlig förstörelse. Om något av detta händer är det redan för sent att rädda hårdvaran, skadan är redan skedd. Informationen som finns lagrad på hårdvaran kan räddas om det finns säkerhetsrutiner så som dagliga säkerhetskopieringar som görs varje natt. Säkerhetskopieringen bör lagras på en annan plats, om en brand skulle inträffa och både informationen som finns i systemet och informationen som säkerhetskopierats går förlorad i branden så har säkerhetsåtgärden varit för inget.

2.3.2 Logiska hot

Logiska hot kan leda till skador som inträffat på grund av att obehöriga användare har fått tillgång och loggar in på en annan persons konto, det kan även vara hindrande av tjänst, hit räknas *denial of service* (*DoS*) som kort beskrevs tidigare. Ett logiskt hot kan även vara manipulering av information.

2.3.3 Mänskliga/organisatoriska hot

Det räcker inte med att ha den senaste tekniken och den senaste säkerhetsutrustningen för att ett företag ska vara säkert mot attacker som exempelvis virus och intrång. Användare kan även trots den tekniska säkerheten förstöra den säkra väggen som säkerhetsutrustningen byggt upp enbart genom en knapptryckning. För att undvika detta hot gäller det att hålla alla användare uppdaterade och utbildade.

Enligt Nohlberg (2007) riktar ofta attackeraren in sig på personer som kanske saknar kunskaper om säkerheten på ett företag. Detta betyder att ju mer anställda vet om säkerhet och olika hot ett företag kan utsättas för, ju säkrare blir företagets information samt att det leder till att det är svårare för en attackerare att komma åt informationen.

2.4 Informationssäkerhetspolicy

En informationssäkerhetspolicy är enligt Al-Hamdani och Dixie (2009) en policy som organisationer använder sig av för att beskriva hur de tänkt skydda organisationens tillgångar. Lundmark och Palm (2003) skriver att en informationssäkerhetspolicy är ledningens syn på informationssäkerhet. Det är viktigt att policyn förklarar de skyldigheter som alla personer som använder systemet har. Al-Hamdani och Dixie (2009) skriver om innehållet i en informationssäkerhetspolicy och beskriver några exempel, dessa är:

- Hur åtkomst till datorsystem beviljas.
- Hur ordentlig användning av datorsystem sker.
- Hur man ska agera vid en säkerhetsincident.
- Vilka lagar och regler gäller.

En policy ses ofta som en riktlinje enligt Al-Hamdani och Dixie (2009). Lundmark och Palm (2003) skriver att en policy ska beskriva målet med företagets säkerhetsarbete från ledningens sida. I policyn ska det även motiveras vilken typ och vilken grad av säkerhet som organisationen behöver och varför den säkerheten behövs.

2.5 Attackerare

Pfleeger och Pfleeger (2006, S. 7) skriver att en attack sker när en människa eller ett program utnyttjar ett systems svagheter och utför attacken. En attackerare måste ha dessa tre saker för att utföra en attack:

- **Metod**: Han eller hon måste ha rätt kunskaper och verktyg för att utföra attacken.
- **Möjlighet**: Attackeraren måste ha tillräckligt med tid och möjlighet för att kunna utföra och lyckas med attacken.
- **Motiv**: Det måste finnas en anledning till att attackeraren utför en attack mot systemet.

Om någon av dessa tre faktorer saknas för en attackerare som planerar att utföra en attack mot ett system så inträffar aldrig attacken (Pfleeger och Pfleeger, 2006, S. 8). De skriver också att det inte är lätt att ta bort någon av dessa faktorer.

Nohlberg (2007) skriver att få möjligheten att utföra en attack i dagens samhälle är relativt enkelt eftersom flertalet av dagens system har tillgång till Internet. Detta gör att attackerare får en möjlighet att ta sig in i systemet.

Enligt Pfleeger och Pfleeger (2006, S. 399-403) kan motiven skiljas åt, en angripare kan utföra en attack för att han eller hon vill ha en utmaning, det kan liknas med att klättra ett berg eller andra extremsporter. En angripare kan även utföra en attack eftersom han eller hon vill få berömmelse för den utförda attacken. Pengar och spionage är ett annat motiv för att utföra en attack. Personen som utför attacken kan ingå i en grupp som sysslar med organiserad brottslighet och de vill att han eller hon ska utföra attacken.

Olika typer av attackerare

I sin rapport skriver Nohlberg (2007) om olika typer av attackerare, det som skiljer dem åt är vilka mål de har med attacken. De olika typerna översätts inte till svenska då det kan skapas misstolkningar i översättningen.

- The Novice: Personer som har begränsade kunskaperna för att skapa egna program för att utföra attacker. Kallas ofta för Script Kiddies
- The Cyber Punk: Dessa personer har lite högre kunskaper, är ofta unga män och riktar in sig på högt uppsatta mål. Det är inte ovanligt att de har kommit i kontakt med vandalism tidigare.
- The Internal: Personer som använder sin åtkomst i exempelvis ett företag för att öka sin ekonomi eller för att straffa företaget genom att hämnas om de känner att de blivit dåligt behandlade.
- The Pretty Thief: Attackerare som börjar som vanliga tjuvar och som sedan lär sig att använda teknologi för att förbättra sin ekonomi. Dessa personer har begränsade färdigheter till en början när det gäller teknologin som används, men blir skickligare ju längre tiden går.

- The Old Guard: Denna typ av attackerare ser hackning som en utmaning och är nyfiken. Dessa personer är ofta skickliga och saknar kriminell avsikt, de delar förmodligen med sig av sin information.

- The Professional Criminal: Personer som är skickligare än tidigare nämnda typer, kanske till och med före detta spioner som använder sina färdigheter för att öka sin ekonomi. Dessa personer arbetar ofta för en grupp inom organiserad brottslighet och blir sällan påkomna.

- The Information Warrior: Attackerare som är motiverade av sin patriotism och de använder sina kunskaper och färdigheter för att förstöra för ett annat land.

Hur utför en attackerare sin attack? De sätter sig inte ner vid en dator och påbörjar en attack som man får se i TV serier och filmer där de på några sekunder tar sig in i systemet och kan få den information som de är ute efter. En smart attackerare planerar sin attack, undersöker systemet som han eller hon ska attackera. På samma sätt som en bankrånare undersöker den bank som han eller hon ska råna, kollar vart säkerhetskamerorna finns, om det finns några andra säkerhetsmekanismer och hur många säkerhetsvakter som banken har (Pfleeger och Pfleeger, 2006, S. 404).

2.6 Social engineering

Roßling och Muller (2009) skriver att social engineering är konsten att manipulera människor till att utföra handlingar eller ge ut viktig information. Nohlberg (2007) skriver att social engineering är en teknik där en obehörig person lyckas utge sig för att vara en person som har behörighet och på så sätt få tag i information eller resurser. Sasse och Flechais (2005) skriver att den berömde hackaren Kevin Mitnick avslöjade att han sällan behövde knäcka någons lösenord, han upptäckte att det var lättare att lura personer att ge honom sitt lösenord genom en rad olika *social engineering* tekniker.

Thornburgh (2004) skriver om en något överdriven men ändå en grundläggande struktur av en social engineering attack:

"Hej! Jag är någon du kan lita på och jag låter som om jag vet vad jag pratar om. Jag jobbar på någonting som du troligen inte vet något om. Därför behöver jag få lite information från dig som du normalt sett inte ger ut till främlingar, men som sagt, du kan lita på mig!".

Pfleeger och Pfleeger (2006, S. 405-406) skriver att meningen med en social engineering attack är att få offret att hjälpa attackeraren. Ofta utger sig angriparen för att vara någon inom företaget som har problem och är stressad så att offret inte ska kontrollera angriparens berättelse. Eftersom attackeraren efteråt tackar offret överdrivet så tror han eller hon att inget är fel och tänker inte mer på händelsen och berättar då inte heller för någon vad som hänt. Det kan gå lång tid innan skadan som skett efter en sådan händelse uppmärksammas.

2.7 Prokrastinering

Steel & Ferrari (2013) skriver att prokrastinering kan uppfattas som en form av självreglerande misslyckande där vi frivilligt skjuter upp en uppgift som måste göras trots att vi vet att det bara blir värre om vi skjuter upp den.

Steel (2007) menar att någon prokrastinerar när den personen skjuter upp början eller slutförandet av en planerad uppgift. Steel (2007) skriver även att det finns en positiv sida av prokrastinering, den positiva sidan av prokrastinering kan användas för att skjuta upp saker för att undvika stress. Denna sektion riktar främst in sig på prokrastineringens negativa sida.

Steel (2007) skriver att 80-95% av studenter på högskolenivå prokrastinerar, skjuter upp uppgifter för att göra något annat och 75% av studenterna anser sig själva som prokrastinerare. Bland vuxna skriver Steel (2007) att mellan 15-20% prokrastinerar och över 95% av alla prokrastinerare önskar att minska sin prokrastination.

Varför prokrastinerar människor? Steel (2007) skriver om några orsaker till varför människor prokrastinerar:

2.7.1 Uppgiftens karaktär

Det kan vara en uppgift som en person tycker är mindre jobbig att utföra och väljer att utföra den istället (Steel, 2007). Två orsaker till varför personer väljer bort en uppgift förklaras nedan.

Tajmingen av belöningen och straffet

Steel (2007) skriver att ju längre ifrån en händelse är ju mindre verkan har den på människors beslut. Eftersom deadlinen för en uppgift är så långt borta väger straffet att förlora tid till att utföra uppgiften mindre än belöningen att göra vad man vill för tillfället.

Avsky till uppgiften

Steel (2007) syftar på händelser och uppgifter som personen tycker är otrevliga. Personer vill gärna undvika otrevligheter och ju otrevligare en situation är ju större risk är det att den skjuts upp eller undviks (prokrastinering). Hur mycket en person ogillar en uppgift kan även handla om personliga egenskaper såsom uttråkad, lat eller avsaknad av motivation.

2.7.2 Individuella karaktärsdrag

Prokrastinering kan också bero på prokrastinerares personligheter och hur de är som personer.

Neuroticism

Tro att man är otillräcklig för uppgiften och tro att omgivningen är för svår och krävande. Rädsla för misslyckande, lågt självförtroende, tvivla på sin förmåga att göra bra ifrån sig. När personen misslyckas med en uppgift så tror de att det tyder på att de är otillräckliga som personer. Vid en svår uppgift, för att skydda sitt självförtroende så hittar personen en orsak till att skjuta upp eller undvika uppgiften.

Ovänlighet
Steel (2007) skriver att de största motiveringarna till prokrastinering är trotsighet, fientlighet och ovänlighet. Människor med de karaktärsdragen är mer troliga att prokrastinera.

Extraversion
Steel (2007) skriver att de personer som är extroverta beskrivs ofta som sociala, optimistiska, utåtriktade, energiska, uttrycksfulla och impulsiva. Det är mer troligt att impulsiva personer prokrastinerar eftersom de lever i nuet och de gör det som de vill för tillfället och tankar om framtiden väger inte lika tungt som de begär som de har just då.

Skötsamhet
Prokrastinering ska enligt Steel (2007) associeras med distraktion, dålig organisation och låg motivation att prestera. Med distraktion menas att personer lätt får tankar på annat än den uppgiften som de ska utföra. Organisation syftar på ordning och reda, att planera sitt dagliga liv och sätta upp mål. Personer med motivation att prestera sätter mål för sig själva och uppskattar ofta att prestera.

En anställd på ett företag kan prokrastinera genom att välja att inte följa en säkerhetspolicy av olika anledningar. Dessa anledningar kan vara att de anställde tycker att det är tidskrävande att följa policyn, han eller hon känner att risken att bli upptäckt är låg och belöningen att tjäna några minuter på att inte följa policyn är därför högre än straffet. Andra anledningar för att inte följa en policy kan vara lathet, att uppgiften är jobbig att utföra, den anställde kan ha hamnat i bråk med ledningen och vill därför hämnas genom att inte följa policyn osv.

3 Problem

I detta kapitel presenteras problemet, det börjar med en övergripande presentation av det problem som detta arbete ska försöka lösa. Det presenteras också ett syfte, motiv och några delmål med arbetet i detta kapitel samt en frågeställning, avgränsning och ett förväntat resultat.

3.1 Problemformulering

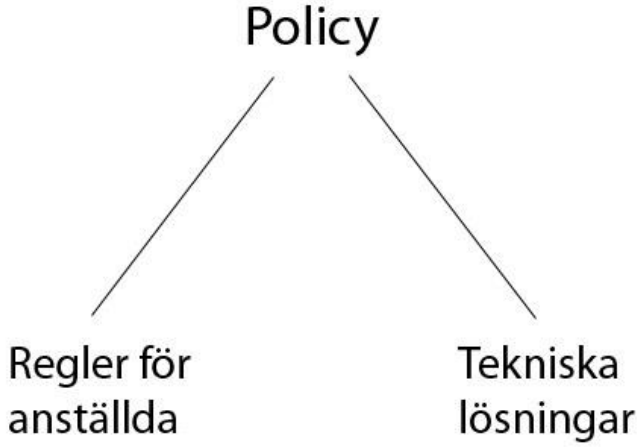
Det finns undersökningar som visar att säkerhetsbrister ofta beror på användarna. I Månssons (2011) undersökning uppdagades flera säkerhetsbrister. Flera av företagen i Månssons studie hävdade att dessa brister kunde kopplas till de anställdas kunskaper.

I Kapitel 2 beskrev Nohlberg (2007) att en attackerare ofta riktar in sig mot användare eller andra personer som saknar eller har begränsade kunskaper om informationssäkerhet. Sasse och Flechais (2005) skriver att den berömde hackaren Kevin Mitnick avslöjade att han sällan behövde knäcka någons lösenord, han upptäckte att det var lättare att lura personer att ge honom sitt lösenord genom en rad olika *social engineering* tekniker.

Sasse och Flechais (2005) skriver att Kevin Mitnick berättade att attackerare har varit bättre än säkerhetsdesigners på att ge uppmärksamhet till den mänskliga faktorn i säkerhet. Detta har gett dem en enorm fördel som de har kunnat utnyttja.

Eftersom attackerare ofta riktar sina attacker mot användare så försöker företagen skydda sig genom att ha regler beskrivna i sin informationssäkerhetspolicy för hur användarna får och inte får agera. En informationssäkerhetspolicy är enligt Al-Hamdani och Dixie (2009) en policy som organisationer använder för att beskriva hur de tänkt skydda organisationens tillgångar. Lundmark och Palm (2003) skriver att en policy ska beskriva målet med företagets säkerhetsarbete från ledningens sida. I säkerhetspolicyn ska det även motiveras vilken typ och vilken grad av säkerhet som organisationen behöver och varför den säkerheten behövs. Det är viktigt att anställda förstår säkerhetspolicyn så att de kan förstå varför säkerheten är viktig och hur de ska arbeta för att uppnå den säkerheten.

Aloul (2010) skriver att organisationer utökar sin användning av avancerade säkerhetsteknologier och tränar samtidigt sina säkerhetsexperter för att göra sin organisation så säker som möjligt. Mycket lite resurser används till att öka organisationens vanliga användares säkerhetsmedvetande, vilket gör att de blir den svagaste länken i organisationen.



Figur 3: Policy - Regler för anställda och tekniska lösningar

Ett stort problem när det gäller den mänskliga faktorn är att anställda ibland kan välja att inte följa de regler som ledningen har satt upp för sitt företag. Som figur 3 visar så består en policy av regler för de anställda och tekniska lösningar. För att få en fungerande policy krävs det att de regler och de tekniska lösningar som finns kompletterar varandra så att företaget blir säkrare. Om en anställd väljer att inte följa de regler som ledningen har satt upp eller om företaget har för få eller inga tekniska lösningar kan detta leda till säkerhetsbrister i företaget och företaget kan då bli sårbar för olika hot.

Det är därför viktigt att ha tekniska lösningar som kan hjälpa till att skydda företaget mot mänskliga fel. Dessa fel är svåra att undvika då det är vanligt att människor gör fel (Man är bara mänsklig). Det är vanligt att företag, utöver de regler som de sätter upp också inför dessa tekniska lösningar som på något sätt fångar upp och rättar till de fel som vi människor råkar göra. Ett exempel på en sådan teknisk lösning är en mekanism som automatisk loggar ut en anställd ur företagets system när han eller hon har varit inaktiv i exempelvis 15 minuter.

Att köpa och införa tekniska säkerhetslösningar betyder dock inte att systemet automatiskt får ökad säkerhet om användarna inte har tillräckligt hög säkerhetsmedvetande eller om de av något skäl skulle välja att inte följa policyn. Wang (2010) skriver att användare ibland väljer bort de säkerhetslösningar som finns tillgängliga, som exempelvis virusskydd eller kryptering av e-post. De kanske kopplar bort virusskyddet för att de tycker att det är störande, de kanske ger ut sina lösenord till personer för att de ska kunna logga in själva och fixa ett problem. Det finns teorier kring varför användare gör detta.

Sasse och Flechais (2005) skriver att användare väljer att inte använda säkerhetslösningar eftersom:

- De har problem att använda säkerhetsverktygen på ett korrekt sätt.
- De förstår inte att data, mjukvara och systemen är betydande för företagets verksamhet.
- De tror inte att deras tillgångar är i fara, de tror inte att just de ska bli attackerade.

- De förstår inte att deras beteende sätter tillgångarna i fara.

Andra orsaker kan vara att personer prokrastinerar när det gäller att använda säkerhetslösningar. I sektionen 2.7 beskrivs beteendet att skjuta upp eller undvika uppgifter. De regler som ledningen har satt upp kan vara svåra att följa, krångliga att följa eller vara tidskrävande och den anställde väljer istället att inte följa den regeln. Att personer prokrastinerar kan också bero på personliga egenskaper så som dåligt självförtroende, att de anställda inte tror att de är kapabla till att efterfölja de regler som satts upp eller att de har en rädsla för att misslyckas och väljer istället att inte följa de reglerna över huvudtaget. Det kan också bero på att de anställda ogillar företagets ledning och vill helt enkelt inte följa de reglerna som ledningen satt upp.

Det kan alltså finnas en mängd olika orsaker till att människor inte följer sitt företags säkerhetspolicy. För företag är det därför viktigt att skapa sig en bild av hur efterlevnaden av policyn är på företaget. Den kunskapen kan sedan användas för att ta fram åtgärder i form av utbildning eller tekniska lösningar som kan kompensera för de brister som upptäcks när det gäller efterlevnaden.

3.2 Motivering och Syfte

Detta arbete syftar till att undersöka hur bra efterlevnaden av en säkerhetspolicy är på företag och hur den eventuella bristen av efterlevnaden kan hanteras.

I sitt arbete skriver Månsson (2011) att det är intressant att göra en undersökning på hur bra de anställdas kunskaper är angående olika hot ett företags informationssystem kan utsättas för. Det är även intressant att undersöka hur de anställda på företaget ser på informationssäkerhetspolicyn, om de följer den eller om det finns ett gap mellan sättet som anställda idag beter sig på företaget rent säkerhetsmässigt och sättet som de enligt policyn ska betet sig på arbetsplatsen rent säkerhetsmässigt. Det är viktigt att undersöka detta eftersom det lätt kan ske misstag om människor inte vet hur de ska hantera information på ett sätt som företaget tycker är säkert. Om anställda inte hanterar informationen på ett säkert sätt så betyder det att företagets informationssäkerhet försämras och företaget blir mer sårbar för olika hot.

Det är viktigt att lösa det problem som arbetet presenterar eftersom flera anställda inte följer de regler som ledningen på ett företag har satt upp och det är vanligt att anställda inte använder de tekniska säkerhetslösningar som finns tillgängliga. Anledningen kan vara att de inte förstår varför de ska använda dem eller helt enkelt inte vet hur de ska användas. Om ledningen på företagen dessutom tror att de anställda följer deras regler för hur arbetet ska utföras och om de i själva verket inte gör det, så kan det skapa stora säkerhetsbrister i företaget. Det är därför viktigt att skapa en strategi för hur dessa skillnader mellan ledningen och anställda ska identifieras och hur de sedan ska hanteras.

3.3 Frågeställning

Detta arbete fokuserar på följande frågeställning:

- *Finns det någon skillnad mellan det sätt som företags säkerhetspolicy beskriver hur en anställd ska uppföra sig och hur de anställda idag faktiskt uppför sig?*
- *Hur väl fångar tekniska lösningarna upp de eventuella brister som finns?*

3.4 Delmål

För att besvara den frågeställning som detta arbete ställer har några delmål tagits fram:

- *Ta reda på hur olika informationssäkerhetspolicys ser ut.*
- *Undersöka efterlevnaden av säkerhetspolicys.*
- *Undersöka huruvida tekniska lösningar kan fånga upp de brister som finns.*
- *Validera den strategi som tas fram.*

3.5 Avgränsningar

Det här arbetet undersöker inte allt en säkerhetspolicy kan ta upp. Eftersom arbetet fokuserar på efterlevnaden av säkerhetspolicys så prioriteras de delar av en säkerhetspolicy som handlar om saker som personer kan välja att inte följa. Arbetet fokuserar alltså inte på delar av policys som är på företagsnivå. Ett exempel på en del i en policy som arbetet inte fokuserar på: "Säkerhet, kvalitet och miljötänkande skall genomsyra alla delar av IT-arbetet på [Företag]" (Vinci Energies 2009).

3.6 Förväntat resultat

Företag som denna undersökning utförs på blir förhoppningsvis mer medvetna om hur bra deras anställda efterlever den policy som företaget har infört och vill att de anställda ska följa. Eftersom de blir mer medvetna om de anställdas kunskaper om policyn så får de reda på om de behöver utbilda personalen ytterligare eller om de behöver skaffa sig fler tekniska säkerhetslösningar för att göra företaget säkrare och minska den eventuella säkerhetsrisk som deras anställda skapar.

Efter detta arbete blir företags anställda förhoppningsvis mer medvetna om att den säkerhetspolicy som företaget har valt är viktig för företaget och att det är viktigt att följa den policyn för att företaget ska kunna förbli säkert. Det förenklar arbetet för företagets administratörer och säkerhetsexperter när det gäller säkerheten eftersom företagets anställda blir mer medvetna om företagets policy och vilken vikt den har för företaget. Detta leder i sin tur till att anställda blir mer medvetna om olika hot mot företagets informationssäkerhet. Denna kunskap följer även med de anställda hem till deras egna hem vilket leder till att säkerheten hemma förbättras vilket gör att företagets laptops och smartphones som de anställda eventuellt är tillåtna att ta med hem efter arbetet blir säkrare.

4 Metod

I detta kapitel beskrivs de metoder som kan användas för att samla in data till undersökningen så att frågeställningen i kapitel 3.2 kan besvaras. Här beskrivs också vilket tillvägagångssätt som användas för att ta fram information inom problemområdet och besvara frågeställningen. Det diskuteras även om validitet och reliabilitet och källkritik.

4.1 Möjliga metoder för insamling av data

Att samla in data för att kunna utföra sin undersökning går att göra på flera olika sätt. De sätten som beskrivs nedan är de alternativ som undersökts och anses vara lämpliga inför detta arbete.

4.1.1 Kriterier för att välja metod

För att kunna välja vilka metoder som ska användas för att samla in information till undersökningen krävs kriterier. Kriterierna som krävs för metoderna inför detta arbete beskrivs nedan:

- Metoden ska vara användbar.
- Metoden ska kunna bidra med data till undersökningen.
- Metoden bör kunna genomföras på ett sätt som skapar så få problem som möjligt.
- Metoden ska inte vara för tidskrävande.
- Metoden ska vara rimlig att genomföra.

4.1.2 Fallstudie

En fallstudie är enligt Berndtsson et al. (2008, S. 62 - 63) ett projekt där ett fenomen undersöks mer ingående i ett naturligt tillstånd. Fallstudier involverar ofta ett begränsat antal fall. De fall som ska undersökas kan vara en organisation, en avdelning i organisationen, en grupp eller en specifik person på företaget. Eftersom det är en organisation som detta arbete utför sin undersökning på är en fallstudie av företaget en lämplig metod för att samla in data. En fallstudie görs på ett företag för att ta reda på hur säkerhetspolicyn på företaget följs. Det krävs fler metoder för att samla in data från anställda och säkerhetsexperter på företaget.

4.1.3 Litteraturstudie

Med litteraturundersökning menar Berndtsson et al. (2008, S. 58 - 60) en systematisk lösning av ett problem, lösningen sker genom att granska redan publicerade källor med ett specifikt syfte. Till detta arbete används litteraturstudie för att samla in data genom att kolla på tidigare gjorda policys och standardpolicys. Det valdes att använda främst vetenskapliga artiklar för att hämta informationen från eftersom innehållet i dem har en god kvalité. Tidigare gjorda intervjufrågor och enkätfrågor kontrolleras också för att se vad de innehåller så att frågorna till intervjun och enkäten ska bli så bra som möjligt.

4.1.4 Intervjuundersökning

I en intervjuundersökning ställs mer djupgående frågor i jämförelse mot enkätundersökningar, dessa tar längre tid att besvara och de ställs ofta till ett färre antal människor och företag i jämförelse mot enkätundersökningar. I en intervjuundersökning så ska frågorna vara öppna, det vill säga att personen som blir intervjuad ska kunna besvara frågorna med sina egna ord och frågorna ska inte vara ledande (Berndtsson et al. 2008, S. 60 - 62). Denna metod för att samla in data till undersökningen är lämplig eftersom det krävs mer djupgående frågor till en person som kan mycket om den policy som ska följas. En intervjuundersökning anses vara en kvalitativ undersökning eftersom det ger färre svar från färre personer och företag i jämförelse med en enkätundersökning.

4.1.5 Enkätundersökning

När det talas om en enkätundersökning så förknippas det med användningen av enklare frågor (Berndtsson et al. 2008, S.63). Enkätundersökningar används ofta när fler svar från flera olika människor krävs. Fördelen med enkätundersökningar är enligt Berndtsson et al. (2008) att det med lite resurser går att nå ut till människor och företag. Denna metod för att samla in data till undersökningen är lämplig eftersom undersökningen vill nå ut till anställda inom företaget och ta fram information om hur väl de följer policyn. En enkätundersökning anses vara en kvantitativ undersökning eftersom det ger svar från flera personer och företag i jämförelse med en intervjuundersökning.

4.1.6 Experiment

Ett experiment fokuserar enligt Berndtsson et al. (2008, S.65) på några få variabler och hur de påverkas under experimentets gång. Ett experiment används ofta för att bestämma om en hypotes stämmer eller inte. Det är möjligt att använda experiment som metod för att samla in data till detta arbete. Genom att utföra hot som är möjliga om en anställd inte följer företagets säkerhetspolicy och sedan se hur den anställde reagerar på hotet, om de agerar på rätt sätt eller fel sätt. Denna metod valdes inte därför att det är svårt att kontrollera experiment som inkluderar människor och det är svårt att få tillstånd att göra experimentet på ett företag på grund av säkerhetsrisker

4.2 Vald metod

En summering av de metoder som anses vara lämpliga för att svara på frågeställningen i sektion 3.3 beskrivs nedan.

För att få fram information om olika policys och hur intervjufrågor skrivs och även hur enkätfrågor skrivs så valdes metoden litteraturstudie.

En fallstudie valdes för att undersöka hur företags säkerhetspolicy efterföljs av anställda. Studien utförs på ett företag och dess anställda i ett naturlig tillstånd, d.v.s. arbetet på företaget fortgår utan störningar under undersökningens gång. I denna fallstudie används ytterligare två metoder som behövs för att samla in data och besvara frågeställningen, en intervjuundersökning och en enkätundersökning. Intervjuundersökningen ger data om säkerhetspolicyn hos företaget och enkätundersökningen ger data om efterlevnaden.

Eftersom undersökningen utförs genom en fallstudie på ett företag kan resultaten variera från företag till företag. Ett resultat som ett företag får ut kan skilja från det resultat som ett annat företag får ut med samma undersökning. Därför kan resultatet som undersökningen får inte användas som ett slutgiltigt övergripande resultat för framtida undersökningar inom

området. Däremot är strategin som tagits fram för att genomföra undersökningen generell och kan användas av andra företag eller organisationer för att undersöka hur väl policyn efterlevs hos dem.

I intervjuundersökningen intervjuas en person på företaget som är väl insatt i frågor om företagets informationssäkerhetspolicy. Under denna intervju ges det en stor möjlighet att få ut information om hur företaget vill att information ska behandlas på arbetsplatsen och hur företaget vill att anställda ska hantera informationen. Eftersom det är en kvalitativ undersökning av säkerhetspolicyn som krävs till en början så ansågs det lämpligast att börja med en intervjuundersökning för att få fram information om företagets informationssäkerhetspolicy.

För att sedan få fram information om hur anställda ser på och hur mycket de följer företagets informationssäkerhetspolicy så används metoden enkätundersökning där de anställda får svara på frågor som är baserade på svaren från intervjun om företagets informationssäkerhetspolicy. I denna enkätundersökning ställs också frågor om de anställdas säkerhetsvanor hemma i sitt eget hem. Eftersom det krävs flera svar från företagets anställda för att få en bra bild över hur anställda på företaget hanterar information så är en kvantitativ undersökning lämpligast för att få fram tillräckligt mycket data från anställda för att besvara frågeställningen.

4.3 Avgränsning

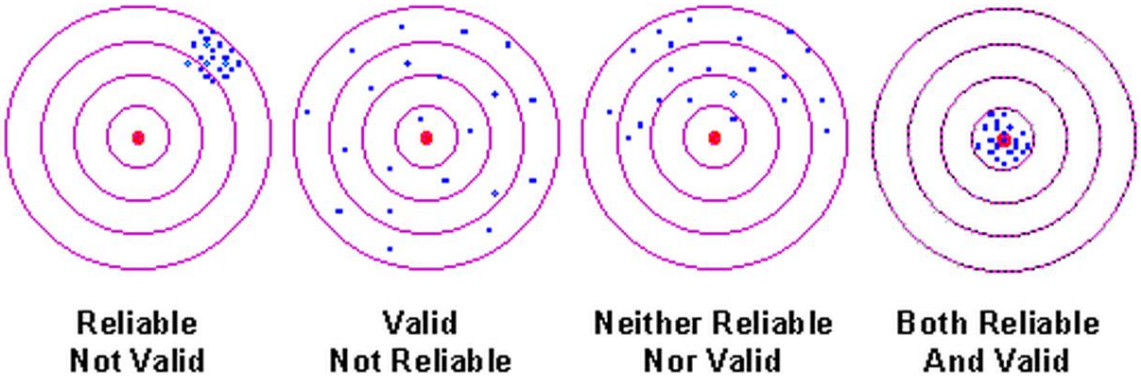
Detta arbete studerar inte alla möjliga policys som finns tillgängliga och det studerar inte heller alla tekniska lösningar på alla möjliga säkerhetsproblem. Eftersom undersökningen utförs med en fallstudie så innebär detta en avgränsning. De delar som är relevanta för fallstudien studeras och presenteras. Metoden för att få fram resultatet, med avseende på delmålen kan återanvändas och undersökningen kan göras på vilket företag som helst.

4.4 Reliabilitet och Validitet

Med reliabilitet avser noggrannheten i undersökningen och hanteringen av den data som samlades in. Det kan också avse hur pålitlig resultatet från undersökningen är. Det kan sägas att forskaren försöker göra undersökningen på ett felfritt sätt. Golafshani (2003) skriver om tre typer av reliabilitet när det handlar om kvantitativa undersökningar:

1. Huruvida de mätningar som görs upprepade gånger får samma resultat.
2. Stabiliteten av mätningarna över en längre tid.
3. Likheter i mätningarna under samma tidsperiod.

Med validitet menar Cook och Beckham (2006) att det beskriver om resultaten från den undersökning som utförts går att lita på och om de mäter de saker som det är tänkt att undersökningen ska mäta. Figur 4 nedan beskriver reliabilitet och validitet på ett mer bildligt sätt.



Figur 4: Reliabilitet och Validitet, från Trochim (2006).

Figur 4 består av 4 ringar, för att undersökningen ska vara valid och reliabel skall resultaten hamna i ring 4 (räknat från vänster). Genom att se till att resultaten inte hamnar i de två första ringarna kan det inte heller komma i ring nummer tre. För att inte hamna i ring nummer ett så handlar det om val av frågor, val av respondenter och för att inte hamna i ring nummer två handlar det om antalet respondenter, ju fler respondenter ju bättre blir resultatet.

De åtgärder som tagits för att resultaten inte ska hamna i ring nummer ett är att frågorna inte ska vara ledande och att frågorna ska ställas på ett korrekt sätt, både i intervjuundersökningen och i enkätundersökningen. För att säkerställa att rätt frågor ställs under intervjun och enkäten studeras en artikel om hur intervjufrågor och enkätfrågor ska ställas på ett korrekt sätt och att frågorna inte blir ledande på något sätt (Walonick, 2010). Handledaren till arbetet konsulteras också för att se att rätt frågor ställs. En ytterligare artikel studeras, denna handlar om prokrastinering och den studeras för att få en modell över hur människor fungerar (Steel, 2007).

För att resultaten inte ska hamna i ring nummer två används flera källor. Flera anställda från företaget får svara på enkätundersökningen så att det ska bli ett normaliserat och rättvist resultat.

Det kan visa sig vara svårt att få fram bra svar från de anställda som deltar i undersökningen eftersom de förmodligen vill visa sig från sin bästa sida. För att få så bra och pålitliga svar som möjligt så görs enkäten helt anonym, ledningen har då ingen möjlighet att se vem som svarade vad i enkäten och de anställda riskerar ingenting med att svara ärligt.

4.5 Källkritik

För den information som tas med i detta arbete ska vara relevant för området som arbetet behandlar och den ska även vara tidsmässigt relevant och inte vara för gammal. Informationen som tas med kontrolleras så att olika källor inte motsäger varandra.

5 Genomförande

I detta kapitel beskrivs hur arbetet har genomförts.

5.1 Litteraturstudie

I detta arbete samlades information om problemområdet in genom en litteraturstudie av flera publicerade arbeten från flera olika källor, både böcker och artiklar. Vetenskapliga artiklar studeras främst för att veta att innehållet och den fakta som hittas är av bra kvalitét.

Dessa arbeten togs fram genom sökningar i Högskolan i Skövdes Biblioteks databaser, framförallt databasen IEEE Xplore användes mest. Sökmotorerna Google Scholar och Google användes också för att hitta material till arbetet. Dessa källor studerades för att få fram information om olika hot mot ett företags information, men även andra centrala begrepp inom informationssäkerhet. Att använda sig av källor från olika arbeten är bra för att stärka den information och fakta som hittas.

Litteraturstudie används också för att ta reda på mer information om hur intervjufrågor och enkätfrågor ska ställas och att de ställs på ett korrekt sätt.

5.2 Fallstudie

Detta arbete utför sina undersökningar på ett företag, företaget vill vara anonymt eftersom de vill skydda sin verksamhet och sin information. De vill inte att deras eventuella svagheter ska bli kända för omvärlden. Därför kallas företaget i detta arbete helt enkelt "företaget". Fallstudien på företaget består av två undersökningar, en intervjuundersökning och en enkätundersökning.

5.2.1 Intervjuundersökning

Det beskrevs tidigare i sektion 4.2 Vald metod att en intervjuundersökning valdes som en av metoderna för att samla in data till undersökningen, detta för att få en djupare förståelse för den policy som finns på företaget. Det gjordes en intervju med en person på företaget, denna person skulle vara väl insatt i företagets säkerhetspolicy, detta för att han ska kunna svara på de djupa frågorna som ställs.

För att kunna ställa bra frågor till den personen om företagets säkerhetspolicy så studerades vissa delar av företagets egen säkerhetspolicy innan intervjun utfördes för att se inom vilka områden de har en policy. Även andra dokument om policys studerades för att göra frågorna bättre, bland annat flera mallar för säkerhetspolicys från SANS (SANS u.å.) och en artikel om prokrastinering (Steel, 2007). Handledaren till arbetet konsulterades också för att göra frågorna bättre och även se till att frågorna ställdes på ett rätt sätt och inte var ledande.

När frågorna ansågs vara färdiga utfördes intervjun, denna intervju gjordes på företagets område för att personen från företaget skulle känna sig bekväm och avslappnad så att han kunde tala mer öppet. Själva intervjun spelades in så att det var möjligt att lyssna på den flera gånger och intervjuaren tog även anteckningar under hela intervjun så att sammanfattningen av frågorna skulle bli så bra som möjligt. Innan intervjun hade mål satts upp för varje fråga så att intervjuaren visste exakt vad han ville ha ut från varje fråga och fortsatte att ställa frågor tills det målet som satts var uppfyllt. Under intervjun ställdes flera frågor inom varje

område i policyn och det ställdes även flera kontrollfrågor till personen från företaget så att det personen från företaget sade stämde.

Efter intervjun gjordes en sammanställning av intervjun baserat på inspelningen och anteckningarna som gjordes under intervjun. Sammanställningen skickades slutligen in till företaget så att de kunde kontrollera att företagets säkerhetspolicy tolkats rätt och korrigera eventuella missförstånd som skett under intervjuns gång. Den färdiga sammanställningen av intervjun kan ses i bilaga A.

5.2.2 Enkätundersökning

Sektion 4.2 beskriver att en enkätundersökning används för att samla in data till undersökningen, detta för att kunna nå ut till fler personer för att fråga hur de efterföljer företagets policy. Det är viktigt att nå ut till många personer så att fler svar fås tillbaka. På så sätt blir det slutliga resultatet en normaliserad bild över hur de anställda efterlever företagets policy.

För att enkätfrågorna skulle bli så bra som möjligt så lästes en artikel om hur enkätfrågor ska skrivas och vad man ska tänka på när man skriver enkätfrågor (Walonick 2010). Handledaren för arbetet konsulterades också för att göra frågorna så bra som möjligt och att de ställdes på ett korrekt sätt och att ledande frågor undveks. Frågorna som enkäten består av baserades på den intervju som gjordes tidigare och sammanfattningen av den. En artikel om prokrastinering lästes och användes också som material för att skapa enkätfrågorna (Steel, 2007). I enkäten ställdes det frågor om företagets policy och dess olika delar för att ta reda på om de anställda följer dem, i enkäten finns också kontrollfrågor som kontrollerar att de svarar samma alternativ på frågor som ställs annorlunda. Det ges även scenarier där de anställda får svara på hur de skulle reagera i den situationen. Dessa används för att kontrollera att de anställda skulle agera på samma sätt som de svarade i frågorna.

När alla frågorna till enkäten var klara skickades frågorna in till företaget så att deras ledning fick läsa dem och godkänna dem. När frågorna var godkända och klara så skapades enkäten med hjälp av Google Drives verktyg "Form". Detta verktyg valdes för att det var beprövat samt att det var lätt att sammanställa och se svaren. Dessutom var Form tillgängligt helt gratis till skillnad från liknande verktyg som man endast kunde använda ett begränsat antal gånger eller endast kunde göra ett visst antal frågor och skicka ut enkäten till ett begränsat antal personer och endast få svar från ett begränsat antal personer. Valet att göra enkäten över Internet gjordes dels för att företaget som undersökningen gjordes på har haft en bra svarsfrekvens på liknande undersökningar som gjorts tidigare samt att det är lättare att skicka ut enkäterna (endast en länk som skickas med). Det är dessutom lättare att nå ut till fler personer samt att det går snabbare att få svaren tillbaka till skillnad mot att personligen gå till företaget och dela ut enkäterna och sedan samla in dem igen. Att de anställda på företaget har erfarenhet av att göra liknande enkäter som skickats ut genom företaget gör att chanserna för att fler ska besvara enkäten förmodligen är högre eftersom de redan vet att de inte straffas för något som de svarar i enkäten eftersom den är anonym.

Det valdes att främst använda sig av frågor med svarsalternativ i enkäten eftersom enkäten då skulle gå snabbare att genomföra än om de anställda själva skulle få skriva i svaren. Det gör också att enkäten blir enklare att genomföra vilket kan göra att fler anställda väljer att göra enkäten. Att enkäten går fort att genomföra gör att fler anställda kan tänka sig att besvara enkäten och att enkäten kan ställas till fler personer på företaget vilket gör att det ökar chanserna till ett standardiserat svar från företagets anställda. För att fler personer

skulle svara på enkäten och att svaren som de anställda gav skulle bli så ärliga som möjligt gjordes enkäten helt anonym.

När enkäten var klar skickades den ut genom företagets säkerhetsexpert som intervjun gjordes med eftersom de anställda då litar mer på enkäten och på så sätt kunna få fler svar från fler personer. Den färdiga enkäten kan ses i bilaga B. Med det e-postmeddelandet som enkäten skickades ut i följde även ett personligt meddelande som beskrev enkäten och vad den handlade om, detta för att fler personer skulle vilja svara på enkäten. Detta meddelande kan läsas i Bilaga C.

Möjligheten att de anställda väljer att inte besvara enkäten finns. Enkäten är därför utformad så att så många som möjligt ska svara på den. Det utgås från modellen i sektion 2.7. Uppgiftens karaktär, att enkäten skulle ta lång tid att utföra eller att den anställde skulle avsky uppgiften. Enkäten är gjord på ett sätt så att den ska gå fort att genomföra, den svarande svarar främst med svarsalternativ vilket går snabbare att göra än om den svarande själv skulle få skriva svaren. Om den svarande skulle avsky uppgiften att svara på en enkät så är sannolikheten låg att denne utför enkäten.

När det handlar om individuella karaktärsdrag så kan den svarande tro att uppgiften är för svår att utföra. De anställda på företaget är vana vid att besvara enkäter över Internet och denna enkät består främst av svarsalternativ vilket gör den enkel att utföra. Den svarande kan också ha en personlighet som är trotsig, detta är svårt att göra någonting åt. Väljer den svarande att vara trotsig så är sannolikheten låg att han eller hon svarar på enkäten. Den svarande kan vara impulsiv. Detta har tänkts på genom att använda sig av svarsalternativ vilket gör att enkäten går fort att genomföra. Den anställde kan även ha en låg motivation för att utföra uppgiften. Detta har tänkts på genom att förutom göra enkäten enkel att genomföra och dessutom på ett sätt som gör att den går fort att genomföra, även skicka med ett meddelande med enkäten som förklarar vad enkäten handlar om och vad den anställde hjälper till med genom att svara på enkäten. Detta kan göra att motivationen för att utföra enkäten höjs. Att en person som svarar på enkäten skulle ha dålig självinsikt hanteras genom kontrollfrågor och scenarier.

5.3 Frågor

Enkäten delas upp i delar, den första delen är en generell del där den svarande får svara på frågor om kön, ålder, utbildningsnivå och antal år som de arbetat på företaget. Dessa frågor ställs för att det skapar en generell bild över personen och den data kan användas under analysen för att upptäcka korrelationer mellan de olika svarande.

De andra delarna enkäten är uppbyggd av är de olika områdena som företagets säkerhetspolicy består av. Nedan motiveras frågorna i de olika delarna.

5.3.1 Lösenord

Företagets system har satt en gräns för hur kort ett lösenord får vara (minst 7 tecken) samt att de har gjort så att användaren måste ha bokstäver och siffror i lösenordet. Det kan vara intressant att se om användaren anstränger sig för att hjälpa till att göra företagets system säkrare genom att välja ett längre lösenord eller väljer de att göra minsta möjliga. Det kan därför vara intressant att se hur många tecken de svarandes nuvarande lösenord har.

5.3.2 Skrivbord
Det står specifikt i företagets säkerhetspolicy att de anställda inte får lämna känslig information framme. Det är därför viktigt att ställa en fråga om det ifall de anställda tycker att det är jobbigt eller tidskrävande att plocka bort informationen, så de lämnar den framme. Det ges även ett scenario för att kontrollera att den svarande svarar samma på en fråga som är ställd på ett annat sätt.

5.3.3 Systemet
I säkerhetspolicyn står det att de anställda måste låsa datorn när de lämnar den. Därför ställs en fråga om det samt att ett scenario ges för att kontrollera om de anställda efterlever den policy som finns på företaget eller om de möjligtvis tycker att det är jobbigt att låsa datorn, det kan vara så att de helt enkelt glömmer av det.

5.3.4 Besökare
Anställda får enligt säkerhetspolicyn varken ta med sig besökare in på företagets område med sitt eget behörighetskort eller lämna besökare på området oövervakade. Det ställs frågor i enkäten om dessa samt att scenarier ges för att kontroller detta. Detta är viktigt att undersöka eftersom det finns en möjlighet att de anställda tycker att det är tidskrävande eller jobbigt att följa denna policy.

5.3.5 Mobila enheter
Enligt säkerhetspolicyn får de anställda inte låna ut sina arbetslaptops till sitt/sina barn. Det ges både ett scenario och en fråga ställs i enkäten för att kontrollera att de anställda inte lånar ut sina arbetslaptops. De anställda kan tro att risken att bli upptäckt är så låg att belöningen att hans/hennes barn får roligt är större än straffet. Det är därför viktigt att undersöka om de anställda följer denna policy.

5.3.6 Nätverk och Internet
I säkerhetspolicyn står det att de anställda inte får använda företagets nätverk eller Internet till något som inte är arbetsrelaterat. Frågor och kontrollfrågor ställs därför inom detta område för att kontrollera om de gör det. Detta är viktigt att undersöka eftersom anställda kan tycka att belöningen att exempelvis gå in på en rolig hemsida är högre än det eventuella straffet.

5.3.7 E-post
Det står i företagets säkerhetspolicy att de anställda inte får öppna e-post eller bilagor från avsändare de inte känner till och att de inte får klicka på okända länkar. Det kan vara så att anställda inte ser meningen med att följa denna policy och saknar därför motivation för att följa den. Därför är det viktigt att ställa frågor inom detta område för att kontrollera om de anställda följer policyn.

5.3.8 Fysisk säkerhet
Företagets anställda får enligt säkerhetspolicyn inte låna ut deras behörighetskort och inte heller släppa in någon annan på företagets område med sitt eget behörighetskort. I enkäten ställs frågor och scenarier ges på området för att kontrollera om de efterlever policyn. Detta är viktigt att undersöka eftersom de anställda kan tycka att det är tidskrävande att följa denna policy.

5.4 Sammanställning

De resultat som de anställda skickar in granskas och analyseras dels med de verktyg som ingår i Googles tjänst "Form". Där ses svaren från de anställda i grafer och det går lätt att urskilja vilka som svarade vad på frågorna i enkäten. Med hjälp av Form skapas ytterligare grafer i programmet Microsoft Office Excel.

Till sist undersöker även arbetet om det finns någon koppling mellan de olika deltagarna i undersökningen. Dessa kopplingar kan exempelvis vara liknande ålder, liknande uppgifter i arbetet eller om personerna är av samma kön, vilken utbildningsnivå de har, hur många år de arbetat på företaget och vilka tidigare arbeten de haft. Ett exempel kan vara att personer i en ålder svarade liknande på en fråga och personer i en annan ålder svarade på ett annat sätt eller att personer av samma kön svarar liknande osv.

6 Resultat

I detta kapitel presenteras undersökningens resultat.

Enkäten skickades ut till 80 personer som arbetar på IT-avdelningen på företaget. 45% av de personer som fått enkäten svarade på den (37 personer).

Av de som svarade på enkäten så är 19% kvinnor och 81% män. Åldern på de som svarade på enkäten varierade mellan 25år och 59 år och medelåldern på alla som svarade är ca. 42 år.

De tjänster som personerna som svarat har på det företaget som undersökningen utförts på är olika, nämligen: Application Developer, System Analyst, Application Support, Project Manager, Process & Method Specialist, Infrastructure Architect, Technical Architect, Software Architect, Administrator, Technician, System Developer, Product Manager, Business Analyst och Delivery Coordinator.

Vad gäller erfarenheten av arbetet (hur länge de jobbat på företaget) så har 75% av de personer som svarat på enkäten jobbat på företaget längre än 5 år, 3% har jobbat i 3 - 5 år, 14% har jobbat i 1 - 2 år och 8% av dem har jobbat på företaget i mindre än ett år.

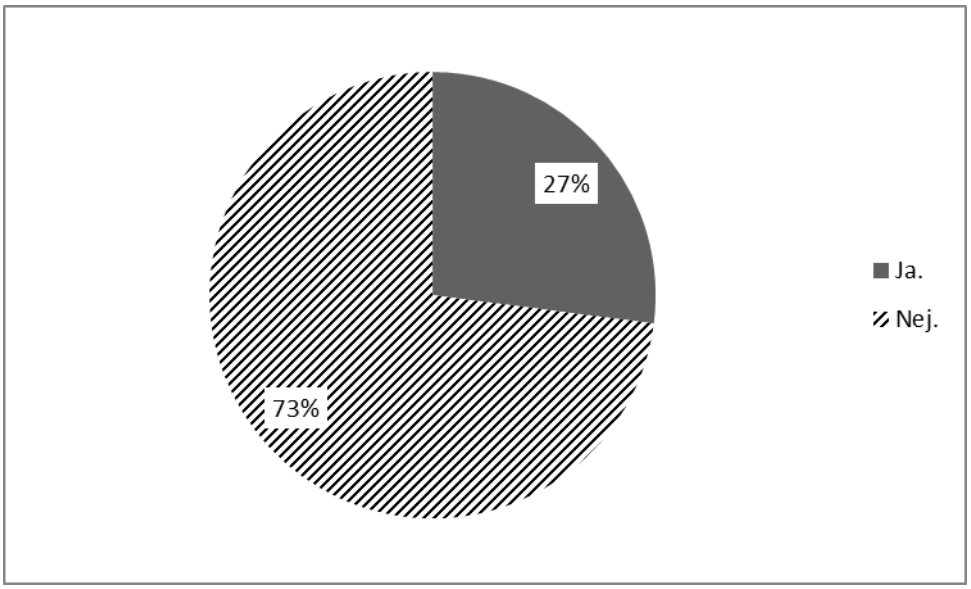
När det gäller de anställdas utbildning så svarade 78% att de hade en utbildning på högskolenivå/universitetsnivå. 19% av dem har en utbildning på gymnasienivå och 3% har en utbildning på grundskolenivå.

De anställdas svar på enkäten visar att 42% tidigare arbetat på företag med liknande säkerhetspolicys, 15% har arbetat på företag där de inte har några säkerhetspolicys alls, 20% svarade att de arbetat på företag som har mindre säkerhetspolicys än det företag de arbetar på nu och 10% svarade att de arbetat på företag med fler säkerhetspolicys. 13% av de som svarade på enkäten har inte haft något arbete tidigare eller att de innan detta arbete studerat.

Nedan följer några grafer som visar några av resultaten från enkätundersökningen som utfördes på ett företags anställda. Frågorna visas inte i den ordning som de ställdes, frågorna har istället delats in i de områden som de tillhör i säkerhetspolicyn så att läsaren kan få en bättre överblick över några av de frågor som ställdes från varje område.

6.1 Lösenord

De anställda på företaget fick svara på frågan "Hur många tecken har du i ditt nuvarande lösenord?" och de fick alternativen (1) 7-8 tecken och (2) fler tecken. På den frågan svarade 84% att de endast har 7-8 tecken i sitt nuvarande lösenord och 16% svarade att de hade fler tecken.



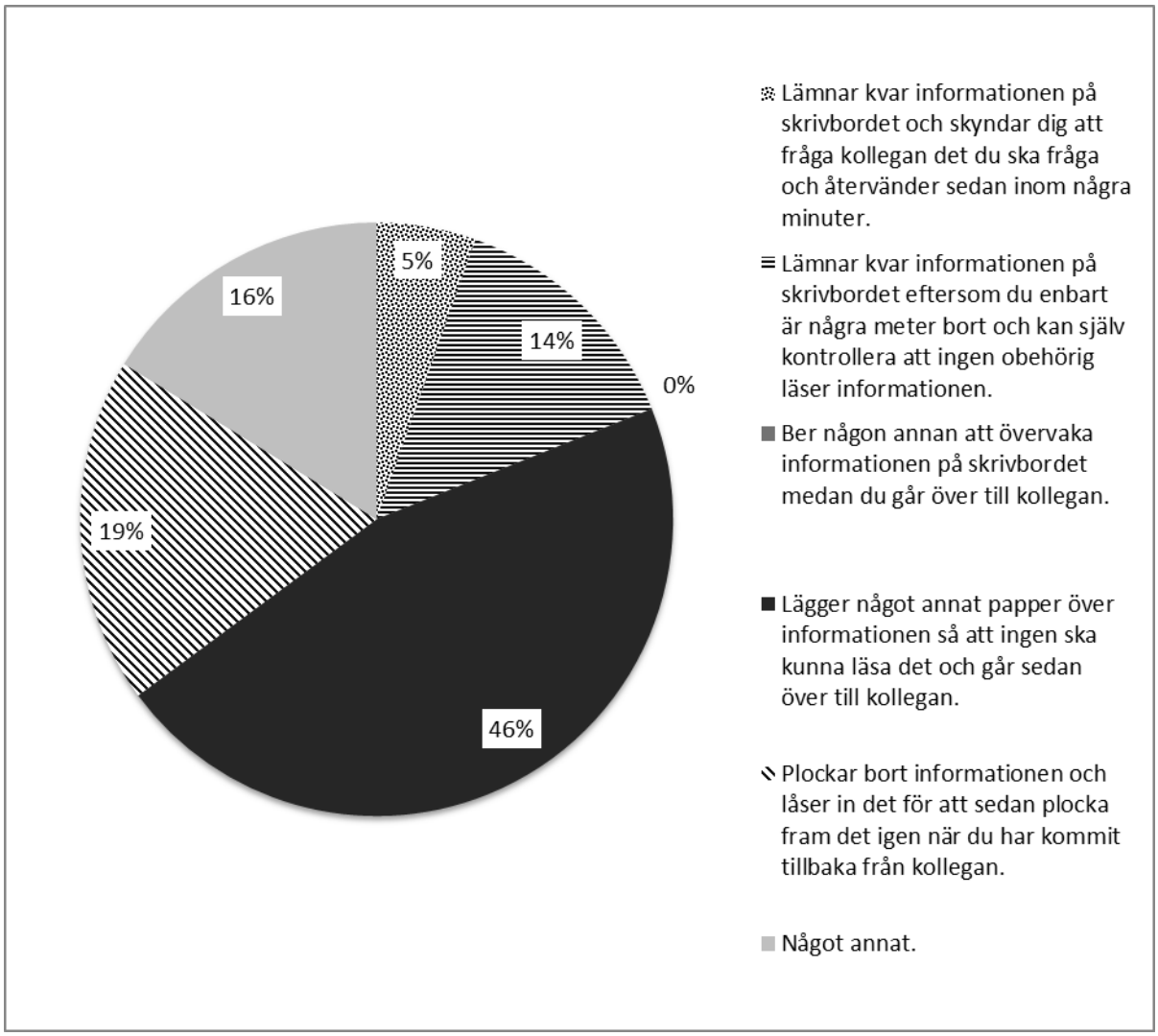
Figur 5: Har du någon gång delat med dig av ditt lösenord till någon person?

Frågan; "Har du någon gång delat med dig av ditt lösenord till någon" visas i figur 5 och de flesta svarade nej på den frågan. Företagets policy säger att lösenord inte får delas med andra, det ska endast innehavaren av lösenordet veta. I enkäten frågades även de anställda om någon arbetskollega någon gång hade berättat sitt lösenord för honom/henne. Svaren från den frågan var likt det som visas i figur 5.

6.2 Skrivbord

Enligt företagets policy får inte anställda lämna kvar känslig information på sitt skrivbord när de lämnar det. Företagets anställda fick därför frågan; "Har du någon gång lämnat känslig information på ditt skrivbord när du lämnat skrivbordet?" ställd till sig. På frågan finns 3 alternativ, (1) Ja, (2) Nej eller (3) Jag har aldrig hanterat känslig information. Resultatet av den frågan blev: 38% svarade att de aldrig hade hanterat känslig information, 54% svarade att de aldrig har lämnat någon känslig information på sitt skrivbord när de lämnat det. 8% svarade att de någon gång hade gjort det.

I enkäten fick de anställda även svara på scenarier där de ska föreställa sig situationen och välja det alternativ som bäst förklarar hur han eller hon skulle agera i den situationen. Ett scenario var att den anställda satt vid sitt skrivbord med känslig information och behövde sedan gå över till en kollega som satt ca. 15m bort och fråga en sak. Efter det ställdes frågan; "Vad gör du?". Figur 6 visar resultatet av den frågan.



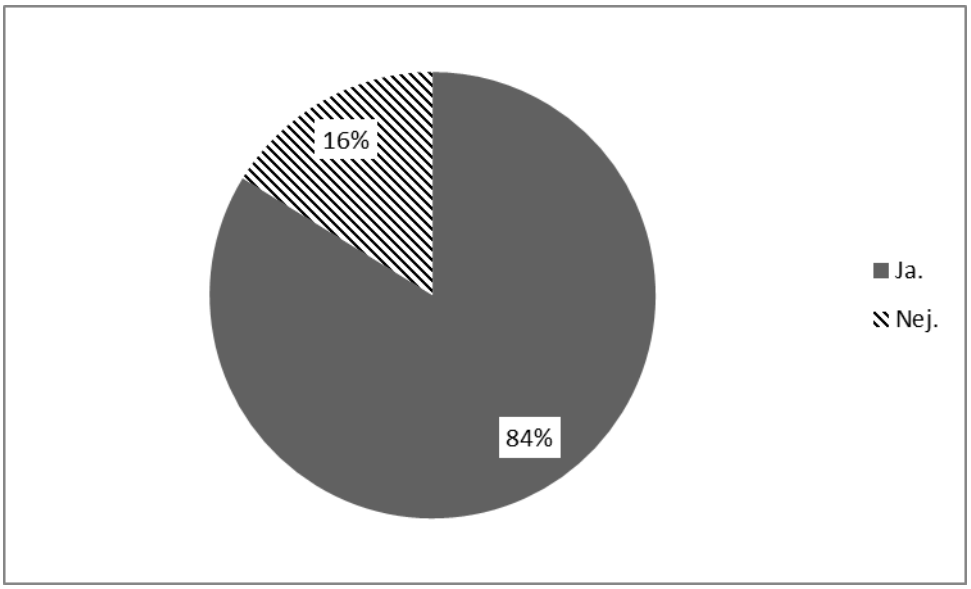
Figur 6: Scenario - Du sitter vid ditt skrivbord med känslig information och du ska gå över till en kollega och fråga en sak (kollegan sitter 10-20m bort). Vad gör du?

Enligt företagets policy så ska de anställda svara att de skulle plocka bort den känsliga informationen innan de går iväg från sitt skrivbord. Istället är det endast 19% av de anställda som svarade att de skulle agera på detta sättet och 65% svarade att de i någon form skulle lämna kvar den känsliga informationen på skrivbordet. 16% svarade att de skulle agera på något annat sätt än de alternativ som gavs.

6.3 Systemet

I företagets säkerhetspolicy står det att anställda måste låsa datorn när de lämnar den. Därför frågades de anställda frågan; "Låser du alltid din dator när du lämnar den?". Till frågan följer 2 st alternativ, ja och nej. Av de som svarade på enkäten svarade 78% att de alltid låser sin dator när de lämnar den och 22% svarade att de inte alltid gör det.

Ett scenario ges i enkäten där den svarande sitter vid sin dator och arbetar, plötsligt blir han eller hon törstig och går därför iväg för att hämta någonting att dricka. Den anställde vet att han eller hon enbart kommer vara borta i högst 5 minuter. Den svarande får sedan frågan; "Låser du din dator?". Resultatet på den frågan visas i figur 7.



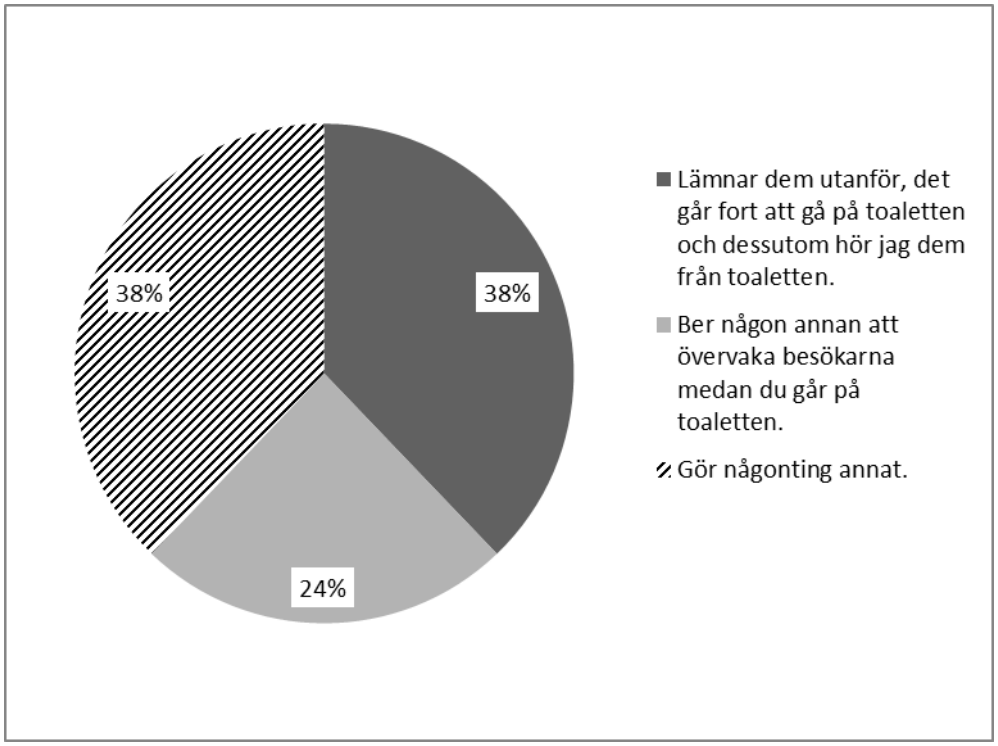
Figur 7: Scenario - Du sitter vid din dator och arbetar och kommer på att du är väldigt törstig och går iväg för att hämta någonting att dricka. Du vet att du enbart kommer vara borta i max 5 minuter. Låser du din dator?

Som figur 7 ovan visar så är det liknande resultat på scenariot och frågan och majoriteten av de som svarat på enkäten svarade att de alltid låser sin dator när de lämnar den. Enligt företagets policy ska de anställda alltid låsa sina datorer när de lämnar dem.

6.4 Besökare

Det står även i företagets säkerhetspolicy att de anställda inte får lämna besökare oövervakade. För att ta reda på det ställdes frågan; "Har du någon gång lämnat besökare oövervakade?". De alternativ som de svarande har att välja mellan är: (1) Ja, (2) Nej och (3) Jag har aldrig haft besökare. Resultaten från denna fråga blev: 32% svarade att de någon gång hade lämnat besökare oövervakade, 51% svarade att de inte hade gjort det och 16% svarade att de aldrig hade haft några besökare.

Ett scenario beskrevs i enkäten där den svarande hade med sig besökare in på företagets område och plötsligt behövde han eller hon gå på toaletten. Efter det ställdes frågan; "Vad gör du med besökarna?". Resultatet från den frågan visas i figur 8 nedan.

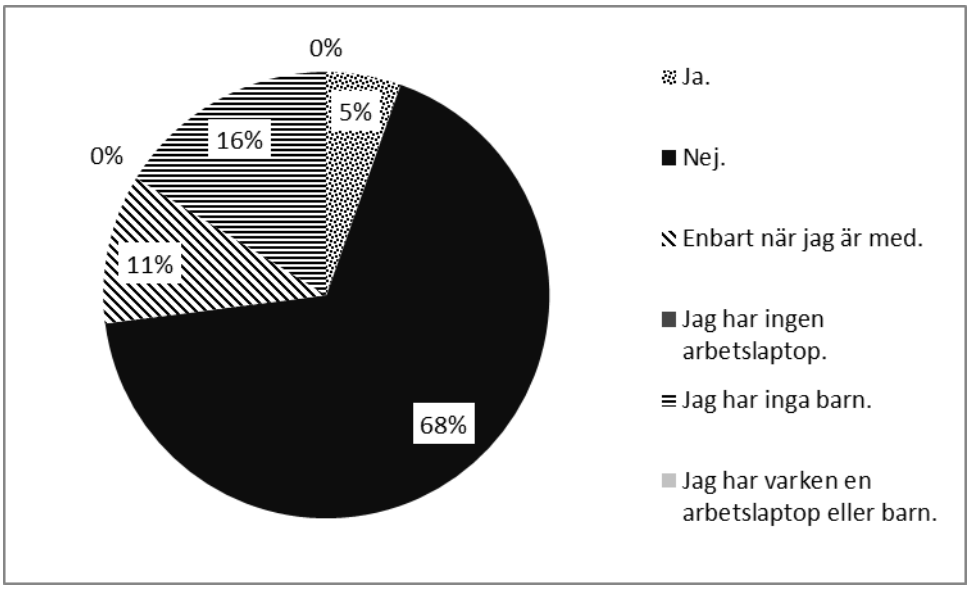


Figur 8: Scenario - Du har några besökare med dig inne på företagets område, plötsligt behöver du gå på toaletten. Vad gör du med besökarna?

Figur 8 ovan visar att 38% av de som svarade på enkäten skulle lämna besökarna utanför toaletten, oövervakade medan 24% skulle be någon annan att övervaka besökarna under tiden han eller hon gick på toaletten. 38% svarade att de skulle göra någonting annat än de alternativ som gavs.

6.5 Mobila enheter

I företagets säkerhetspolicy står det att de anställda inte får låna ut sina arbetslaptops till sina barn. För att kontrollera detta ställdes frågan; "Lånar du ut din arbetslaptop till ditt/dina barn?" och även ett scenario gavs där den svarandes barn kom fram till henne eller honom och frågade om att få låna arbetslaptopen. Resultatet från frågan visas nedan i figur 9.

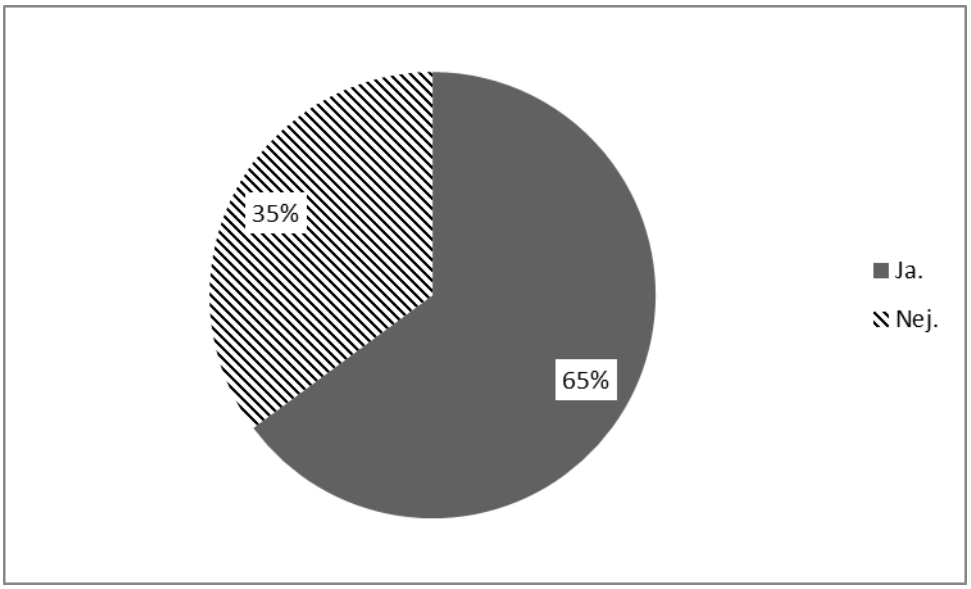


Figur 9: Lånar du ut din arbetslaptop till ditt/dina barn?

Figur 9 ovan visar att majoriteten av de som svarade på enkäten att de inte lånar ut sin arbetslaptop till sitt/sina barn. Resultaten från scenariot visade sig vara liknande de resultat som frågan resulterade i.

6.6 Nätverk

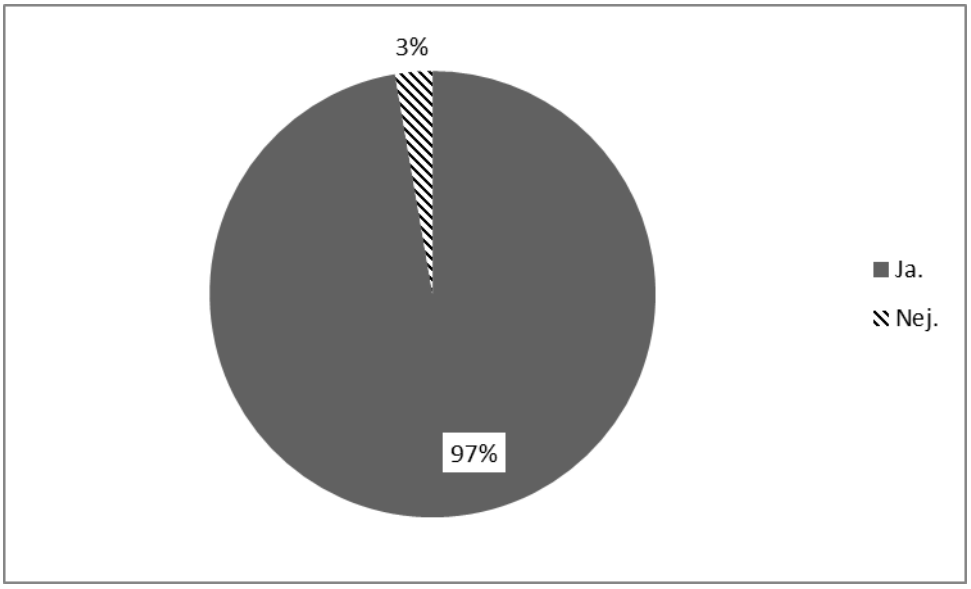
Företagets anställda får enligt säkerhetspolicyn inte använda företagets nätverk till något som inte är arbetsrelaterat. Frågan; "Har du någon gång använt företagets nätverk till något som inte är arbetsrelaterat?" ställdes till de svarande för att kontrollera att de inte gjorde det. De svarsalternativ som finns är antingen ja eller nej. Som figur 10 nedan visar så svarade 65% att de någon gång har använt företagets nätverk till något som inte är arbetsrelaterat och 35% svarade att de aldrig hade gjort det.



Figur 10: Har du någon gång använt företagets nätverk till något som inte är arbetsrelaterat?

6.7 Internet

Det står även i företagets säkerhetspolicy att de anställda inte heller får använda företagets Internet till något som inte är arbetsrelaterat. En fråga i enkäten besvarar om de gör detta. Frågan lyder; "Har du någon gång använt företagets Internet till något som inte är arbetsrelaterat?" och har 2 svarsalternativ. Ett av alternativen är ja och det andra nej. Figur 11 nedan visar resultaten från den frågan.

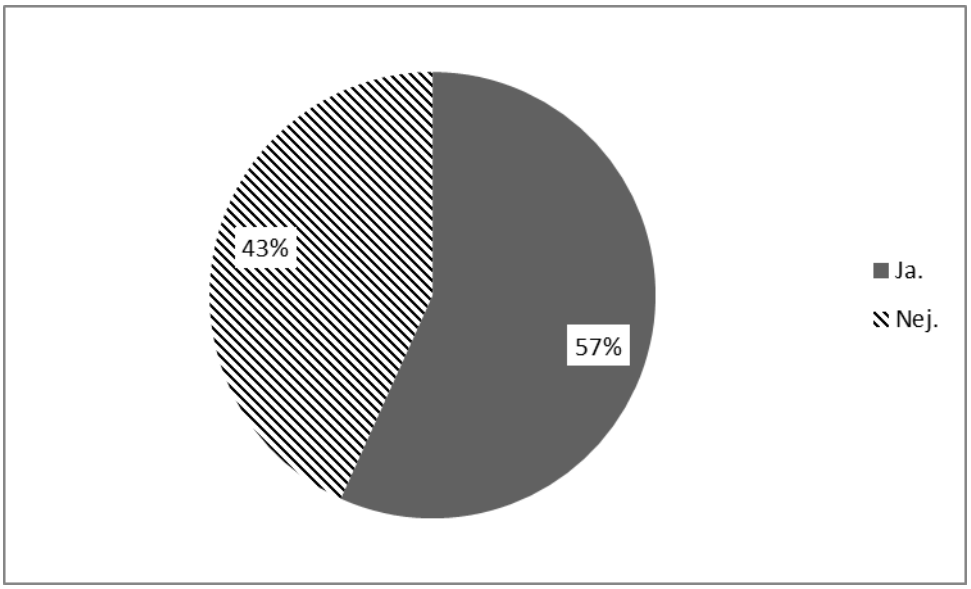


Figur 11: Har du någon gång använt företagets Internet till något som inte är arbetsrelaterat?

Som resultaten i figur 11 visar svarar flera att de någon gång har använt företagets Internet till något som inte är arbetsrelaterat.

6.8 E-post

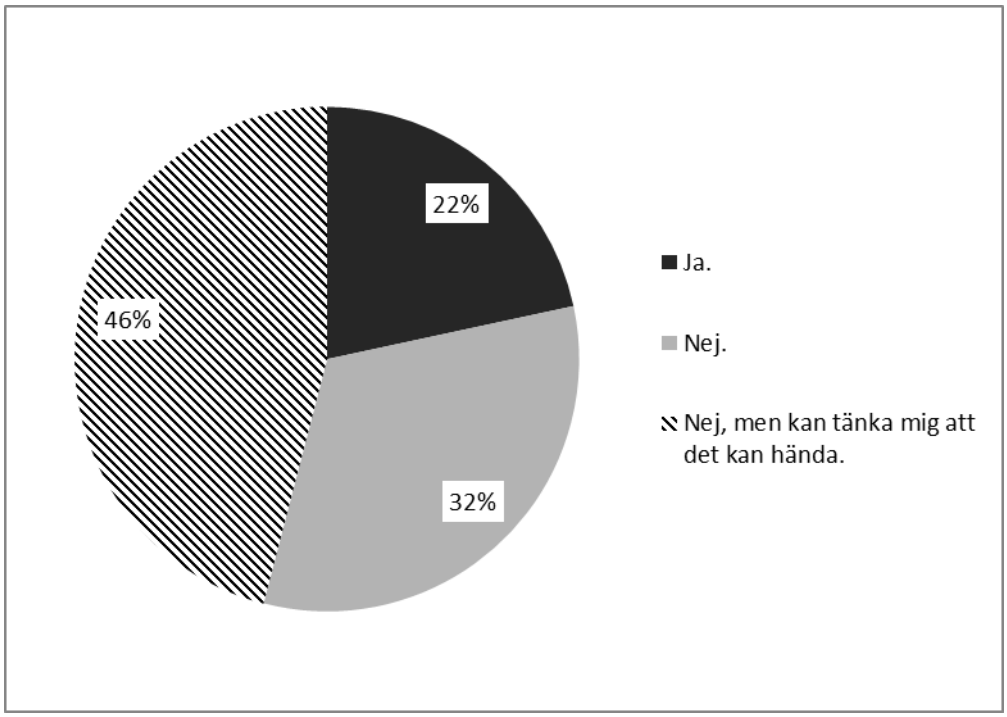
Det står i företagets säkerhetspolicy att de anställda inte får öppna e-post från avsändare de inte känner till. För att kontrollera detta ställdes frågan; "Har du någon gång öppnat e-post från en avsändare du inte känner till?". Till den frågan gavs 2st svarsalternativ, ja eller nej. Resultatet på den frågan visas i figur 12.



Figur 12: Har du någon gång öppnat e-post från en avsändare som du inte känner till?

6.9 Fysisk säkerhet

Det står i företagets säkerhetspolicy att de anställda varken får låna ut sitt behörighetskort till någon annan eller släppa in någon annan med det. Behörighetskortet ska endast användas för att släppa in den person som äger det. För att kontrollera om de anställda lånar ut sina behörighetskort ges ett scenario där en arbetskollega kommer fram till den svarande och frågar om han eller hon kan låna den svarandes behörighetskort för att hämta något i hans eller hennes bil. Därefter ställs frågan; "Låter du honom/henne låna ditt behörighetskort?". Resultatet på frågan kan ses i figur 13 nedan.



Figur 13: Scenario - En arbetskollega som också är en bra kompis till dig frågar dig om han/hon kan låna ditt behörighetskort som ligger på ditt skrivbord för att springa ut till sin bil och hämta en grej. Låter du honom/henne låna ditt behörighetskort?

För att kontrollera om de anställda släpper in någon annan med sitt behörighetskort ställs frågan; "Har du någon gång använt ditt behörighetskort för att släppa in någon på företagets område?" i enkäten. Den svarande får välja mellan 3st svarsalternativ, (1) Ja, (2) Nej eller (3) Nej, men det skulle kunna hända. Resultatet på frågan blev: 38% av de svarande har någon gång släppt in någon på företagets område med sitt behörighetskort, 57% hade aldrig gjort det och 5% svarade att de aldrig hade gjort det men kunde tänka sig att det kan hända.

6.10 Övrigt

I en sektion i företagets säkerhetspolicy står där att anställda inte får tala illa om företaget eftersom det kan skada företagets image. Därför ställdes frågan; "Har du någon gång talat illa om företaget?" i enkäten. De alternativ som den svarande har att välja på är antingen ja eller nej. 35% av de som svarade på enkäten har någon gång talat illa om företaget och 65% svarade att de inte hade gjort det.

7 Relaterad forskning

De undersökningar som finns inom detta ämnesområde är inte lik denna undersökning som har för avsikt att undersöka om det finns någon skillnad på hur ett företags säkerhetspolicy vill att anställda ska hantera information och hur de ska bete sig på arbetsplatsen rent säkerhetsmässigt och hur de i idag verkligen hanterar företagets information och hur de idag beter sig på arbetsplatsen.

Månson (2011) skriver om olika hot mot ett företags informationssystem och gör kvalitativa intervjuer av flera företag för att ta reda på vilka hot som är de största mot företags informationssystem samt vilken skada de hoten kan orsaka. Han beskriver även hur företagen kan skydda sig mot dessa hot och vem eller vad som kan vara orsaken till hoten. Han gör ingen undersökning på de anställda, bara på en kvalitativ undersökning vilka hot som är störst mot företag och inte mot anställda.

Andersson och Vanhatalo (2002) skriver om hur säkerhetsmedvetandet bland personal inom den offentliga sektorn där det finns en säkerhetspolicy och en utbildningsplan för personalen. De använder sig av en kvantitativ undersökning där de skickar ut enkäter till personalen som får svara på de frågor som de ställt i enkäten. Enligt dem är en policy ett sätt att styra hur användaren ska hantera information. Det är enligt Andersson och Vanhatalo (2002) inte tillräckligt att enbart ha en säkerhetspolicy, det krävs att användaren har kunskaper om reglerna och att de förstår varför det är viktigt att följa dem. Den undersökning de gjorde kollar på hur medvetna personalen är om hot men kollar inte om de anställda efterlever den policy som är vald av företaget. Det är viktigt att personalen är både säkerhetsmedvetna och att de efterlever företagets säkerhetspolicy.

8 Analys

I detta kapitel analyseras de svar som de anställda på företaget har bidragit med. Nedan tas intressanta iakttagelser upp som upptäckts under undersökningen.

8.1 Lösenord

De anställda får inte dela med sig av sitt lösenord. I enkäten gavs ett scenario där en person ringde till den svarande och utgav sig för att vara företagets systemadministratör och bad om att få den svarandes användarnamn och lösenord för att lösa ett problem.

Endast 3% svarade att de skulle lämna ut sitt användarnamn och lösenord så att problemet skulle lösas fort. Resterande svarade att de antingen inte alls lämnar ut användarnamnet och lösenordet eller att de inte lämnade ut användarnamnet och lösenordet samt berättade för sin chef vad som hade hänt.

I frågan om hur många tecken de anställda har i sitt nuvarande lösenord svarade 16% att de hade fler än den minst tillåtna gränsen och alla var män. Utbildningsnivån är jämt fördelat över svaren och vad gäller antal års erfarenhet av jobbet på företaget så hade alla som svarade att de hade ett längre lösenord än vad som minst krävdes jobbat på företaget i över 1 år och medelåldern är 41 år.

För att skydda systemet mot att anställda har för enkla lösenord kan systemet konfigureras på ett sätt så att den inte tillåter lösenord under ett visst antal tecken, det kan även konfigureras så att lösenordet måste bestå av siffror, stora bokstäver, små bokstäver och andra tecken.

8.2 Skrivbord

Det stod i företagets säkerhetspolicy att de anställda inte får lämna kvar känslig information på sitt skrivbord när han eller hon lämnar skrivbordet. I enkäten ställdes en fråga som rent ut frågar om den svarande någon gång har lämnat känslig information på skrivbordet när han eller hon lämnat det. De svarsalternativ som erbjöds till den frågan var: Ja, nej eller jag har aldrig hanterat känslig information.

Det gavs också 2 st scenarier där den svarande fick ta ställning till hur han eller hon skulle agera i en sådan situation. I det första scenariot satt de svarande vid sitt skrivbord med känslig information och behövde gå och hämta något att dricka. Enkäten frågade sen vad den svarande skulle göra med den känsliga informationen under tiden. Till scenariot ges den svarande olika svarsalternativ. Han eller hon kunde antingen lämna kvar informationen och skynda sig att uträtta ärendet, be någon annan att vakta den känsliga informationen under tiden han eller hon uträttade ärendet, vända pappret med informationen upp och ned så att ingen kan läsa det och sedan uträtta ärendet, lägga ett annat papper över den känsliga informationen så att ingen kan läsa informationen och uträtta ärendet, plocka bort informationen och uträtta ärendet för att sedan ta fram informationen igen när han eller hon kom tillbaka eller göra något annat.

I det andra scenariot satt den svarande vid sitt skrivbord med känslig information och behövde gå bort till sin kollega som satt ca 15 m bort. Sedan frågades den svarande vad han eller hon skulle göra med den känsliga informationen under tiden. Som i det tidigare

scenariot fick den svarande olika svarsalternativ. Han eller hon kunde lämna kvar informationen och skynda sig att uträtta ärendet borta hos sin kollega och återvända till sitt skrivbord, lämna kvar informationen på skrivbordet och själv kontrollera att ingen obehörig läser informationen bortifrån kollegans skrivbord, be någon annan övervaka informationen under tiden, lägga ett annat papper över den känsliga informationen, plocka bort informationen innan han eller hon går bort till kollegan för att sedan plocka fram det igen när han eller hon återvände eller göra något annat.

Enligt företagets säkerhetspolicy skulle de svarande svara nej på frågan. De skulle även svara att de plockade bort den känsliga informationen innan de utförde ärendena i båda scenarierna för att sedan plocka fram informationen igen när de var klara med ärendet.

På frågan svarade majoriteten att de aldrig har lämnat känslig information på sitt skrivbord när de lämnat det. På de båda scenarierna svarade majoriteten att de skulle lägga ett annat papper över den känsliga informationen så att ingen kan läsa informationen och sedan uträtta sitt ärende.

De resultat från de båda scenarierna jämförs med de resultat från de personerna som svarade nej på frågan om de någon gång hade lämnat känslig information på sitt skrivbord när de lämnat det. I det första scenariot svarade endast 35% att de skulle plocka bort informationen innan de lämnade skrivbordet för att utföra ärendet. 25% svarade att de skulle lägga ett papper över den känsliga informationen och 10% skulle vända upp och ned på pappret.

I det andra scenariot svarade endast 30% att de skulle plocka bort informationen innan de lämnade skrivbordet, 40% svarade att de skulle lägga ett annat papper och 10% skulle lämna kvar informationen utan att gömma det.

Majoriteten svarade alltså för båda scenarierna att de skulle lägga ett papper över den känsliga informationen innan de lämnade skrivbordet trots att majoriteten hävdade att de aldrig lämnar känslig information framme. I det första scenariot svarade 42% av alla kvinnor i undersökningen att de skulle lägga ett papper över den känsliga informationen innan de lämnade skrivbordet och 30% av männen svarade samma. medelåldern för alla som svarade att de skulle lägga ett papper över den känsliga informationen är 42 år. I det andra scenariot svarade 71% av alla kvinnor att de skulle lägga ett papper över den känsliga informationen innan de lämnade skrivbordet och 40% av alla män svarade samma. Medelåldern för alla svarande som svarade att de skulle lägga ett papper över den känsliga informationen är 41,5 år.

Det togs fram liknande statistik för de som faktiskt svarade att de skulle ha plockat bort den känsliga informationen innan de lämnade skrivbordet för att utföra ärendet. I det första scenariot svarade 28,5% av alla kvinnor som medverkade i undersökningen att de skulle plocka bort den känsliga informationen innan de lämnade skrivbordet och 23% av alla män svarade samma. Medelåldern för alla som svarade att de skulle plocka bort informationen innan de lämnade skrivbordet är 48,5 år. I det andra scenariot svarade 14% av alla kvinnor i undersökningen att de skulle plocka bort den känsliga informationen innan de lämnade skrivbordet och 20% av alla män svarade samma. Medelåldern för alla som svarade att de skulle plocka bort informationen innan de lämnade skrivbordet är 48år.

Utbildningsnivån och antal år de anställda har jobbat på företaget är jämt fördelat över de olika svarsalternativen.

Resultaten från undersökningen tyder på att de anställda på företaget inte följer den säkerhetspolicy som ledningen har skapat gällande känslig information.

Att skydda ett företag mot att deras anställda lämnar kvar känslig information på sitt skrivbord när de lämnar det kan vara svårt. Genom att installera fler övervakningskameror i lokalerna så kan ledningen se om de anställda faktiskt lämnar känslig information på sitt skrivbord när de lämnar det. Efter att de upptäckt att anställda gör det kan de ge ut en tillsägelse eller en varning. Det faktum att det finns övervakningskameror i lokalerna gör att de anställda förmodligen tänker mer på vad de gör med den känsliga informationen.

När det gäller elektroniska dokument kan det till en viss del spåras vad de anställda gör med dem genom loggar. Genom att de anställda vet att deras handlingar i systemet loggas och att ledningen kan se vad de gör med den känsliga informationen leder förmodligen till att de tänker efter vad de gör med den känsliga informationen.

8.3 Systemet

I företagets säkerhetspolicy står det att de anställda måste låsa sina datorer när de lämnar den. Resultaten från enkäten tyder på att majoriteten av de anställda på företaget låser sina datorer när de lämnar dem. Det ställdes en fråga och det gavs även ett scenario för att kontrollera om de anställda låste sina datorer när de lämnade dem. Både frågan och scenariot tyder på att de anställda på företaget följer policyn när det handlar om att låsa sina datorer innan de lämnar dem. Av de som inte följer policyn så är alla män, både i frågan och scenariot. Medelåldern för de som svarade att de inte låser datorn är ca 40-41 år. Utbildningsnivån och antal år på företaget är jämt utspritt bland resultaten.

En teknisk lösning för de anställda som väljer att inte låsa datorn eller helt enkelt glömmer att låsa datorn är att konfigurera systemet att automatiskt låsa datorn efter en viss tid, datorn kan låsas efter exempelvis 15 minuter.

8.4 Besökare

När de anställda tar med sig besökare in på företagets område får de inte lämna dem utan uppsyn. Majoriteten svarade att de aldrig har lämnat några besökare oövervakade. Bland alla kvinnor i undersökningen svarade ca 42% att de aldrig hade lämnat sina besökare oövervakade och ca 53% av alla männen svarade samma. Medelåldern för alla personerna som svarade att de aldrig lämnat besökare oövervakade är ca 44 år. Antal år på företaget och deras utbildningsnivå är jämt utspridda bland resultatet.

Av de som svarade att de aldrig hade lämnat besökare oövervakade svarade ca 37% av dem att de skulle lämna sin besökare utan uppsyn utanför toaletterna medan han eller hon gick på toaletten, detta kan på ett sätt ses som att den svarande lämnar besökarna oövervakade. Resultaten tyder på att majoriteten av de anställda inte följer den policy som ledningen tagit fram när det gäller att inte lämna besökare utan uppsikt.

En teknisk lösning som finns tillgänglig för att se till att besökare hålls under uppsikt är övervakningskameror, dessa kan sättas upp så att de täcker hela företagets område. Genom att göra det är alltid besökare övervakade.

8.5 Mobila enheter

Företagets mobila enheter får enligt policyn inte lånas ut till de anställdas barn. För att kontrollera om de följer denna policy ställdes en fråga i enkäten som tog upp detta ämne samt att ett scenario gavs till den svarande. Enligt resultaten från enkäten så följer företagets anställda denna policy.

8.6 Nätverk

Företagets nätverk får inte användas till något som inte är arbetsrelaterat. I enkäten ställdes en fråga där den svarande fick svara på om han eller hon följde företagets policy. Enligt resultaten visade det sig att majoriteten av de anställda inte följer den policy som ledningen tagit fram och använder företagets nätverk till sånt som inte är arbetsrelaterat.

Av alla män som svarade på enkäten svarade 66,5% att de använde företagets nätverk till saker som inte är arbetsrelaterat och 57% av kvinnorna som deltog i undersökningen svarade samma. Medelåldern för de som svarade att de använde företagets nätverk till saker som inte är arbetsrelaterat är ca 42 år. Utbildningsnivån och antalet år på företaget som de svarande har arbetat är jämt fördelat över svarsalternativen.

Loggning av trafik kan leda till att de anställda väljer att följa policyn, genom att annonsera att det sker loggningar av trafiken i företagets nätverk kan detta avskräcka de anställda från att bryta mot denna policy. Det är även möjligt att blockera viss trafik som inte önskas på företagets nätverk.

8.7 Internet

Det finns en liknande policy för företagets Internet, de anställda får inte använda Internet till något som inte är arbetsrelaterat. Resultaten från enkäten visade att endast 3% av de svarande följer denna policy. Alla de som svarade att de aldrig använt företagets Internet till något som inte är arbetsrelaterat är män och medelåldern är ca 38 år. Utbildningen för dem ligger på högskolenivå. Antalet år de arbetat på företaget är över 3 år.

Det ställdes också en fråga i enkäten som frågade om de anställda någon gång använt företagets Internet för att besöka pornografiska hemsidor. Alla de anställda svarade att de aldrig hade försökt använda företagets Internet för att besöka pornografiska hemsidor.

För att få de anställda som inte följer policyn att följa den kan en teknisk lösning vara att införa loggar som loggar allt som de anställda går in på genom företagets Internet, det går även att blockera hemsidor som företaget inte vill att de anställda ska gå in på under arbetstid som exempelvis Facebook, Twitter och Google+.

Att de anställda vet om att företaget loggar allt som de gör på Internet leder förmodligen till att de blir avskräckta från att använda företagets Internet till saker som inte är arbetsrelaterade.

8.8 E-post

Enligt företagets säkerhetspolicy står det att de anställda inte får öppna e-post från avsändare de inte känner till. Enligt resultaten från enkäten följer majoriteten av de svarande inte företagets policy. De som svarade att de någon gång öppnat e-post från avsändare de inte känner till består av 60% av alla män som deltog i undersökningen och 43% av alla kvinnor. Medelåldern för de som svarade att de någon gång har öppnat e-post från avsändare de inte känner till är ca 41 år. Utbildningsnivån och antal år de arbetat på företaget är jämt fördelat bland svarsalternativen.

En teknisk lösning för att hjälpa de anställda att följa denna policy på ett enklare sätt är att införa filter som filtrerar bort okänd e-post som exempelvis spam och reklam mm.

8.9 Fysisk säkerhet

Det står i företagets säkerhetspolicy att de anställda varken får släppa in någon annan på företagets område med sitt eget behörighetskort eller låna ut sitt behörighetskort. Enligt resultatet från enkäten så svarade majoriteten att de inte släppte in andra personer på området med sitt eget behörighetskort, i enkäten ställdes en fråga samt att det gavs ett scenario.

I enkäten ställdes det även en fråga om de anställda lånade ut sitt behörighetskort till andra personer. Resultaten från den frågan säger att majoriteten svarade att de inte lånade ut sitt behörighetskort. När sedan resultaten från scenariot studerades upptäcktes det att majoriteten nu hade svarat annorlunda. Denna gången svarade majoriteten att de aldrig hade lånat ut sitt behörighetskort men att de kunde tänka sig att det skulle kunna hända.

På frågan svarade 66% av alla män i undersökningen att de aldrig hade lånat ut sitt behörighetskort och 57% av kvinnorna svarade samma. På scenariot svarade 57% av alla kvinnor i undersökningen att de aldrig hade lånat ut sitt behörighetskort men att de kunde tänka sig att det skulle kunna hända och 43% av männen svarade samma.

Av de som svarade nej på frågan om de någon gång hade lånat ut sitt behörighetskort så var det bara 50% av dem som svarade nej även på scenariot. De andra ändrade sig till antingen ja eller nej, men kan tänka mig att det kan hända.

De som på frågan svarade att de någon gång lånat ut sitt behörighetskort består av 27% av alla män i undersökningen och 43% av alla kvinnor. De som svarade samma på scenariot består av 20% av alla män i undersökningen och 28% av alla kvinnor.

Medelåldern för de som på frågan svarade att de någon gång har lånat ut sitt behörighetskort är ca 38 år. För de som svarade samma på scenariot är medelåldern ca 37 år. Utbildningsnivån och antalet år de arbetat på företaget är jämt utspritt över svarsalternativen på både frågan och scenariot.

En teknisk lösning för att hindra företagets anställda från att släppa in andra personer med sitt eget behörighetskort kan vara att använda sig av en biometrisk autentiseringsmekanism tillsammans med behörighetskortet. Ett exempel är att använda behörighetskort och de anställdas fingeravtryck. Det kan också gå att konfigurera systemet så att ett och samma kort inte kan användas mer än en gång under ett visst tidsintervall. Lösningen med biometrisk

autentiseringsmekanism går också att använda för att få de anställda att följa policyn om att inte låna ut sina behörighetskort.

8.10 Övrigt

Det stod även i företagets säkerhetspolicy att de anställda inte får tala illa om företaget. Resultatet från enkäten visade att majoriteten av företagets anställda följer denna policy. Den grupp som inte följer denna policy består av 43% av alla kvinnor i undersökningen och 33% av alla män. Medelåldern för de som svarade att de någon gång talat illa om företaget är ca 35 år. Utbildningsnivån för majoriteten av denna grupp ligger på högskolenivå och de har varit på företaget i mer än ett år.

Det ställdes frågor i enkäten om hur de anställda tyckte om företagets policys, detta för att se om möjligheten fanns att de anställda tycker att företagets policys är jobbiga att följa eller att det är för tidskrävande och att de anställda därför på något sätt prokrastinerar när det gäller till att efterleva den policy som företagets ledning tagit fram.

Samma fråga ställdes till de svarande om alla områden som tagits med i enkäten, "Tycker du att företagets policy om [område] på något sätt är:". De svarande fick välja på 6 olika svarsalternativ. (1) Otydlig, (2) Svår att följa, (3) Krånglig att följa, (4) Tidskrävande, (5) Bra som den är och (6) Övrigt.

Enligt resultaten från enkäten visade det sig att majoriteten av de svarande tyckte att företagets policys var bra som de är. Det framgick även från resultaten att några av de anställda inte kände till flera av företagets policys, detta genom att de anställda själva skrivit så efter svarsalternativ "Övrigt" där de ombads att skriva en mening om vad de menade med övrigt. Av de som hade något att påpeka om företagets policys så var det flest som tyckte att policyn om mobila enheter var otydlig.

Det är viktigt att utbilda de anställda om företagets egen policy och berätta vad som menas med policyn och varför den policyn finns, vilken nytta den har för företaget och vilken skada som skulle orsakas om den inte fanns, på detta sätt förstår de anställda varför de ska följa policyn och de får en liten insyn på vilka konsekvenser som finns om policyn inte följs.

9 Slutsats

I detta kapitel beskrivs de slutsatser som arbetet medfört. Det ges en sammanfattning av arbetet och det förs en diskussion om arbetet samt att framtida arbete presenteras.

9.1 Sammanfattning

Att anställda väljer att inte följa en policy kan bero av flera anledningar, det kan vara så att personerna i fråga väljer att inte följa den p.g.a. lathet, okunnighet eller andra personliga anledningar.

Resultaten från denna undersökningen visade att flera av företagets anställda inte följer de säkerhetspolicys som företagets ledning tagit fram för att skydda företagets information. Det finns även flera anställda som faktiskt följer de säkerhetspolicys som finns på företaget. Alla anställda kan alltså inte dras över en kam.

9.2 Diskussion

Det bidrag som detta arbete tillför är en strategi för att upptäcka och förhindra att anställda på företag inte efterlever den säkerhetspolicy som ledningen på företaget tagit fram för att skydda företagets information. Denna strategi har validerats genom en fallstudie på ett företag där strategin användes för att undersöka om deras anställda följer den policy som finns på företaget.

Fler företag kan använda strategin för att upptäcka om sina egna anställda inte efterlever den policy som finns på företaget. Strategin är alltså generaliserad, den är inte framtagen för att passa endast ett företag.

De delmål som tagits fram för att hjälpa till att besvara den frågeställning arbetet har är:

- *Ta reda på hur olika informationssäkerhetspolicys ser ut.*
- *Undersöka efterlevnaden av säkerhetspolicys.*
- *Undersöka huruvida tekniska lösningar kan fånga upp de brister som finns.*
- *Validera den strategi som tas fram.*

Målet att ta reda på hur olika informationssäkerhetspolicy ser ut uppfylldes då flera olika källor har studerats för att se hur en sådan policy ser ut. En mall för hur företag ska skriva sin policy har studerats för att se inom vilka områden en säkerhetspolicy vanligtvis skrivs (SANS, u.å.). Företagets egna säkerhetspolicy har också studerats för att få en tydligare bild över hur företagets säkerhetspolicy ser ut. Det gjordes även en intervjuundersökning med företagets säkerhetsansvarig angående företagets säkerhetspolicy där de delar av företagets säkerhetspolicy som är mest relevanta för undersökningen diskuterades.

Nästa mål, att undersöka efterlevnaden av säkerhetspolicys uppfylldes eftersom det i undersökningen gjordes en enkätundersökning där företagets anställda fick svara på en enkät som handlade om efterlevnaden av företagets säkerhetspolicy. I enkäten ställdes även kontrollfrågor för att kontrollera att svaren är tillförlitliga.

Att undersöka huruvida tekniska lösningar kan fånga upp de brister som finns uppfylldes då sektion 7.2 diskuterar olika förslag på tekniska lösningar som företaget kan införa för att få deras anställda att efterleva deras policy mer.

Målet att validera den strategi som tagits fram uppfylldes eftersom den har använts i den fallstudie som genomförts på ett företag för att identifiera brister i efterlevnaden av den säkerhetspolicy som företagets ledning tagit fram för att skydda dess information.

Den nytta som samhället får av arbetet är att organisationer inom exempelvis vården och militären kan använda sig av strategin för att upptäcka brister hos de anställdas efterlevnad av säkerhetspolicys inom organisationen. Det är viktigt att anställda inom vården följer de säkerhetspolicys som tagits fram till den organisationen eftersom de ofta hanterar viktig information så som personnummer och annan information om patienter mm. Det är inte bra för organisationen om de anställda väljer att inte följa en policy om hur de ska hantera den informationen så att den möjligtvis läcker ut till någon som inte är behörig att läsa den informationen. Detta kan skada organisationens image om det läcker ut till exempelvis media att anställda inom organisationen inte följer de säkerhetspolicys som de ska följa. Det kan även skada patienter genom att information om deras hälsa som de inte vill att någon ska känna till läcker ut. Detta kan även leda till att förtroendet för vården blir sämre vilket i sin tur kan leda till att patienter inte avslöjar all information till exempelvis doktorn så att patientens vård blir lidande eftersom han eller hon inte vill avslöja viktig information som kan ha betydelse i patientens behandling i rädsla av att det ska läcka ut.

Det är viktigt att ta hänsyn till etiska aspekter vid undersökningar, de svarande ska inte behöva ge ut information som kan identifiera dem. I denna undersökning skulle de svarande ge ut information som kön, ålder, utbildningsnivå och antal år på företaget vilket inte är tillräckligt för att kunna identifiera dem. Det är också viktigt att de svarande får behålla sin personliga integritet. Det diskuterades i sektion 7.2.9 om övervakningskameror, det är viktigt att de anställda godkänner användandet av övervakningskameror och att den information som erhålls från övervakningskamerorna inte används till något som kan kränka de anställdas integritet.

Det upptäcktes i undersökningen att det var skillnad på hur de anställda svarade på frågorna och scenarierna. Exempelvis i frågan om känslig information så svarade majoriteten att de aldrig hade lämnat känslig information på sitt skrivbord när de gått iväg och i scenariot svarade majoriteten att de skulle lägga ett annat papper över den känsliga informationen. Detta kan tyda på att de anställda medvetet väljer att inte följa policyn av olika anledningar. Det kan även tyda på att de anställda inte är medvetna om att de agerar fel, de kanske misstolkar säkerhetspolicyn. I exemplet med den känsliga informationen stod det i policyn att de anställda inte fick lämna känslig information framme på skrivbordet. Detta kanske de anställda tolkade som att de inte fick lämna känslig information synligt på skrivbordet, så de lade ett annat papper över den känsliga informationen. Om de anställda inte är medvetna om att de begår misstag så är utbildning av policyn en bättre lösning för att förbättra säkerheten än att införskaffa tekniska lösningar. Det är viktigt att företagets anställda känner till den säkerhetspolicy som finns på företaget och även varför den finns.

9.3 Framtida arbete

Om undersökningen fortsatt en ytterligare tid skulle det vara intressant att få in svar från fler personer på företaget, helst från alla anställda på företaget för att få en mer komplett bild över hur alla företagets anställda efterlever den policy som företagets ledning tagit fram.

Det skulle också vara intressant att se en liknande undersökning som görs under en längre tid och på fler företag. Genom att göra detta kan undersökningen skapa resultat som sprider sig över företags gränser. Det skulle vara intressant att se om det finns liknelser av beteendet att inte följa säkerhetspolicyn hos anställda på flera olika företag eller om beteendet ligger på företagsnivå.

Det vore även intressant att göra en uppföljning på samma företag efter några år för att se om undersökningen lett till några förändringar och även om de anställda blivit mer säkerhetsmedvetna.

Referenser

Al-Hamdani, W.A. & Dixie, W.D. (2009) *Information Security Policy in Small Education Organization*. Information Security Curriculum Development Conference (S. 72-78).

Aloul, F.A. (2010) *Information security awareness in UAE: A survey paper*. Internet Technology and Secured Transactions (ICITST), 2010 International Conference for (S. 1 - 6).

Andersson, F. & Vanhatalo, P. (2002) *Säkerhetsmedvetande inom offentlig sektor: En fallstudie av värden inom Norrbottens Läns Landsting*. Luleå Tekniska Universitet.

Bendej, A. (2006) *Kartläggning av fysiska säkerhetsåtgärder, skiljer dessa sig mellan små och stora företag*. Högskolan i Skövde.

Bengtsson, J. & Ollsson, J. (2003) *Informationssäkerhet*. Högskolan i Trollhättan, Uddevalla.

Berndtsson, M. Hansson, J. Olsson, B. & Lundell, B. (2008) *Thesis Projects: A Guide for Students in Computer Science and Information Systems* (2:a upplagan). Springer-Verlag, London. ISBN-13: 978-1-84800-008-7.

Cook, D.A. & Beckham, T.J. (2006) *Current Concepts in Validity and Reliability for Psychometric Instruments: Theory and Application*. The American Journal of Medicine (S. 166.e7 - 166.e16), 119.

Golafshani, N. (2003) *Understanding Reliability and Validity in Qualitative Research*. The Qualitative Report (S. 597 - 607), Volym 8, utgåva 4. University of Toronto, Toronto, Canada.

Irani, D. Webb, S. Griffin, J. & Pu, C. (2008) *Evolutionary study of phishing*. eCrime Researchers Summit, 2008 (S. 1 - 10).

Khonji, M. Iraqi, Y. & Jones, A (2011) *Mitigation of spear phishing attacks: A Content-based Authorship Identification framework*. Internet Technology and Secured Transactions (ICITST), 2011 International Conference for (S. 416 - 421).

Landstinget Kronoberg (2012) *Informationssäkerhet*. Landstinget Kronoberg, Växjö. Tillgänglig på Internet: http://www.ltkronoberg.se/Om-landstinget/Arbomr/Krisberedskap/Informationssakerhet/. [Hämtad: 2013-02-10].

Lundmark, L. & Palm, H. (2003) *Informationssäkerhet hos myndigheter*. Luleå Tekniska Universitet.

Mohebzada, J.G. El Zarka, A. Bhojani, A.H & Darwish, A. (2012) *Phishing in a university: Two large scale phishing experiments*. Innovations in Information Technology (IIT), 2012 International Conference on (S. 249 - 254).

Månsson, N. (2011) *De största hoten mot ett företags informationssystem*. Lunds Universitet.

Nohlberg, M. (2007) *Social Engineering: Understanding, Measuring and Protecting Against Attacks*. Högskolan i Skövde.

Pfleeger, C. P. & Pfleeger, S. L. (2006) *Security in Computing* (4:e upplagan). Upper Saddle River, NJ. Prentice Hall. ISBN 0-13-239077-9.

Roßling, G. & Muller, M. (2009) *Social Engineering: A Serious Underestimated Problem*. ACM SIGCSE Conference on Innovation and Technology in Computer Science Education (S. 384 - 384).

SANS (u.å.) *Information Security Policy Templates*. SANS. Tillgänglig: http://www.sans.org/security-resources/policies/. [Hämtad: 2013-04-22].

Sasse, MA and Flechais, I (2005) *Usable Security: Why Do We Need It? How Do We Get It?* Cranor, LF and Garfinkel, S,

Steel, P (2007) *The Nature of Procrastination: A Meta-Analytic and Theoretical Review of Quintessential Self-Regulatory Failure*. Psychological Bulletin, vol. 133, nr. 1, S. 65-94.

Steel, P. & Ferrari, J. (2013) *Sex, Education and Procrastination: An Epidemiological Study of Procrastinators´Characteristics from a Global Sample*. European Journal of Personality, Eur.J. Pers. nr. 27, S. 51-58.

Thornburgh, T. (2004) *Social Engineering: The "Dark Art"*. Proceedings of the 1st annual Conference on Information Security Curriculum Development (S. 133 - 135).

Trochim, W.M.K. (2006) *Reliability & Validity*. Research Methods Knowledge Base. Tillgänglig på Internet: http://www.socialresearchmethods.net/kb/relandval.php. [Hämtad: 2013-03-03].

Vinci Energies (2009) *IT-policy*. Vinci Energies Nordic AB. Tillgänglig på Internet: http://www.emillundgren.se/om_oss/IT_policy.pdf. [Hämtad: 2013-04-22].

Walonick, D.S (2010) *A Selection from Survival Statistics*. StatPac, Inc., 8609 Lyndale Ave. S. #209A, Bloomington. ISBN: 0-918733-11-1.

Wang, A. P (2010) *Information Security Knowledge and Behavior: An Adapted Model of Technology Acceptance*. Education Technology and Computer (ICETC), 2010 2nd International Conference on (S. V2-364 - V2-367).

Wang, J. Herath, T. Chen, R. Vishwanath, A. & Rao, R. (2012) *Research Article Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email*. Professional Communication, IEEE Transactions on (S. 345 - 362). Volym: 55. utgåva: 4.

Bilaga A - Sammanställning av intervjun

Lösenord

På företaget finns det en policy för hur lösenord ska skapas, hanteras, skyddas och kontrolleras. Ett lösenord måste innehålla minst 7 tecken, däribland minst en stor bokstav och sedan blandat bokstäver och siffror. Ett lösenord är giltigt i 60 dagar efter det måste det bytas ut. Systemet kommer ihåg de senaste 9 lösenorden och det nya lösenordet får inte vara samma som de 9 senaste. Under en inloggning när lösenordet ska skrivas in har en person 3 försök på sig att skriva in rätt lösenord, efter det blockeras användarkontot. När ett konto är blockerat måste en chef låsa upp det igen eller genom att användaren svarar på en fråga för att identifiera sig. Ett lösenord får inte vara uppskrivet någonstans av säkerhetsskäl.

Skrivbord

Skrivborden på företaget städas varannan dag av ett externt företag. På skrivbordet får de anställda själva välja vad som ska finnas på skrivbordet och vad som inte ska finnas på skrivbordet, dock ska inget känsligt material finnas på skrivborden. Beroende på tjänsten som de anställda har så kan de ha ett privat skrivbord eller en grupp gemensamma skrivbord, de som jobbar på företaget och utför sitt arbete på företagets område får sitt eget skrivbord medan de som inte ständigt utför sitt arbete på företagets område får låna ett skrivbord. Det kontrolleras inte vem som kommer åt de privata skrivborden.

Systemet

För att kunna logga in på systemet krävs det ett användarnamn och ett lösenord. På systemet finns det olika behörighetsnivåer. Från början får personer endast tillgång till sin egen hemmakatalog och sedan får man behörighet till olika tjänster för att kunna börja jobba. Policyn säger att användare måste låsa sina datorer när de lämnar datorn. Glöms detta finns det en säkerhetsåtgärd som automatiskt låser datorn efter att användare varit inaktiva i 10 minuter. Inom varje system på företaget finns det behörighetsnivåer och grupper. Anställda ges endast tillgång till de applikationer som behövs för att de ska kunna utföra sitt arbete, krävs det nåt ytterligare beställs detta hos chefer. Om anställda behöver logga in på företagets system utifrån görs detta genom företagets VPN. Allt på systemet är krypterat, det finns backup av systemet och flera brandväggar som kräver användarnamn och lösenord för att komma in. Systemet kontrolleras genom övervakningar som idag bedrivs i Indien. Det sker övervakningar av systemets belastning och användar-ID. Det finns loggar i systemet som loggar vad användarna gör på systemet.

Besökare

De besökare som kommer till området måste i förväg vara anmälda till vakten av någon person inne på området. När besökarna kommer in på området får personerna varsin besöksbricka som sedan är ett krav för att de ska få vistas på området. Om besökarna ska vistas på företagets industriområde måste de ha en gul besöksväst som tydligt visar att de är besökare på området. Den person som anmält besökarna till området är ansvarig för att besökarna sedan lämnar området igen. Entreprenörer och konsulter måste även de anmälas, ska de göra arbete på området en längre tid kan de få ett lånekort med begränsad behörighet eller ett eget behörighetskort för att själva kunna ta sig in på området. Den person som anmält besökaren är främst ansvarig för att under vistelsen kontrollera besökaren/besökarna, det finns även övervakningskameror på området och vid ingångsportarna som kan övervaka besökare. Besökare ska inte ha någon frihet att kunna gå runt på området på egen hand, besökare ska inte lämnas själva med undantag av entreprenörer och konsulter. Besökare, entreprenörer och konsulter får även skriva på ett sekretessavtal så att de inte avslöjar någon känslig information. Det krävs även ett behörighetskort för att kunna ta sig ut från området så besökare måste eskorteras ut från området.

Mobila enheter

Laptop

En laptop har en ägare och endast den ägaren kan logga in på laptopen om personen inte befinner sig på området eftersom på området finns det ett trådlöst nätverk som gör att laptopen är definierad i nätverket och detta gör att vilken anställd som helst med ett användarnamn och lösenord som är giltigt på företaget kan logga in på den. Alla anställda som har en laptop får ta med den hem och använda den hemma, det finns inga begränsningar mot detta. Barn i hemmet får inte använda laptopen eftersom den är företagets utrustning. Om laptopen används hemifrån säger policyn att de anställd måste tunnla in på företagets VPN och använda laptopen genom företagets nätverk. Anställda som vill ta med sig sin personliga laptop till jobbet får göra detta men den kan inte användas på företagets nätverk eftersom alla enheter på företagets nätverket måste vara definierade. När det handlar om säkerhet av laptops så finns det ingen policy som säger att anställda måste låsa sina datorer. Eftersom hela datorn är krypterad gör det inget om en laptop skulle bli stulen. Det finns ett virusskydd på varje dator på företaget. Om ett virus upptäcks på en dator så skickar den ett larm till övervakningen som sedan kan se vilken dator det handlar om och kan om det behövs blockera datorn från nätverket. Den infekterade datorn tas ur drift och den anställde får låna en annan dator under tiden den rensas. Företaget använder sig inte av någon portsäkerhet vilket gör att en angripare förutsatt att han eller hon har kommit in på området kan ansluta sig till nätverket och infektera nätverket med virus och annan skadlig kod.

Smartphone
Smartphones är inte definierade som en nätverksenhet. Därför kan inte mobiler komma åt systemet. Mobilen kan däremot komma åt de anställdas e-post. En smartphone kräver en pinkod och ett lösenord för att kunna komma in och använda telefonen. Telefonen är även nerlåst med programvara så det går inte installera vad som helst på telefonerna. Endast företagets telefontekniker kan låsa upp telefonerna. Privata telefoner får tas med till arbetet men de kan inte anslutas till företagets trådlösa nätverk eftersom telefonerna inte är definierad i nätverket. Företagets anställda får ha sin privata telefon som arbetstelefon, dock måste företagets SIM-kort (telefonnummer) användas. Det är inte möjligt att ha sitt privata SIM-kort (telefonnummer) som arbetsnummer. Alla telefoner får tas med hem utanför arbetstid, det är inte ett krav att svara i telefonen efter arbetstid. Flera anställda har en sådan roll i företaget att de ska vara tillgängliga dygnet runt, alla dagar i veckan, detta eftersom företaget är globalt och det kan ringa personer från andra tidszoner som exempelvis Indien. Hela telefonen är krypterad och den skyddas även med användarnamn och lösenord. Ett SIM-kort från företaget får inte användas för att betala vissa tjänster, man får till exempel inte att betala en parkeringsavgift med företagets telefon. Företagets telefoner kontrolleras inte av företagets övervakning eftersom den inte är definierad i nätverket, det enda telefonerna kommer åt i företagets system är de anställdas e-post.

VPN

Företagets VPN används för alla uppkopplingar till nätverket utifrån. För att kunna logga in via företagets VPN krävs ett användarnamn och en digipassdosa (liknande bankdosa). Alla anställda som har en dosa får använda företagets VPN, de som har arbetsuppgifter utanför företagets område får tillgång till en dosa. Det finns inga specifika regler för att använda företagets VPN. Allt i tunneln är krypterat och trafiken loggas. Under inloggningen med dosan har anställda 3 försök på sig, efter det tredje felaktiga försöket skickas ett larm till övervakningen.

Nätverk

Alla på företaget får använda företagets nätverk, de måste ha ett användarnamn. Det finns ett fabriksnät och ett kontorsnät. Allt på nätverket loggas och om till exempel någon med en okänd IP-adress försöker ansluta så skickas ett larm. Företaget övervakar även nätverket och larmar om nätverket skulle bli för belastat och det finns övervakning av användar-id. Nätverket får inte användas till något som inte är arbetsrelaterat. Hela nätverket är krypterat och det finns även redundans i hela nätverket. Företaget har inget fysiskt skydd för nätverket. Under överlastningsattacker kan företaget avskärma sig och köra allt internt över sitt intranät. Om en kabel inne på företagets område skulle gå av (förstörelse eller olycka) så larmas övervakningen. På hela företagets område finns det tillgång till det trådlösa nätverket så om det trådburna nätverket skulle gå ner så kan de anställda använda det trådlösa nätverket. Det trådlösa nätverket är avskärmat så att det inte är tillgängligt för personer utanför området.

Internet

Internet används till det mesta i företaget, som exempelvis kontakt med kunder, entreprenörer och konsulter och det används även till att sälja företagets produkter. Internet får inte användas till något som inte är arbetsrelaterat, företaget blockerar de flesta sidor på Internet som är klassade som hobbyverksamhet som exempelvis spelsidor, köp och säljsidor osv. Alla på företaget får använda sig av Internet i sitt arbete. Fabriksdatorer som finns i industriområdet är inte uppkopplade på Internet. All trafik loggas så försök till att ansluta sig till blockerade sidor loggas och larmas till övervakningen.

E-post

Policyn säger att anställda inte får öppna e-post från avsändare som de inte känner till. Policyn säger även att de anställda själva är ansvariga för de e-postmeddelanden som de öppnar och läser samt de länkar som de trycker på. Samma policy gäller för bilagor. All e-post som skickas och tas emot är automatiskt krypterat av systemet så att användare inte ska behöva tänka på det. Det finns spamfilter i nätverket som stoppar de flesta spammeddelanden som kommer utifrån. Det finns även redundanta e-postservrar så att anställda inte ska förlora sin e-post. De anställdas kataloger för e-post har ett begränsat utrymme.

Fysisk säkerhet

Företagets anställda autentiserar sig med ett passerkort, det krävs ingen kod till passerkortet dagtid men på kvällstid krävs även en kod tillsammans med passerkortet för att kunna autentisera sig. Personer som ska ta sig in på området måste gå igenom en av ett flertal grindar, dessa grindar är kameraövervakade och några av grindarna är även bemannade av företagets vakter. Kamerorna på området aktiveras genom rörelse. De anställdas kontor går inte att låsas och det krävs inget behörighetskort för att ta sig in på ett kontor, däremot krävs det ett behörighetskort för att komma in på avdelningarna och det finns olika behörighetszoner på företagets område. Hela området är inhägnat och kameraövervakat så att personer inte ska kunna ta sig in oupptäckta. Om något ska transporteras ut från området med bil krävs ett fordonspass som är kopplat till behörighetskortet, det är inte många personer som har ett sådant pass. Bilarna som åker ut kan bli stoppade och kontrollerade. Personlig utrustning som exempelvis laptops är det ingen kontroll på. Lyckas man komma in på området så kan man förstöra något och det går att slänga in något över inhägnaden såsom stenar som kan förstöra saker. De fönster som är riktade ut mot gatan är försedda med skottsäkert glas. När det gäller brandsäkerhet har företaget en egen brandkår samt automatisk släckning på vissa områden. Släckutrustningen kontrolleras efter ett schema. Allt loggas och vakter kör ut på sina ronder inne på området utanför kontorstid. Det finns en sensor på alla dörrar som larmar vakten om dörrarna varit öppna i mer är 30-60 sekunder. Det finns inget specifikt skydd mot företagets lokaler förutom inhägnaden runt området. Det finns ett inbrottslarm installerat på lokalerna som i dagsläget inte är aktiverade eftersom de har anställda på plats dygnet runt.

Social Engineering

Det finns en policy på företaget om social engineering, eftersom social engineering inte är så vanligt i Sverige så uppmanas de anställda att läsa den policyn när de ska resa till vissa länder. Policyn säger att man ska vara försiktig med vem du kontaktar och vem som kontaktar dig. Det finns fler policys om säkerhet förutom den mot social engineering. De anställda får inte göra något som skadar företagets varumärke som exempelvis slåss ute på stan med en jacka med företagets märke på, de får heller inte skriva eller tala illa om företaget på sociala nätverk. Det finns inga specifika säkerhetsåtgärder mot social engineering förutom att de anställda ska använda ett sunt förnuft. Det finns inte heller något krav för hur stor kunskap de anställda ska ha om social engineering. Det finns ingen utbildning mot enbart social engineering, däremot får alla anställda genomgå en grundutbildning i säkerhet med säkerhetsansvarig på avdelningen och en ytterligare elektronisk utbildning. De anställda måste vartannat år genomgå den elektroniska utbildningen och den uppdateras ständigt med nytt material.

Övrigt

Säkerhetsansvarig på avdelningen tror att de anställda är väl medvetna om policyn men att de av olika anledningar väljer att inte följa den till punkt och pricka. Detta kan skada företagets varumärke.

Om de anställda inte följer företagets policy kan de riskera att bli avskedade beroende på hur allvarlig situationen är.

Det ges skriftliga varningar till de anställda som inte följer policyn, efter 3st skriftliga varningar så avskedas den anställde. Det kan eventuellt ges en tillsägelse om skadan är liten som verkar som en varning innan en skriftlig varning ges.

Bilaga B - Enkäten

Personligt

Är du:

- Man?
- Kvinna?

Hur gammal är du?

_____

Vad heter den tjänst du har på företaget idag?

_____

Hur många år har du arbetat på företaget?

- Mindre än 1 år.
- 1-2år.
- 3-5år.
- Längre än 5år.

På vilken nivå är din högst avslutade utbildning?

- Grundskolenivå.
- Gymnasienivå.
- Högskolenivå/Universitetsnivå.

Vilka arbeten har du haft tidigare? (Kryssa i fler alternativ om du haft olika arbeten med olika policys)

- Arbeten med liknande säkerhetspolicys.
- Arbeten där de inte hade några säkerhetspolicys alls.
- Arbeten med mindre säkerhetspolicys.
- Arbeten med fler säkerhetspolicys.
- Jag har inte haft tidigare arbeten innan / Jag har studerat innan.

På din arbetsplats, har du:

- Ett privat skrivbord.
- Ett gemensamt skrivbord som kan ändras från dag till dag.

Lösenord

Har du någon gång delat med dig av ditt lösenord till någon person?

- Ja.
- Nej.

Har en arbetskollega någon gång berättat sitt lösenord för dig?

- Ja.
- Nej.

Scenario: En person ringer till dig och säger att han är en systemadministratör på företaget och ber dig om ditt användarnamn och lösenord för att lösa ett problem som du snart kommer att få utstå. Vad gör du?

- Lämnar inte ut ditt användarnamn och lösenord.
- Lämnar ut ditt användarnamn och lösenord så att problemet kan lösas fort.
- Du kontrollerar först med din chef så att allt sköts korrekt.
- Lämnar ut ditt användarnamn och lösenord och säger till din chef.
- Lämnar inte ut ditt användarnamn och lösenord och säger till din chef.

Hur håller du koll på dina lösenord?

- Jag skriver upp dem någonstans.
- Jag har en applikation där jag lagrar alla mina lösenord.
- Jag kommer ihåg dem.
- Jag har ett annat sätt.

Hur många tecken har du i ditt nuvarande lösenord?

- 7-8 tecken.
- Fler tecken.

Har du någon gång återanvänt något av dina arbetslösenord privat? (såsom Facebook osv.).

- Ja.
- Nej.

Tycker du att företagets lösenordspolicy på något sätt är:

- Otydlig.
- Svår att följa.
- Krånglig att följa.
- Tidskrävande.
- Bra som den är.
- Övrigt. _____

Skrivbord

Har du någon gång lämnat känslig information på ditt skrivbord när du lämnat skrivbordet?

- Ja.
- Nej.
- Jag har aldrig hanterat känslig information.

Scenario: Du sitter vid ditt skrivbord med känslig information, plötsligt känner du att du behöver gå på toaletten. Vad gör du?

- Lämnar kvar informationen på skrivbordet och skyndar dig att uträtta ärendet och återvänder inom några minuter.
- Ber någon annan att övervaka informationen på skrivbordet medan du uträttar ärendet.
- Vänder pappret med informationen upp och ner så att ingen kan läsa det och uträttar sedan ärendet.
- Lägger något annat papper över informationen så att ingen ska kunna läsa det och uträttar sedan ärendet.
- Plockar bort informationen och låser in det för att sedan plocka fram det igen när du uträttat ärendet.
- Något annat.

Scenario: Du sitter vid ditt skrivbord med känslig information och du ska gå över till en kollega och fråga en sak (kollegan sitter 10-20m bort). Vad gör du?

- Lämnar kvar informationen på skrivbordet och skyndar dig att fråga kollegan det du ska fråga och återvänder sedan inom några minuter.
- Lämnar kvar informationen på skrivbordet eftersom du enbart är några meter bort och kan själv kontrollera att ingen obehörig läser informationen.
- Ber någon annan att övervaka informationen på skrivbordet medan du går över till kollegan.
- Lägger något annat papper över informationen så att ingen ska kunna läsa det och går sedan över till kollegan.
- Plockar bort informationen och låser in det för att sedan plocka fram det igen när du har kommit tillbaka från kollegan.
- Något annat.

Tycker du att företagets skrivbordspolicy på något sätt är:

- Otydlig.
- Svår att följa.
- Krånglig att följa.
- Tidskrävande.
- Bra som den är.
- Övrigt. _____

Systemet

Låser du alltid din dator när du lämnar den?

- Ja.
- Nej.

Scenario: Du sitter vid din dator och arbetar och kommer på att du är väldigt törstig och går iväg för att hämta någonting att dricka. Du vet att du enbart kommer vara borta i max 5 minuter. Låser du din dator?

- Ja.
- Nej.

Tycker du att policyn för företagets system på något sätt är:

- Otydlig.
- Svår att följa.
- Krånglig att följa.
- Tidskrävande.
- Bra som den är.
- Övrigt. _____

Besökare

Anmäler du alltid besökare till vakten?

- Ja.
- Nej.
- Jag har aldrig haft besökare.

Har du någon gång tagit med en besökare in på området med ditt eget behörighetskort?

- Ja.
- Nej.
- Jag har aldrig haft besökare.

Scenario: Du och en kompis står utanför företagets område en vacker vinterdag, din kompis jobbar inte på företaget och har därför inte ett behörighetskort. Du måste in på området och fixa en sak, detta tar ca. 15 minuter. Lämnar du din kompis stående ute i kylan medan du går in och fixar det du ska göra?

- Ja, jag låter honom stå och vänta de korta 15 minuterna.
- Nej, jag låter honom följa med in i värmen.
- Jag gör något annat.

Har du någon gång lämnat besökare oövervakade?

- Ja.
- Nej.
- Jag har aldrig haft besökare.

Scenario: Du har några besökare med dig inne på företagets område, plötsligt behöver du gå på toaletten. Vad gör du med besökarna?

- Lämnar dem utanför, det går fort att gå på toaletten och dessutom hör jag dem från toaletten.
- Ber någon annan att övervaka besökarna medan du går på toaletten.
- Gör någonting annat.

Tycker du att företagets besökspolicy på något sätt är:

- Otydlig.
- Svår att följa.
- Krånglig att följa.
- Tidskrävande.
- Bra som den är.
- Övrigt. _____

Mobila enheter

Lånar du ut din arbetslaptop till ditt/dina barn?

- Ja.
- Nej.
- Jag har ingen arbetslaptop.
- Jag har inget barn.
- Jag har varken en arbetslaptop eller barn.

Scenario: Ditt 12-åriga barn får en dag syn på din arbetslaptop och frågar om han/hon får låna den för att kolla Facebook. Vad svarar du?

- Ja.
- Nej.
- Okej, men jag måste alltid vara med när du använder den.
- Något annat.

När du använder din laptop hemma, ansluter du dig alltid till företagets nätverk innan du börjar surfa på den?

- Ja.
- Nej.
- Jag har ingen arbetslaptop.

Använder du din arbetstelefon för att kolla din e-post?

- Ja.
- Nej.
- Jag har ingen arbetstelefon.

Tycker du att företagets policy för mobila enheter på något sätt är:

- Otydlig.
- Svår att följa.
- Krånglig att följa.
- Tidskrävande.
- Bra som den är.
- Övrigt. _____

Nätverk

Har du någon gång använt företagets nätverk till något som inte är arbetsrelaterat?

- Ja.
- Nej.

Har du någon gång delat med dig av personliga bilder eller filmer till arbetskollegor över företagets nätverk?

- Ja.
- Nej.

Tycker du att företagets policy för nätverket på något sätt är:

- Otydlig.
- Svår att följa.
- Krånglig att följa.
- Tidskrävande.
- Bra som den är.
- Övrigt. _____

Internet

Har du någon gång använt företagets Internet till något som inte är arbetsrelaterat?

- Ja.
- Nej.

Har du någon gång försökt gå in på en hemsida med pornografiskt innehåll?

- Ja.
- Nej.

Tycker du att företagets Internetpolicy på något sätt är:

- Otydlig.
- Svår att följa.
- Krånglig att följa.
- Tidskrävande.
- Bra som den är.
- Övrigt. _____

E-post

Har du någon gång öppnat e-post från en avsändare som du inte känner till?

- Ja.
- Nej.

Klickar du på okända länkar?

- Ja.
- Nej.

Öppnar du bilagor från avsändare som är okända för dig?

- Ja.
- Nej.

Tycker du att företagets policy för e-post på något sätt är:

- Otydlig.
- Svår att följa.
- Krånglig att följa.
- Tidskrävande.
- Bra som den är.
- Övrigt. _____

Fysisk säkerhet

Har du någon gång lånat ut ditt behörighetskort till någon?

- Ja.
- Nej.
- Nej, men jag tror att det skulle kunna hända.

Scenario: En arbetskollega som också är en bra kompis till dig frågar dig om han/hon kan låna ditt behörighetskort som ligger på ditt skrivbord för att springa ut till sin bil och hämta en grej eftersom hans/hennes kort ligger långt ner i väskan. Låter du honom/henne låna ditt behörighetskort?

- Ja.
- Nej.
- Nej, men kan tänka mig att detta kan hända.

Har du någon gång använt ditt behörighetskort för att släppa in någon på företagets område?

- Ja.
- Nej.
- Nej, men det skulle kunna hända.

Scenario: Din kollega som du känner väl och umgås mycket med på arbetstid anländer samtidigt som dig på morgonen precis innan ni ska gå in på företagets område. Han/hon har redan sitt behörighetskort i handen och du har ditt kvar i plånboken/fickan/väskan. Ber du honom/henne att släppa in dig också?

- Ja.
- Nej, jag tar upp mitt eget behörighetskort.

Tycker du att företagets policy för fysisk säkerhet på något sätt är:

- Otydlig.
- Svår att följa.
- Krånglig att följa.
- Tidskrävande.
- Bra som den är.
- Övrigt. _____

Övrigt

Har du någon gång talat illa om företaget?

- Ja.
- Nej.

Tänker du dig för vad du gör när du representerar företaget?

- Ja.
- Nej.

Bilaga C - Utskicket

Hej!

Jag heter Jimmy Andersson, jag studerar på Högskolan i Skövde på programmet Nätverk och systemadministration (NSA). Jag gör en enkätundersökning till min C-uppsats om [Företagets] säkerhetspolicy, jag hoppas verkligen att du vill svara på enkäten, den tar ca. 10-15 minuter. Undersökningen är 100% anonym och ingen kan se vad just du har svarat så var snäll och svara ärligt.

Mvh
Jimmy Andersson