

Hur kan företag skydda sig mot nätbedrägeri?

Anna Lindahl

Examensarbete / Degree Thesis
Företagsekonomi/Financial Management
2018

Anna Lindahl

EXAMENSARBETE	
Arcada	
Utbildningsprogram:	Företagsekonomi
Identifikationsnummer:	5816
Författare:	Anna Lindahl
Arbetets namn:	Hur kan företag skydda sig mot nätbedrägeri?
Handledare (Arcada):	Linda Puukko
Uppdragsgivare:	-
<p>Sammandrag:</p> <p>Då Informationsteknikens utveckling medför möjligheter, men också stora säkerhetsrisker. Trots att den här utvecklingen har pågått en lång tid finns det begränsat med information för den enskilda individen om hur man kan skydda sig mot nätbedrägeri. Då människan i systemet oftast är den största säkerhetsrisken, är det viktigt att alla vet grunderna i hur ett nätbedrägeriförsök kan se ut och vad man ska göra för att undvika en attack. Följderna av en attack kan vara avgörande för ett företags rykte men kan även ha en stor ekonomisk inverkan. Syftet med det här arbetet är att beskriva vad nätbedrägeri är, de vanligaste formerna av bedrägeri, och hur man kan skydda sig mot en attack. Metoden som använts är allmän litteraturoversikt för att sammanställa ett beskrivande arbete av det material som redan finns tillgängligt på nätet och i tryckt litteratur. Första delen av arbetet beskriver vad nätbedrägeri innebär, medan andra delen beskriver vad som kan göras för att förebygga en attack. Arbetet kan utnyttjas av enskilda personer som är intresserade av ämnet och vill förbättra sitt eget beteende på webben och företag som vill se över sina egna informationssäkerhetsprocesser.</p>	
Nyckelord:	Nätbedrägeri, cyberattack, informationssäkerhet, förebyggande
Sidantal:	37
Språk:	Svenska
Datum för godkännande:	

DEGREE THESIS	
Arcada	
Degree Programme:	
Identification number:	
5816	
Author:	Anna Lindahl
Title:	How can companies protect themselves against cyber fraud?
Supervisor (Arcada):	Linda Puukko
Commissioned by:	
<p>Abstract:</p> <p>As information technology develops, there will be big opportunities, but also high security risks. Although this development has lasted for a while, there is limited information for the common individual on how to protect against network fraud. Since the person in the system usually is the biggest security risk, it is important that everyone knows the basics of how a network fraud attempt might look like and what to do in order to avoid an attack. The consequences of an attack can be crucial to the reputation of a company but it can also have a major financial impact. The purpose of this thesis is to describe what network fraud is, what the most common forms of fraud are, and how to protect against an attack. The method used is a general literature review to compile a descriptive work of the material already available online and in printed sources. The first part of the work describes what fraud is, while the second part describes what can be done to prevent an attack. This thesis can be used both by private persons who wants to learn more about this topic and by companies that want to review their own information security processes.</p>	
Keywords:	Cyber fraud, cyber-attack, information security, prevention
Number of pages:	37
Language:	Swedish
Date of acceptance:	

OPINNÄYTE	
Arcada	
Koulutusohjelma:	
Tunnistenumero:	
Tekijä:	Anna Lindahl
Työn nimi:	Miten yritykset voivat suojata verkkopetoksia vastaan?
Työn ohjaaja (Arcada):	
Toimeksiantaja:	
<p>Tiivistelmä:</p> <p>Tietotekniikan kehittymisen myötä mahdollisuudet kasvavat, mutta samalla kasvavat myös tietoturvariskit. Tietoturvan heikentymistä on tapahtunut jo jonkin aikaa. Siitä huolimatta tietoa yksityishenkilön mahdollisuuksista suojautua nettihuijauksia vastaan löytyy rajoitetusti. Yleensä ihminen on järjestelmän suurin turvallisuusriski, ja siksi onkin tärkeää, että jokainen osaa tunnistaa huijausyrityksen peruselementit. Jokaisen pitäisi myös tietää, miten tulisi toimia suojautuakseen hyökkäyksestä. Hyökkäyksen seurauksena yrityksen maine saattaa kolhiintua. Tämän lisäksi hyökkäykset saattavat vaikuttaa haitallisesti yrityksen talouteen. Tutkielmassani kuvailen netissä tapahtuvaa huijaustoimintaa, sen tavallisimpia muotoja ja toimenpiteitä nettihuijauksien välttämiseksi. Tutkielman lähteenä on käytetty olemassa olevaa aihetta käsittelevää, painettua ja netissä julkaistua kirjallisuutta. Ensimmäisessä osassa määrittelen nettihuijausta tekona. Toisessa osassa kuvailen toimenpiteitä, joiden avulla voimme ennaltaehkäistä huijauksia. Tästä tutkielmasta voi olla hyötyä aiheesta kiinnostuneille ja nettikäyttäjytymistään kehittäville yksityishenkilöille sekä tietoturvaprosessiaan kehittäville ja päivittäville yrityksille.</p>	
Avainsanat:	Verkkopetos, tietoverkkorikollisuus, tietoturva, ennataehkäisy
Sivumäärä:	37
Kieli:	Ruotsi
Hyväksymispäivämäärä:	

INNEHÅLL / CONTENTS

1	Inledning.....	6
1.1	Problembakgrund	7
1.2	Syfte och frågeställningar	8
2	Metod.....	9
2.1	Allmän litteraturoversikt	9
2.2	Tillvägagångssätt.....	10
2.3	Avgränsning.....	11
2.4	Sökprocess.....	11
2.5	Begreppsdefinitioner.....	12
3	Vad är nätbedrägeri?.....	13
3.1	Riktad attack.....	14
3.2	Nätfiske.....	15
3.3	Pharming	15
3.4	Online betalnings bedrägeri	16
3.5	CEO Fraud	16
3.6	Falska fakturor.....	17
3.7	Cyberstalking.....	18
3.8	Identitetsstöld	18
3.9	Kriminalitet bland de anställda	19
3.10	Internetbaserad kriminell tjänstsektor.....	19
3.11	Vem har ansvar för företagets risker?	20
3.12	Case:	20
4	Vilka följder har en attack?	21
5	Hur kan man skydda sig?	23
5.1	Teknik och programvaror	24
5.2	Användarens riskprofil.....	25
5.3	Praktiska råd för säkra lösenord.....	26
5.4	Personalens attityder.....	27
5.5	Informationssäkerhets Policy	28
5.6	Förberedelser för en attack	30
6.	Diskussion	31
	Källor / References	34

1 INLEDNING

Utvecklingen av informationsteknologi skapar både utmaningar och möjligheter. Dessa förändringar medför att samhället blir mer sårbart och skapar därigenom stora säkerhetsutmaningar. Sårbarheterna som uppstår i dagens globala IT-system är en av de mest komplexa säkerhetsfrågorna just nu, och i den närmaste framtiden. (Informationssäkerhet- trender 2015, s. 6)

Informationssäkerhet är inte längre endast ett ämne som berör personer med tekniskt intresse. Företagens beslutfattare kommer allt oftare att behöva hantera konflikter där informationssäkerhet ställs mot andra värden. Dessa frågor är komplexa och kräver såväl engagemang som strategiska beslut på högsta nivå inom företag. (Informationssäkerhet- trender 2015, s. 16)

Nätbedrägeri har varit ett aktuellt ämne redan under en längre tidsperiod. Företag har råkat ut för bedrägeriattacker och mist stora summor pengar och sensitiv information har läckt ut i fel händer. Dessa attacker har haft enorma konsekvenser både ekonomiskt och för företagets rykte. Cyberattacker anses vara ett av de största säkerhetshoten vi lever med i nutid. Vi lever i en värld som är beroende av fungerande nätverk och företag bevarar ofta största delen av verksamhetens kritiska system online. Dessa system utvecklas konstant och vi rör oss allt mer från pappersarbete och manuellt arbete mot automatiska system och online tjänster. I takt med att systemen utvecklas, utvecklas även de metoderna kriminella använder sig av för att komma åt företags system och deras information. Detta medför större krav på informationssäkerhet och cybersäkerhet. Företag har ett stort ansvar när det kommer till att bevara företagets sensitiva information utom räckhåll för en tredje parts person. En attack mot ett företags nätverk kan medföra allvarliga konsekvenser mot företagets ekonomi, image samt för företagets kunder och anställda. Vad kan då ett företag göra för att skydda sig mot dessa attacker?

1.1 Problembakgrund

En forskning utförd av Ponemon Institute (2013) visar att de flesta små- och medelstora företagen inte är säkra på hur deras säkerhetsstrategi ser ut och vilka hot de kan möta. Studien visar att 58 procent av de undersökta företagens ledningsgrupp inte ser cyberhot som en signifikant risk och 44 procent säger att en stark cybersäkerhet inte är en prioritet inom företaget. Också små budgeter och okunskap visade sig vara vanliga orsaker till en begränsad cybersäkerhet inom företagen. Trots detta påstod en stor del av respondenterna att det förekommit en cyberattack inom de senaste 12 månaderna.

I en värld som allt mer och mer är driven av sociala nätverk, online transaktioner, information som är lagrad online, processer som drivs genom IT system etc. medför också stora risker. Nätbedrägeri utvecklas i snabb takt och bedrägeri metoderna blir allt mer och mer utvecklade. Dessutom är attackerna ofta svåra, om inte omöjliga, att spåra.

I takt med att attackerna utvecklas, ökar också storleken på skadan som de kan medföra. Varje företag, oberoende storlek, skall se till att de interna processerna är under kontroll. Ett företag skall bland annat se till att de olika systemen har de nyaste uppdateringarna och dataskyddet, att all data endast är tillgänglig med lösenord (bra lösenord), att alla anställda endast har rättigheter till de kritiska programmen, etc. (Bendovschi A. 2015)

Intresse av nätbedrägeri och informationssäkerhets problem fokuserar allt som oftast på själva incidenten eller vad man skall göra efter en attack. Intresse för hur man kan skydda sig för att undvika dessa attacker ligger tyvärr efter. Detta är rätt överraskande i en värld var det är en ständig kamp mellan kriminella och olika personer som försöker skydda systemet. Internet säkerhet sägs vara en ny form av krig och ses som nästa platformen i modern krigshistoria. Med tanke på detta dramatiska påstående kan man ju fundera varför det finns så lite kunnande och medvetande kring ämnet? (De Bruijn H, Janssen M. 2017)

Hadnagy et al. Beskriver i sin bok om phishing (Nätfiske) hur de har intervjuat mängder av företag som säger att de upplever stor frustration då de inte hittar information i hur de kan utbilda sina anställda på nätet (Hadnagy, C, & Fincher, M 2015 s. 35-37). Detta

känner skribenten igen efter att själv ha sökt information om hur man kan skydda sig från nätbedrägeri. Det saknas sammanställande dokument som beskriver vad nätbedrägeri är och hur man kan undvika det. Med denna information som bakgrund har jag valt att i detta examensarbete undersöka hur företag kan skydda sig mot nätbedrägeri och vad de nyaste trenderna inom cyberattacker är. På så sätt kan alla de som anser sig vara mindre insatta i ämnet, på ett enkelt sätt uppdatera sin kunskap samt lära sig hur de själva kan påverka sitt företags säkerhet. Arbetet skall vara en sammanställning av den information som hittas på nätet inom ämnet i fråga.

1.2 Syfte och frågeställningar

Syftet med detta arbete är att beskriva vad nätbedrägeri är, vilka olika typer av bedrägeri det finns, vad de nyaste trenderna är samt hur man kan förebygga en attack. Med hjälp av denna information skall personer inom företag som inte är så väl insatta i ämnet kunna fördjupa sin förståelse samt kunna bygga upp egna lämpliga strategier för att skydda sig mot nätbedrägeri. Mindre företag skall också kunna använda detta arbete för att skapa egna interna informationssäkerhets anvisningar enligt sitt behov. På detta sätt kan företag utveckla en mer säker verksamhet. Detta arbete skall vara lättläst för alla, även de som inte är så insatta i ämnet nätbedrägeri och IT system.

Frågeställningar är en viktig del av ett lyckat arbete. Klara och väl genomtänkta frågeställningar ger ofta ett bra forskningsresultat. Frågeställningarna avgör vilken typ av data som samlas in samt vilken forsknings metod som används för arbetet (Bryman A. Et al. s. 79).

För att hållas till ämnet och för att få ett bra slutresultat har dessa frågeställningar formulerats:

- Vad är nät bedrägeri?
- Vilka är de nyaste trenderna inom nät bedrägeri?
- Hur kan företag skydda sig mot nät bedrägeri?

2 METOD

Kvalitativ forskningsmetod kan beskrivas som en strategi som föredrar ord framför kvantitet/numror då man samlar in data samt då man analyserar data. Kvalitativ metod brukar också användas som ett paraplybegrepp för strategier som används för att förstå hur människan tänker, upplever samt förstår omgivningen. (Hammersley M. 2013, s. 12-13)

Kvalitativ forskning har tyngden på att generera samt utveckla beskrivningar och förklaringar än att testa för handläggande hypoteser. Kvalitativ forskning är inte heller lika styrd som kvantitativ forskning, till exempel intervjuer utförs ofta relativt ostrukturerat och styrs därmed inte alltid av intervjuaren. (Hammersley M. 2013, s. 12-13)

Ifall man vill studera redan befintlig data genom ett annat perspektiv eller dimension, så har den kvalitativa metoden i sådana fall ett egenvärde för att nå djupare eller bättre förståelse. (Säljö R. Et. Al. 2010 s.58)

Med denna information som bakgrund kommer det att användas en kvalitativ metod för att samla in data för detta arbete. Då avsikten är att sammanställa informationen som finns tillgänglig känns detta som rätt metod för detta arbete.

2.1 Allmän litteraturöversikt

En allmän litteraturöversikt är ett kvalitativt sätt att belysa det aktuella kunskapsläget inom ett visst område. Denna metod anses vara bra att använda då det inte finns stora mängder goda artiklar att basera en analys på (Forsberg & Wengström, 2008).

Största skillnaden mellan en systematisk litteraturöversikt och en allmän litteraturöversikt är att den allmänna inte har lika strikta krav på att redogöra sökstrategin. Detta betyder dock inte att den allmänna bygger på en sämre sökning. Susanne Gustafsson på Karolinska institutet skriver att det alltid är frågan om en litteraturöversikt ifall skribenten svarar nej på någon av följande frågor:

- Har jag en tydlig klinisk fråga med etablerade inklusions- och exklusionskriterier?

- Är vi minst två personer som kan gå igenom resultatet?
- Har jag tid att gå igenom en väldigt stor mängd artiklar?
- Finns det resurser att (om möjligt) översätta material som är på ett språk som inte behärskas i gruppen? (Gustafsson Susanne, 2015)

I detta arbetets fall svarar skribenten nej på en del av dessa frågor, därmed är detta arbete en litteraturöversikt och inte en systematisk litteraturstudie.

2.2 Tillvägagångssätt

Som metod för detta arbete används allmän litteraturstudie (litteraturöversikt) för att samla in material till teoridelen. Eftersom ämnet som undersöks är relativt nytt, finns det begränsat med forskningar som är pålitliga och av bra kvalité.

Syftet med en allmän litteraturstudie är i detta fall att sammanställa en beskrivande bakgrund av det material som hittas på nätet samt som tryckta källor. Med hjälp av denna sammanfattning skall det vara möjligt att beskriva kunskapsläget inom detta område.

Orsaken till att denna metod används är just på grund av avsaknaden av forskningar. Ifall det skulle finnas tillräckligt med relevanta forskningar skulle en systematisk litteraturstudie ha varit en mer passande metod. (Forsberg C. & Wengström Y., 2013 s. 25)

Material (sekundärdata) som används för detta arbete är vetenskapliga artiklar, böcker, tidningsartiklar, kursmaterial samt publikationer.

Första delen av arbetet kommer att beskriva vad nätbedrägeri är och vad för typs attacker det kan vara frågan om. Dessutom kommer det beskrivas vad en attack har för konsekvenser på företaget. Andra delen av arbetet kommer att fokusera på vad man kan göra för att undvika dessa attacker. Arbetet kommer att baseras på resultaten av litteraturforskningen.

2.3 Avgränsning

Jag väljer att avgränsa arbetet till små- och medelstora företag, eftersom stora företag ofta redan har interna processer för hur de hanterar sin säkerhet. Dock gäller samma information också stora företag, men eftersom de redan ofta har interna processer gjorda kommer informationen att gynna de lite mindre företagen samt privat personer som är intresserade av ämnet. Termen nätbedrägeri är väldigt bred och därmed har jag valt att avgränsa arbetet till företagens informationssäkerhet samt till hur företag kan undvika betalningsbedrägeri.

2.4 Sökprocess

Eftersom ämnet utvecklas i snabb takt har jag valt att begränsa sökandet till material som är publicerat 2010 eller senare för att det skall kännas relevant och inte föråldrat. Dessutom prioriteras material som är efter 2014. Det material som är före 2014 och väljs med i arbetet anses inte av skribenten vara föråldrat.

Databaser som använts:

- Academic Search Elite (EBSCO)
- Science direct
- ABI/INFORM
- Ebrary (E-böcker)

Sökord som använts:

- Cyber attacks
- Cyber threats
- Cyber crime
- Risks
- Risk Management
- Cybersecurity
- Cyberterrorism
- Secure payments
- Cash Management

- Phishing

Efter att ha gjort litteratur sökning med hjälp av dessa sökord och databaser har jag hittat 15 relevanta artiklar jag kommer använda i detta arbete. Förutom dessa artiklar hittades annat användbar material ur databaserna som till exempel olika tidskrifter.

Utöver det elektroniska materialet kommer böcker att användas som söks fram på Ebrary med hjälp av samma sökord som ovan.

2.5 Begreppsdefinitioner

Bedrägeri: kan innebära att man blir lurad av en gärningsman som leder till ekonomisk skada för personen i fråga. (Polisen.se)

Cybersäkerhet: Processen att skydda information genom att förebygga, identifiera och reagera på attacker. (National institute of Standards and Technology, 2017)

Nätbedrägeri: En attack som riktar sig mot cyberomgivningen och de program som drivs av den. En cyberattack kan rikta sig mot till exempel bank- och betalningssystem. (Tietotekniikan termitalkoot)

Risk management: Med risk management vill man identifiera risker samt vidta lämpliga åtgärder för att minska på skada. (National institute of Standards and Technology, 2017)

Pharming: Pharming innebär att en hacker försöker ta över kontrollen av användarens dator genom att styra in användaren från den korrekta servern till sin egen server. (Tietosuoja 2010)

Phishing/Nätfiske: E-post som sänds från en opålitlig källa i syfte om att komma åt sensitiv information eller sprida skadligt program. (Hadnagy, C, & Fincher, M 2015 s. 35)

Informationssäkerhet: Informationssäkerhet innebär hur man kan skydda den värdefulla informationen som vi har. (informationssäkerhet.se,2018)

3 VAD ÄR NÄTBEDRÄGERI?

Nätbedrägeri, eller cyberattack, är en attack som utförs från en dator till en annan dator, system eller webbsida för att komma åt sensitiv information eller tillgänglighet till offrets dator och vad som finns sparat på den(The windows club). I detta avsnitt är det meningen att reda ut vad nätbedrägeri innebär, vad de nyaste trenderna är inom nätbedrägeri samt utreda vad för skada en nätbedrägeri kan medföra. Som produkt av detta kommer sedan en guide att skapas med anvisningar för hur dessa attacker kan undvikas.

Idag har så gott som alla brotten it-koppling. De mest tydliga typerna är brott som utförs med hjälp av modern teknik, som dataintrång eller datorbedrägeri. Dagens moderna kommunikationsvägar gör att även brott som kreditkorts bedrägeri och bluff fakturor har stora elektroniska inslag. Ofta handlar det därmed om gamla brott i ny form. (Informationssäkerhet- trender 2015, s. 35)

Dell (Sonic wall) beskriver nätbedrägeri med fyra steg:

1. Informationssökning/Spaning: Angriparen börjar sin attack genom att ta reda på så mycket som möjligt om offret eller organisationen som planeras attackeras. Denna information söks ofta från öppna nätsidor och kan vara bland annat vad för aktuella projekt som är på gång i företaget eller vad för samarbetspartners de har. Målet med detta steg är att lära sig så mycket som möjligt om offret samt att hitta offrets svagheter i system och nätverk. Till den första fasen hör också skanning av företagets tjänster för att identifiera svagheter i program varorna. Cyber kriminella är färdiga att göra vad som helst för att komma åt svagheterna. (Dell, Sonic WallAnatomy)
2. Intrång och avancerade attacker: Allt efter att angriparen har identifierat svagheterna kan angriparen använda informationen för att komma åt nätverk.
3. Införing av skadliga program: Efter att man kommit åt ett nätverk kan angriparen spårlöst införa skadliga program för att kunna kontrollera systemen. Det kan vara frågan om till exempel ett skadligt program som gör att angriparen kan kontrollera på distans systemen eller till exempel ett destruktivt program för att medvetet orsaka skada i systemet. (Dell, Sonic WallAnatomy)

4. "Clean up": Fjärde och sista steget av en attack är att bli av med spåren av attacken. Det gäller också för angriparen att vara försiktig i de tidigare skedena av attacken för att behålla sin anonymitet. Målet med detta steg är att radera alla spår som blivit kvar av attacken. En professionell kriminell kan komma åt ditt nätverk utan att du ens märker det. (Dell, Sonic WallAnatomy)

För att kunna skydda sig mot en attack är det bra att veta vad en attack i teorin går ut på. Därför är det viktigt för alla anställda på ett företag att vara medvetna om dessa steg samt vad det finns för olika metoder att komma åt din sensitiva information.

(Dell, Sonic WallAnatomy)

I följande avsnitt kommer de olika nätbedrägerimetoderna att beskrivas.

3.1 Riktad attack

Kriminella som är ute efter att göra vinst utgår ofta ifrån attackera där var risken att bli fast är liten och chansen att komma åt informationen är stor. Man väljer alltså objekt som inte kräver så stor arbetsinsats för att göra vinst. Däremot om man vill komma åt en viss information kan den kriminella vara färdig att offra mera av sin tid för att lyckas attackera det bestämda målet. Detta kallas för en riktad attack. En riktad attack är en kränkning av informationssäkerheten riktad mot en bestämd aktör. Ett exempel på en sådan attack kan vara att angriparen skickar ett e-postmeddelande riktat till offret med till exempel en länk till ett skadligt program. Ifall länken öppnas kan sabotageprogrammet infektera datorn. På detta sätt kommer angriparen åt sensitiv information som finns på datorn. Angriparen kan då samla åt sig information från datorn samt utvidga angreppet till övriga delar av det interna nät som objektet ingår i. Dessa mail som rör sig är ofta väldigt trovärdiga och genomtänkta. Mottagaren kan ofta betrakta mailet som pålitligt och att det är förknippat med den dagliga verksamheten. Detta är på grund av att angriparen utför en utförlig informationssöknings process för att kunna utforma ett så trovärdigt mail som möjligt. (Finansministeriet 2009/6)

3.2 Nätfiske

Phishing, eller nätfiske/lösenordsfiske, innebär att man sänder e-post som visar sig vara sända från en opålitlig källa med mål att kunna påverka eller komma åt sensitive information. Det kan vara frågan om mail som innehåller bilagor med skadliga program, länkar som lurar dig att ladda ner ett skadligt program eller länk som lurar dig till en påhittad nätsida var du kan luras till att ange sensitiv information. (Hadnagy, C, & Fincher, M 2015 s. 35-37)

Dessa phishing försök kan vara riktade till ett visst mål, eller sedan mer allmänna som skickas ut till en större massa. De attackerna som är riktade till ett visst mål är väl genomtänkta och angriparna skriver meddelanden som är relevanta och personliga. På grund av detta kan riktad phishing vara svår att upptäcka och att försvara sig mot. (Hadnagy, C, & Fincher, M 2015 s. 35-37)

Nästan alla som har en e-post adress har varit ett mål för denna typ av nätbedrägeri någon gång. Det kan uppges i meddelandet att man skall donera pengar till ett visst konto för att hjälpa personer i behov eller till exempel ett meddelande från din bank att överlåta lösenordsuppgifter. Utöver privat personer är vanliga arbetare en stor målgrupp för denna typ av nätbedrägeri. Dessa personer kanske inte har så stor möjlighet att själva påverka, men ifall de ger ut lösenord/sensitiv information kan det ha drastiska följder för företaget. (Hadnagy, C, & Fincher, M 2015 s. 35-37)

Phishing är ett väldigt vanligt sätt för cyber terrorister/kriminella att komma åt sensitiv information och kan medföra enorma ekonomiska konsekvenser för ett företag. Därför är det väldigt viktigt att alla som arbetar på just ditt företag är medvetna om denna risk. (Hadnagy, C, & Fincher, M 2015 s. 35-37)

3.3 Pharming

Pharming innebär att en hacker försöker ta över kontrollen av användarens dator genom att styra in användaren från den korrekta servern till sin egen server. Hackern smyger in ett spionprogram på datorn som hjälper till att ta över kontrollen, med hjälp av detta program kan angriparen styra kommunikationen till sina egna sidor. Avsikten med detta är att försöka få användaren att överlåta hemliga identifikationskoder och annan

information som gör att angriparen kommer åt sensitiv information som till exempel bank koder. Skillnaden mellan Phishing och Pharming är att med Phishing försöker angriparen öppet få information av offret, medan i Pharming försöker angriparen få information utan att användaren är medveten om det. (Tietosuoja,2010)

3.4 Online betalnings bedrägeri

Det förekommer mer och mer transaktioner online då mer och mer av försäljningen flyttar sig online. Detta innebär också att antalet brott som sker ökar inom näthandeln. Angriparna riktar sig då på personer som köper, säljer eller handlar online. Det finns många olika sätt angriparna kan lura pengar åt sig via online handel. Här är några exempel:

- Genom att annonsera produkter till billiga priser, men aldrig skicka några varor till den betalande kunden.
- Rikta sig mot företag för ett försök på att fakturera dem för tjänster som aldrig funnits.
- Dra nytta av naturkatastrofer genom att föreställa sig vara välgörenhetsorganisationer som begär donationer

(Australian cybercrime online reporting network, 2018)

3.5 CEO Fraud

Personer i företag som sköter om betalningar kan också bli uppmanade att fort betala en räkning av någon som påstår sig vara företagets Vice Direktör. Detta kallas CEO Fraud/Vice Direktör bedrägeri och har med de senaste åren blivit allt vanligare.

Angriparna närmar sig företagets ekonomiavdelning eller annan avdelning som sköter om betalningar av räkningar eller förflyttning av pengar med hjälp av identiteten av Vice Direktören. Den falske direktören ber personer med rättigheter till att göra betalningar att föra över en viss summa pengar till ett visst konto. Ofta tilläggs ännu det att betalningen är försenad för att skapa extra mycket press på offret. Ett annat sätt som används är att skicka betalnings kommandon på en fredag eftermiddag då den anställda redan har börjat fundera på att åka hem för att fira helg.(Viestintävirasto, 2015)

Också i dessa fall har angriparen ofta gjort en grundlig informationssökning av företaget och gjort en e-post adress som är väldigt lik företagets egen webb adress. Dessa små skillnader i adresserna missas lätt ifall offret har bråttom eller är ouppmärksam. Det är också möjligt att e-posten kommer från Vice Direktörens riktiga e-post, som har blivit hackad. Därför är det viktigt att alla betalningar bekräftas av fler personer innan betalningen skickas iväg (Viestintävirasto, 2015). Andra sätt att bekämpa felaktiga betalningar kommer att gås noggrannare igenom senare i detta arbete.

3.6 Falska fakturor

Denna typ av bedrägeri går ut på att angriparen kommer åt till exempel en leverantörs faktura och byta ut det riktiga kontonumret till ett tredje parts kontonummer (angriparens). Denna typs bedrägeri riktas ofta till fakturor med större summor att betala. Angriparen är också här ofta väl förberedd och pålitlig eftersom ett noggrant bakgrunds jobb görs innan den riktiga attacken utförs. Angriparen kan komma åt en faktura genom att:

- -hacka sig in på någondera partens epost konto för att få reda på information om fakturan
- -få information av opålitliga anställda (anställda kan också vara den kriminella)
- skicka e-post från en felaktig- men liknande epost adress som leverantören använder
- utförlig research av information som finns tillgänglig om företagen i fråga på nätet
- genom att komma åt en faktura med hjälp av den vanliga posten och ändra uppgifterna på original fakturan. (Cripps: Invoice Fraud- a real threat to your business, 2015)

Fakturan ser ofta väldigt lik ut den riktiga som kommer från leverantören men den anställda som skall betala fakturan kan enkelt betala fakturan utan att dubbelkolla kontonumrets ursprung och övriga alarmerande aspekter. Trots att kunden inte vet om att den betalar fakturan till en kriminell, försvinner inte skyldigheten att betala original fakturan till leverantören. Detta medför en ekonomisk förlust för företaget. Det är normalt då leverantören skickar påminnelser om fakturan som det kommer fram att företaget blivit lurat. (Cripps: Invoice Fraud- a real threat to your business, 2015)

3.7 Cyberstalking

Detta är en ny typ av bedrägeri var angriparen aktivt följer med allt vad personen i fråga gör online. Angriparen följer inte fysiskt med vad personen gör, utan följer med vad personen har för online aktivitet för att få fram så mycket information om personen i fråga som möjligt. Denna informationen kan till exempel användas med att plåga personen i fråga, vilket är ett brott mot personens integritet, eller att till exempel använda informationen för att utföra något annat brott i personens namn. Denna typ av kriminalitet inkluderar även pedofiler och andra sexuella brott. (Digit.in 2018)

3.8 Identitetsstöld

Identitetsstöld förekommer då angriparen kommer åt personlig information som sedan används för att till exempel stjäla pengar eller utföra övriga kriminella aktiviteter. Personlig identitetsstöld innebär att en oauthoriserad person kommer åt en persons sensitiva information som används för att komma åt pengar, ägendom, eller för att åstadkomma annan kriminell aktivitet. Till en persons personliga information hör namn, adress, telefon nummer, körkortsnummer, social skydds nummer, var man arbetar, arbets id, kontonummer, kreditkortnummer och så vidare. (Collins, JM 2016 s. 8-9)

Med hjälp av denna information kan angriparen komma åt spar-, och pensionskonton, öppna nya kredit kort, ta över existerande konton, köpa tjänster online, vara delaktig i pengatvätt och övrig organiserad kriminell funktion och så vidare. Listan på olika möjligheter är lång på vad en kriminell kan göra med en persons identitet. (Collins, JM 2016 s. 8-9)

Kriminella kan komma åt din personliga information bland annat genom:

- Nätfiske, du kanske avslöjar information via telefon eller internet till fel person.
- Att komma åt dina online konton
- Söka fram personlig information från social media
- Olagligt söka information om dig som finns sparad på företagets databas.

(Australian cybercrime online reporting network, 2018)

Företags identitetsstöld innebär att angriparen koncentrerar sig på företagets sensitiva information. Denna typ av identitetsstöld har blivit allt vanligare på grund av att företag ofta har högre kreditgränser än en privat person, de har fler händelser på kontona vilket gör det svårare att bli upptäckt, det finns ofta fler personer i företaget som har tillgång till kontot vilket också gör det svårare att upptäcka den kriminellas fotspår.

(Collins, JM 2016 s. 9-10)

3.9 Kriminalitet bland de anställda

Oförsiktiga anställda som sparar sensitiv information på osäkra platser för att underlätta det egna jobbet medför en stor risk för företaget. Risker här kan vara till exempel att dela maskiner med andra anställda, före filer över till hemdatorn eller genom att ge bort lösenord. (Computer Fraud and Security, 2015, s. 6)

Förna anställda som tar med sig data efter avslutat arbetskontrakt är ett brett problem världen runt. Det har visat sig att tidigare anställda ofta tar med sig material från arbetsplatsen oberoende av vilka omständigheter arbetskontraktet avslutats. De tidigare anställda använder företagets information hos den nya arbetsgivaren. Det kan vara frågan om allt från affärsidéer till kunduppgifter/kontakter. Detta kan orsaka stora problem för den tidigare arbetsplatsen. (Computer Fraud and Security, 2015, s. 6)

3.10 Internetbaserad kriminell tjänstsektor

Arbetsdelning och specialisering inom områden gäller även hos kriminella. Crime-as-a-service är en kriminell internetbaserad tjänstesektor som erbjuder färdiga komponenter som kriminella kan köpa för att utföra deras egna attacker utan att behöva göra allt själva. Ett exempel på detta är webbhotell som ger kriminell driftsäkerhet och anonymitet. Dessa webbhotell sätts upp i länder med svag- eller obefintlig it-lagstiftning, vilket gör det extremt svårt att få serverna nedstängda eller att spåra vem som ligger bakom. (Informationssäkerhet- trender 2015, s.36-37)

Ett annat exempel är malware-as-a-service. Detta är olika färdiga lösningar med skadliga koder som kan återanvändas i olika sammanhang. Denna verksamhet har tjänster som liknar kommersiella företag såsom kundsupport, uppdateringar och utveckling av produkter. Med hjälp av programmet försöker de kriminella få skadliga program nedladdade till offret och på det sättet komma åt sensitiv information. (Informationssäkerhet- trender 2015, s.36-37)

Ransomware är en skadlig kod som installeras på offrets dator som gör det möjligt för angriparen att kryptera datorn eller delar av material som finns på datorn. Angriparen kräver sedan den attackerade en summa pengar för att denne skall återfå kontrollen över sin egen dator. (Informationssäkerhet- trender 2015, s.36-37)

3.11 Vem har ansvar för företagets risker?

Det sägs att risk hanteras på alla olika nivåer i ett företag, men riskerna ägs av styrelsen och ledningsgruppen. Det slutliga ansvaret att leda och hantera företaget och dens risker ligger här. Även om aktiviteter kan delegeras neråt i organisationen kan ansvar aldrig delegeras. Därmed skall det vara i ledningsgruppens djupaste intresse att se till att företaget har bra risk hanterings program och ett fungerande skydd mot nätbedrägeri. Ledningsgruppen skall även se till att hela personalen, på alla nivåer, är medvetna om hur viktiga de är i kedjan mot ett säkrare företag. (Touhill G. et al., 2014 s. 38)

3.12 Case:

Det finns otaliga exempel på både företag och privat personer som blivit utsatta för nätbedrägeri attacker. Bland stora företag kan bland annat google, Yahoo!, UPS och eBay nämnas. Tyvärr är det väldigt vanligt att företag inte rapporterar sina attacker på grund av de ryktet en attack kan medföra företaget. Nedan beskrivs ett case som utsatte eBay för en känd attack.

CNBC rapporterar år 2014 att eBay utsatts för en attack var de kriminella kommit åt en databas som innehöll krypterade lösenord, adresser samt telefon nummer. Det har inte hittats några bevis på att de skulle ha kommit åt finansiell information eller kredit korts

information. Företaget berättar att de kriminella kom åt informationen via oförsiktiga anställdas internet beteende. (CNBC, 2014)

Strax efter attacken sänkte företaget finansiella målsättningarna för året. Följderna av attacken syntes i företagets andra kvartal rapport då det rapporterades att den breda attacken gjorde att försäljningsvolymen minskade. Också användar aktiviteten minskade jämfört med innan attacken. Trots detta var ändå det finansiella resultatet i stort sätt bättre än förväntat. Användare och experter kritiserade stort eBays bristande i kommunikation om vad som hänt, samt hur dåligt de implementerade lösenords bytandet för användarna, de anser till och med att detta var det som orsakade mest skada för företaget. (SC Media, 2014)

Attacken ledde till att eBay aktier föll med 3,2 %. Dessutom orsakar dessa attacker alltid ett dåligt rykte för företaget och det kan vara svårt för kunderna att lite fullt ut på att deras sensitiva information är i säkra händer. (CNBC, 2014)

4 VILKA FÖLJDER HAR EN ATTACK?

Trots alla tekniska sårbarheter som finns, är oftast människan i systemet som är den svagaste länken och luras till att ladda ner skadliga program eller uppge sensitiv information. Trots att allt fler organisationer inför bestämmelser för informationssäkerhet är steget till ordentlig säkerhet långt. Enkla tekniska hjälpmedel för angrepp har sänkt tröskeln för bedrägeri och satt verktyg i händerna för allt fler angripare. De mest kvalificerade angreppsverktygen är ännu hårdvaluta och behållna hos en mindre krets kriminella. (Informationssäkerhet- trender 2015, s. 41)

Information är lätt tillgängligt för vem som helst. Detta kan upplevas som en positiv sak men med tanke på cybersäkerhet medför detta stora krav såväl på företag som på privat personer. Förutom de ekonomiska följderna en attack medför står ett företags rykte på spel när det kommer till informationssäkerhet, ifall sensitiv information läcker ut i fel händer kan det ha drastiska följder. (Tiganoaia B., 2015 s. 239). Till följande presenteras en del av hoten som uppkommer i cybervärlden för företag.

1. Personlig data (Informationssäkerhet): Ifall personlig data läcker ut från ett företag kan det medföra stora förtroende problem i framtiden. Det kan vara frågan om att kundens uppgifter, anställdas uppgifter eller till exempel affärsrelationer kommer i fel händer. Ett företags rykte kan skadas enormt ifall detta händer.
2. Finansiell data (Informationssäkerhet): Med finansiell data menar man att kreditkorts uppgifter eller bank uppgifter kommer i fel händer. Det kan vara frågan om företagets egna finansiella uppgifter, kundens uppgifter eller personalens uppgifter. Alla alternativ kan medföra stora ekonomiska följder samt ett försämrat rykte för företaget.
3. Immateriella rättigheter (Informationssäkerhet): Offer för denna typ av hot är alla företag som utvecklar produkter/tjänster eller forskar inom olika delområden. Då kan det betyda att angriparen kommer åt en produkt som inte ännu är lanserad och lanserar produkten tidigare med ett billigare pris. Detta medför att originalprodukten och företaget som utvecklat produkten inte mera har nytta av sin produkt. Detta i sig medför stor ekonomisk förlust eftersom originalprodukten har tappat sitt värde.
4. Överföring av skadliga program (System relaterade hot): I alla metoder där angriparen kommer åt ett företags dator och system kan följderna vara enorma ekonomiskt. Med hjälp av dessa system relaterade attackerna kan angriparen komma åt sensitiv information samt göra skador på systemen. Allt detta medför såväl ekonomiska som förtroende följder för ett företag.

(Van der Meulen N. 2015 s. 14-17)

I forskningen gjord av Nicole van der Meulen (2015) berättar de intervjuade att de upplever företagets rykte som det största hotet ett företag upplever.

Vissa företag väljer att inte berätta om att deras företag blivit utsatt för nätbedrägeri just av denna orsak. Dessutom har forskning visat att en cyberattack har visat sig påverka ett företags aktiekurs negativt (Informationssäkerhet- trender 2015, s.36-37)

Oftast är det så att en människa blir medveten om ett problem först då de själva förstår eller upplever vad problemet kan medföra. Ett stort problem inom informationssäkerhet är just detta att företag gärna gör sitt allt för att hålla dessa attacker hemliga och då tror

omgivningen att det inte är ett så stort problem som det verkligen är då de inte hör något om det. (De Bruijn H, Janssen M. 2017)

Att återskapa förtroende hos en kund eller motsvarande part kan vara väldigt arbetskrävande och svårt. Alla dessa hot som nämns ovan är bara en del av orsakerna varför det är enormt viktigt att förebygga dessa attacker så gott man kan.

5 HUR KAN MAN SKYDDA SIG?

I följande avsnitt av detta arbete kommer resultatet av den allmänna litteraturöversikten att presenteras. För att kunna hantera nätbedrägeri risker måste det finnas förståelse för organisationens risker och vad som skall prioriteras. Varje företag har unika behov, varav det inte finns ett rätt svar på vad företag borde göra för att på bästa sätt skydda sig mot nätbedrägeri. Tanken är att man med stöd av detta arbetet skall kunna bygga upp sina egna interna processer enligt företagets unika behov. Med hjälp av dessa lättlästa råden skall alla (oberoende kunskap om nätbedrägeri) kunna bekanta sig med vad man som enskild person kan göra för att minska risken att bli utsatt för en attack, samt vad för säkerhetsåtgärder företagsledningen kan tänka på. Man kan till exempel börja med att bygga upp sin egna checklista med vad för svagheter företaget har. Med hjälp av dessa frågor kan man avgöra ifall det finns en säkerhetsrisk då det kommer till rättigheter och skyddandet av sensitiv information:

- Har ni immateriella rättigheter som måste skyddas?
- Har ni just nu eller i framtiden konkurrenter på marknaden som skulle kunna ha nytta av att ha tillgång till era immateriella rättigheter?
- Har ni dessa immateriella rättigheter sparade på ett dator system?
- Är era dator system kopplade till internet?
- Har era datorer USD uttag var det är möjligt att koppla oönskade USD stickor?
- Gör ni regelbundna och frekventa schemalagda back-ups över viktig information?

- Sparar ni denna back-up informationen på ett säkert off-line ställe?
- Använder ni dataflöden från övriga källor till erat system?

Ifall det svaras ja på en av dessa frågor har redan företaget en stor nätbedrägeri risk och säkerhetsåtgärder skall finnas på plats. (Touhill G. et al., 2014 s. 39)

Då det gäller tekniska delen av att skydda sig mot nätbedrägeri kan dessa frågor vara bra att ställa för sig:

- Har du eller ert företag blivit utsatt för en attack?
- Har ni hittat skadliga koder som virus till exempel i era system?
- Finns det andra som använder erat nätverk?
- Finns det nyare versioner av preventionssystem och detektions system som ni inte uppdaterat till?
- Sparar ni data i målnet?
- Använder de anställda telefoner, tabletter eller datorer för att utföra sina dagliga uppgifter?
- Litar ert företag endast på lösenord för att komma åt nätverket och informationen?
- Tillåter ni att koppla upp från främmande platser?

Ifall ni svarat ja på ens en av dessa frågor, har ni en teknisk risk i processerna och säkerhetsåtgärder skall utföras. (Touhill G. et al., 2014 s. 43)

Det är viktigt att analysera vilken information eller vilket system som har en hög riskprofil och som kommer att behöva starkt skydd samt vilka system som har en mindre riskprofil eller var det inte är så farliga konsekvenser ifall en attack skulle ske. (Henning N. 2018)

5.1 Teknik och programvaror

Genom att använda sig av teknik kan man delvis skydda sig mot nätbedrägeri. Man kan investera i olika preventionssystem & detektions system som till exempel brandväggar och

antivirus program. Dessa program fungerar ofta som en bra grund hos alla företag (Leklinder T. 2017).

En hacker kan ofta tillbringa lång tid inne i ett system innan något faktiskt attackeras. Därmed är monitorering av kommunikations aktivitet det bästa sättet att upptäcka en hacker innan något värdefullt försvinner. Det finns system som sköter denna typs av monitorering, dessa kallas Security Information and Event management System (SIEM). Systemet känner igen onormalt beteende som till exempel om någon försöker logga in på en otypisk tidpunkt eller ifall någon har många misslyckade login försök följt av ett lyckat och så vidare. (Leklinder T. 2017)

Då företaget väl investerar i ett system av något slag är det viktigt att systemen också uppdateras regelbundet. Ett ouppdaterat system är alltid en risk. Då ett fel i systemet hittas börjar systemadministratorerna jobba med en ny version var problemet är åtgärdat. Då denna nya versionen är publicerad rekommenderas det att man uppdaterar sina egna system så fort som möjligt. Problemet är att kriminella i det skedet vet om att det funnits ett problem i det gamla systemet och det tar inte länge innan de hittar var felet ligger och kan använda sig av sårbarheten för att utföra en attack. Ifall användaren inte uppdaterat sitt system till den nyaste versionen, är den utsatt för en risk i den gamla versionen. (Yadron D. 2015)

Ett preventionssystem är en viktig del av säkerhetsåtgärder inom datasäkerhet. Dock räcker inte enbart ett bra system för att undvika attacker eller läckage av information om inte personalen har kunskap. (Jepp A. 2017)

5.2 Användarens riskprofil

Inom företag skall den enskilda individens användarprofil vara noggrant anpassad till användarens arbetsuppgifter. Det är viktigt att identifiera vad för information som skall vara tillgängligt till vem. Personer som lämnar företaget skall inte ha möjligheten att ta med sig sensitiv information vidare till nästa arbetsplats. Personen i fråga skall inte ha

tillgång till systemen efter att hon eller han lämnat företaget och profilen skall raderas så att inga oanvända profiler blir aktiva. (Bendovschi A. 2015)

En person som lämnar företaget kan till exempel få för sig att ta med en kopia på en hård disk med information om immateriella rättigheter till ett konkurrerande företag som anställt honom eller henne. (Touhill G. et al., 2014 s. 40)

En person skall inte heller kunna göra transaktioner på egen hand eller ändra på till exempel en användares rättigheter. Detta kallas två faktors autentisering och skall anpassas genom hela organisationen. Med hjälp av denna metod kan man undvika att en person till exempel betalar in pengar till sitt egna konto. (Gualdoni J., et al. 2017)

Autentisering av användare skall vara enligt företagets policy och behov. Det vanligaste sättet att identifiera sig själv i ett system är genom att ha ett användarspecifikt användarnamn och lösenord. Dessa lösenord skall vara tillräckligt starka och inte tillgängliga för någon annan person. Lösenord är inte alltid tillräckligt för att skydda sin profil. Det finns olika typer av random pin genererande system som kan användas för att skapa ytterligare starkare skydd. Dessa system genererar vid inloggning en engångs kod till exempel på användarens telefon. Dessutom finns det olika biometriska lösningar av identifiering som till exempel fingeravtryck. (Bendovschi A. 2015)

Också maskiner som är inaktiva är bra att hålla offline eftersom inaktiva maskiner ofta är oskyddade och omoniterade. Ifall dessa dessutom är kopplade till internet är det ett sätt för inträngaren att komma in i företagets system. Av samma orsak skall oanvända användarkonton och profiler genast raderas då de inte är nödvändiga mera. (Yadron D. 2015)

5.3 Praktiska råd för säkra lösenord

1. Sträva efter att komma på ett lösenord som du kan minnas i ditt minne.
2. Spara inte ditt lösenord på en lapp på bordet, eller till exempel i telefonen.
3. Använd inte dig av lösenord som kan vara lätta att lista ut, som till exempel P@ssW0rd, din hunds namn eller din födelsedag. Det finns system som de kriminella använder för att skanna igenom alla vanligaste lösenord. Dessutom

ifall de gör en ordentlig genomgång av användaren, hittar de information om familjemedlemmar etc online.

4. Lösenord med 14 eller fler tecken är statistiskt sätt mest säkra.
5. Dela aldrig ditt lösenord med någon annan
6. Använd aldrig ditt lösenord till flera än ett ställe
7. Var säker på att du har stora- och små bokstäver, siffror och tecken i ditt lösenord.
8. Ändra lösenordet ofta. Det rekommenderas att det görs varje kvartal. (Touhill G. et al., 2014 s. 46)

5.4 Personalens attityder

Säkerhet innebär ansvar både för människor och system, men hur komplext detta egentligen är faller långt ifrån den vanliga individen. Djup kunskap om säkerhet, IT infrastruktur och vilka typer av attacker som är möjliga är viktiga för att på riktigt förstå vad som pågår. Dock är det inte endast teknologi som spelar en roll i säkerheten. Det har konstaterats att människan är den svagast länken inom internet säkerhets kedjan. Människan är den som skall se till att systemen är uppdaterade, att attacker upptäcks i tid, och att preventiva åtgärder görs. (De Bruijn H, Janssen M. 2017)

I en forskning utförd av Lee Hadlington (2017) är en av nyckel fynden att en anställds attityd gentemot nätbedrägri korrelerar negativt med riskerande internet beteende. Alltså ifall den anställda har en bra kunskapsbas att stå på och företaget har uppmuntrat de anställda till att vara försiktiga är också det mindre sannolikhet att den anställda har ett riskfyllt beteende som senare kan resultera i att företaget blir attackerat.

Impulsivt beteende är också en risk för företagets säkerhet. En person som ofta agerar impulsivt agerar på motsvarande sätt då det kommer en hotfylld situation som till exempel ett mail med en link som man rekommenderas att trycka på. Dessa personer reagerar först och tänker inte efter vad deras reaktion kan leda till för företaget. (Hadlington L, 2017)

Ett annat attitydsproblem hos människan är att man ofta tänker att detta inte kommer att hända mig/mitt företag. Det kanske händer ett annat företag, men inte mitt. Tankesättet är oftast att de företaget som blev attackerat är sämre skyddat än vad det egna företaget är. Denna attityd kan kosta företaget mycket. (De Bruijn H, Janssen M. 2017)

Därmed kan det starkt rekommenderas att företag lägger ner tid på att bygga upp interna processer som de anställda får en positiv attityd gentemot informationssäkerhet. I samma forskning visas dock att 58% av de som deltog i forskningen inte vet hur de kan skydda sitt företag mot nätbedrägeri. Dessutom anser 98 % av de som deltog att säkerhet hör till ledningsgruppen och de högre uppsatta på företaget. (Hadlington L, 2017)

Ett sätt att ändra på denna siffra är att se till att information kommuniceras till hela företaget. Alla skall veta vad de personligen kan göra för att vara en mindre risk för sitt företag. Att ha en informationssäkerhets policy inom företaget kan vara ett sätt att ha sammanställande information om vad som förväntas av personalen. Nedan beskrivs kort vad en informationssäkerhets policy är.

5.5 Informationssäkerhets Policy

Informationssäkerhet är fortfarande en av de mest kritiska faktorerna för de moderna organisationerna. Informationssäkerhets policyn fastställer interna regler inom organisationen som till exempel tillgänglighet av data. Denna policyn skall finnas till för att personalen skall veta vad som förväntas av dem då det kommer till informationssäkerhet, då vi är medvetna om att personer som saknar kunskap kan medföra stora säkerhetsrisker; som till exempel, att använda ett sårbart lösenord, installera otillförlitliga program på datorn eller att använda osäkra applikationer. (De Bruijn H, Janssen M. 2017)

Trots att företag relativt aktivt har av dessa interna policyn händer det allt för ofta att personalen, medvetet eller omedvetet, bryter mot policyns riktlinjer. Detta leder till en risk inom informationssäkerhet. Detta beror ofta på att policyn är bristfällig, otydlig, svårläst eller att den inte anses som prioritet bland anställda. (Alqahtani F. 2017)

En informationssäkerhetspolicy kan innehålla bland annat information om:

- Anvisningar och krav på användarnas lösenord. Längd på lösenordet, siffror och märken, byte av lösenord med jämna mellanrum. Hur lösenord skall förvaras etc.
- Anvisningar och krav på användning av arbetsplatsens e-post. Öppnande av bilagor och vidarebefodrande av e-post.
- Anvisningar och krav på hur internet får användas. Installering av program på arbetsdatorn, vistas på orelevanta internet sidor, osakligt användande av internet. Anvisningar om att använda sociala medier på arbetsdatorn skall tas i beaktande.
- Anvisningar för till vilken typ av externt nätverk som arbetsdatorn får kopplas till. Är det ok att sända sensitiv information via dessa nätverk eller via telefonen?
- Anvisningar och krav på hur sensitiv information skall behandlas. Hur skall dokument som inte längre behövs förstöras? Användning av externa USB stickor. (Alqahtani F. 2017)
- ETC

Det finns många saker som är bra att ha i en intern informationssäkerhets policy. Varje organisation är unik och måste bygga upp sin egna policy enligt företagets specifika risker. Eftersom omgivningen inom detta område utvecklas i snabb takt är det viktigt att informationssäkerhets policyn regelbundet uppdateras.

För att denna policyn skall läsas av de anställda och faktiskt följas, är det viktigt att man inom företaget ser det som en prioritet att skola personalen inom ämnet och dessutom gör anvisningarna lättlästa och tillgängliga för alla. (Alqahtani F. 2017)

Här följer några steg som kan vara bra att tänka på då man börjar utveckla en informationssäkerhets policy:

1. Identifiera: Genom att förstå organisationens kritiska funktioner samt vad deras risker/svaga punkter är kan organisationen enklare prioritera skyddet till rätt

tillgång. För att detta skall vara möjligt är det kritiskt att man känner till organisationen väl samt vad för risker man eventuellt kan vara utsatta för. Detta kan med andra ord kallas risk management.

2. Skydda: Utveckla och implementera metoder för att skydda kritiska system och tillgångar. Till detta steg hör allting från data säkerhet och informationsskydd till personalens kunskap och skolning.
3. Upptäcka: Trots att man vill undvika att utsättas för en attack händer detta tyvärr ibland. Därför är det viktigt att man har sätt att upptäcka en attack. Till detta steg hör monitorering samt att ha olika system/program som upptäcker onormalt beteende i systemen.
4. Reagera: Utveckla och implementera en strategi för vad som görs ifall en attack upptäcks. Till detta steg hör reaktionsplan, kommunikation och analys.
5. Återhämta: Vad skall göras efter att en attack är över för att kunna återgå till vardagen så fort som möjligt? Utveckla och implementera passande aktiviteter för att återhämta tillgångar eller servisar som blivit attackerade. Dessutom skall det i detta skede också finnas en plan för hur man kan undvika en ny attack.

(National institute of Standards and Technology, 2018)

5.6 Förberedelser för en attack

En attack kommer att ske, förr eller senare. Då lönar det sig att vara så väl förberedd som möjligt för att minimera skadan som kommer att ske.

Det finns många som inte gör bra back ups på den kritiska informationen som företaget har. Ett bra tips är att analysera vad som verkligen är så viktigt att det måste sparas på en säker plats. All information är inte lika viktig, finns det för mycket information kan det vara en för stor helhet att hålla koll på.

Cybersäkerhets försäkring kan vara bra att ha. Denna marknaden växer hela tiden och det blir allt vanligare att företag köper en försäkring inom detta området. Alla företag väljer inte att investera i försäkring mot nätbedrägeri, det är upp till varje företag att analysera sin situation och avgöra om en försäkring är nödvändig eller inte.

Det kan vara bra att ha en krisplan samt en plan för hur företaget kan repa sig efter en attack. Desto bättre man är förbered, desto effektivare kan man jobba mot en normal vardag efter en attack. Identifiera alla olika scenario och bygg planer för att vara förberedd då en attack sker. (Touhill G. et al., 2014 s. 299)

6. DISKUSSION

Denna avhandling undersökte vad för information som fanns tillgänglig angående ämnet nätbedrägeri och prevention av nätbedrägeri. Syftet med detta arbetet var att på ett beskrivande sätt sammanfatta information om vad nätbedrägeri är och hur man kan skydda sig mot det.

Nätbedrägeri är ett väldigt aktuellt ämne och kommer att fortsätta vara det också framöver då teknologin utvecklas och världen blir mer och mer internet baserad. Behovet av informationssäkerhet växer i och med vårt stora behov av internet och internet baserade tjänster. Detta kommer medföra allt större ansvar på den enskilda individen, både för att arbetsplatsens information skall bevaras säkert, men också för att man inte själv skall råka ut för nätbedrägeri. Information om vad korrekt internet beteende är skall därför finnas tillgängligt för alla.

Följderna för nätbedrägeri kan vara katastrofala. Det kan vara frågan om personlig data som läckt ut, finansiell data som kommit i fel händer, immateriella rättigheter som kopierats eller till exempel överföring av skadliga program. Olika attacker har olika följder, men ändå anses företagets rykte vara det som skadas mest. Att återfå förtroende hos en kund eller motsvarande part kan vara väldigt svårt.

Avhandlingens resultat visar att det oftast är människan i systemet som anses som den största risk faktorn då det gäller nätbedrägeri. Forskningar visade att de anställdas attityder mot informationssäkerhet var starkt korrelerat med risken för att utsätta företaget för nätbedrägeri. Därmed är det starkt rekommenderat att se till att alla företag,

stora som små, ser informationssäkerhet som en prioritet då det kommer till att skola sina egna personal.

Det kan alltså vara frågan om personal som inte är medvetna om vad som räknas till riskfullt beteende- eller så kan det till och med vara frågan om en person som medvetet utsätter företaget för en attack för egen nytta. I och med att detta är en av de största orsakerna till att en attack kan uppstå skulle det vara intressant att undersöka vad företag gör för att se till att den egna personalen är utbildad. Även många forskningar tog upp hur viktigt det är att företag har deras egna informationssäkerhets policyn, men det är dock oklart hur aktivt personalen verkligen läser den eller är medvetna om att den ens existerar. Detta skulle kunna fungera som ett framtida examensarbete för en person som har intresse av att se över företags interna informationssäkerhets processer.

Det är överraskande hur alla forskningar visade samma sak angående hur omedvetna vi egentligen är om de stora rikserna som cybercrime har medfört trots att det redan pågått en god stund. Ett problem är säkert då många företag inte rapporterar till allmänheten om att de blivit utsatta för att skydda sitt egna rykte? Då blir inte allmänheten medvetna om hur frekventa dessa attacker är, och kanske inte tror att det kan hända till en själv.

Då informationssökningen för detta arbete utfördes, var fokus mer på att hitta material om vad nätbedrägeri är samt om hur man kan skydda sig mot nätbedrägeri. I dagsläget då dessa attacker blir mer vardag än undantag skulle det säkert finnas intresse av att ha en sammanfattande guide över vad man skall göra ifall man blivit utsatt och vad för konsekvenser man kan förvänta sig. Detta kunde vara ett annat exempel på ett framtida examensarbete inom ämnet.

Arbetet har uppnått sitt syfte då svar på alla frågeställningar kan hittas i arbetet, vilket det i detta fall gör. Största utmaningen var att hitta bra och pålitligt material då det inte forskats så mycket inom detta relativt nya ämne. Därmed kan man konstatera att arbetets metod, allmän litteraturöversikt, var passande för detta ändamål. Däremot kan man konstatera att det konstant kommer mer och mer material om ämnet, vilket också

visar att intresse har börjat växa. Redan under denna tid då arbetet skrevs hann situationen med material ändra relativt drastiskt.

De olika sätten som attacker kan utföras på utvecklas med snabb takt, vilket gör att sätten att skydda sig på också måste anpassa sig. Därmed kan det vara att denna information inte kanske mer är lika aktuell efter några år. Trots detta kan informationen i arbetet ändå ses som en bra grund för säkert beteende inom internet världen, och därmed alltid på något vis aktuell.

KÄLLOR / REFERENCES

Alqahtani F. 2017. Developing an information security policy: A case study approach
Hämtad: 21.4.2018

Tillgänglig: <https://www-sciencedirect-com.ezproxy.arcada.fi:2443/science/article/pii/S1877050917329745>

Australian Cybercrime Online Reporting network. Online trading issues

Hämtad: 16.05.2018

Tillgänglig: <https://www.acorn.gov.au/learn-about-cybercrime/online-trading-issues>

Bendovschi A. 2015. Science Direct- Cyber-Attacks- Trends, Patterns and Security Countermeasures

Tillgänglig:

<http://www.sciencedirect.com.ezproxy.arcada.fi:2048/science/article/pii/S2212567115010771>

Hämtad: 13.10.2016

Bryman A. Bell E., 2011. *Business Research Methods*. 765 s.

CNBC, eBay says client information stolen in phishing attack. 2014

Tillgänglig:

<https://www.cnn.com/2014/05/21/eBay-asks-all-users-to-change-passwords.html>

Hämtad: 21.4.2018

Collins, JM 2016, Preventing Identity Theft in Your Business : How to Protect Your Business, Customers, and Employees (1), Wiley, Hoboken, US. Available from: ProQuest ebrary. [29 November 2016].

Computer Fraud & Security, Modern IP theft and the insider threat. 6/2015.

Hämtad: 9.12.2016

Tillgänglig:

<http://www.sciencedirect.com.ezproxy.arcada.fi:2048/science/article/pii/S1361372315300567>

Cripps: Invoice Fraud- a real threat to your business (22.01.2015)

Hämtad: 05.12.2016

Tillgänglig: <http://www.cripps.co.uk/invoice-fraud-real-threat-business/>

De Bruijn H., Janssen M. 2017. Building cybersecurity awareness: The need for evidence-based framing strategies

Hämtad: 15.05.2018

Tillgänglig: https://ac.els-cdn.com/S0740624X17300540/1-s2.0-S0740624X17300540-main.pdf?_tid=bde603ea-fb51-480d-9f71-d85d08def02a3cb095db2a5bc678503f&acdnat=1526392337

Dell, Sonic Wall Anatomy of a cyber-attack, The strategies and tools of cyber-criminals and how to stop them

Hämtad: 22.11.2016

Tillgänglig: <https://www.sonicwall.com/documents/anatomy-of-a-cyber-attack-ebook-24640.pdf>

Digit, The 12 types of cyber crime

Hämtad: 16.05.2018

Tillgänglig: <https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-12-types-of-cyber-crime.html>

Hadlington, L (2017) Human factors in cybersecurity; examining the link between internet, addiction, impulsivity, attitude towards cybersecurity, and risky cybersecurity behaviours

Hämtad: 15.5.2018

Tillgänglig: https://ac.els-cdn.com/S2405844017309982/1-s2.0-S2405844017309982-main.pdf?_tid=57de0d7b-134a-443a-9f5d-5e978bc50c8f&acdnat=1526390316_b85e485a77367a3ee50643e62cec0dd6

Finansministeriet, Kohdistetut hyökkäykset 6/2009

Hämtad: 22.11.2016

Tillgänglig: https://www.vahtiohje.fi/c/document_library/get_file?uuid=c423fe00-d6d4-4bdf-99dc-1f7ac8ecf977&groupId=102

Forsber C., Wengström Y., 2013. Att göra systematiska litteraturstudier. 3dje upplagan. Författarna och bokförlaget Natur & Kultur, Stockholm.

Gualdoni J. Et al 2017, Secure online transaction algorithm: Securing online transaction using two-factor authentication

Hämtad: 21.04.2018

Tillgänglig: <https://www.sciencedirect.com.ezproxy.arcada.fi:2443/science/article/pii/S1877050917318100>

Gustafsson S. Karolinska Institutet 2015.

Hämtad: 11.3.2018

Tillgänglig: <https://kib.ki.se/whatsup/blog/jag-ska-gora-en-systematisk-litteraturoversikt>

Hadnagy, C, & Fincher, M 2015, Phishing Dark Waters : The Offensive and Defensive Sides of Malicious Emails (1), Wiley, Somerset, US. Available from: ProQuest ebrary. [24 November 2016].

Henning N. 2018. Privacy and security Online: Best practices for cybersecurity

Hämtad: 15.5.2018

Tillgänglig:

<http://content.ebscohost.com/ContentServer.asp?T=P&P=AN&K=128707555&S=R&D=afh&EbscoContent=dGJyMNLr40Sep7M4y9f3OLCmr1Cep65Ssqu4TLaWxWXS&ContentCustomer=dGJyMPGqtU%2B1qq5luePfgex44Dt6fIA>

Henricson, M., 2012 Vetenskaplig teori och metod. Från idé till examination inom omvårdnad. Lund: Studentlitteratur

Holm I., Solvang B., 1997. *Forskningsmetodik- Om kvalitativa och kvantitativa metoder*

Informationssäkerhet.se

Hämtad: 16.05.2018

Tillgänglig: https://www.informationssakerhet.se/Om-informationssakerhet-kon/vad_ar_informationssakerhet/

Informationssäkerhet- trender 2015

Hämtad: 6.12.2016

Tillgänglig: <https://www.msb.se/RibData/Filer/pdf/27494.pdf>

Jepp, A. 2017 Protect your data from cyber criminals

Hämtad: 25.4.2018

Tillgänglig: <https://www.publicfinance.co.uk/sponsored-articles/2017/03/protect-your-data-cyber-criminals>

Kaplan, JM, Bailey, T, & O'Halloran, D 2015, Beyond Cybersecurity : Protecting Your Digital Business (1), Wiley, Somerset, US. Available from: ProQuest ebrary. [21 November 2016].

Lecklider T. 2017 Defending against cyberattacks

Hämtad: 21.4.2018

Tillgänglig: <https://www.evaluationengineering.com/defending-against-cyberattacks>

Libicki, MC, Ablon, L, & Webb, T 2015, The Defender's Dilemma : Charting a Course Toward Cybersecurity, RAND, Santa Monica, US. Available from: ProQuest ebrary. [21 November 2016].

Nationalencyklopedin, uppslagsverk

Hämtad: 13.10.2016

Tillgänglig:

<http://www.ne.se.ezproxy.arcada.fi:2048/uppslagsverk/encyklopedi/1%C3%A5ng/risk-management>

National Institute of Standards and Technology, 2018

Hämtad: 30.4.2018

Tillgänglig: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

Polisen, Sverige.

Hämtad: 22.10.2016

Tillgänglig: <https://polisen.se/Utsatt-for-brott/Olika-typer-av-brott/Bedrageri/>

SC Media UK, 2014. eBay counts the cost after "challenging" data breach.

Tillgänglig: <https://www.scmagazineuk.com/ebay-counts-the-cost-after-challenging-data-breach/article/541162/>

Hämtad: 21.4.2018

Säljö R. Et al. 2010. Perspektiv på kvalitativ metod. Studentlitteratur

The Windows club

Hämtad: 22.11.2016

Tillgänglig: <http://www.thewindowsclub.com/cyber-attacks-definition-types-prevention>

Tiganoaia, B. 2015, "THE SECURITY IN THE CYBERSPACE - A RESEARCH",
Niculescu Publishing House, Bucharest, 10, pp. 239.

Tietosuoja, 2010

Hämtad: 24.11.2016

Tillgänglig:

http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutuntoimisto/brochyrrer/pmyMREm5P/Pharming_vad_ar_det.pdf

Tietotekniikan termitalkoot

Hämtad: 13.10.2016

Tillgänglig: <http://www.tsk.fi/tsk/termitalkoot/fi/haku-266.html>

Touhill, Gregory J., and C. Joseph Touhill. Cybersecurity for Executives : A Practical Guide, Wiley, 2014. ProQuest Ebook Central, <https://ebookcentral-proquest-com.ezproxy.arcada.fi:2443/lib/arcada-ebooks/detail.action?docID=1707094>.

Van der Meulen Nicole, Investing in Cybersecurity, 2015 RAND Europe

Hämtad: 6.12.2016

Tillgänglig: https://www.wodc.nl/binaries/2551-full-text_tcm28-73946.pdf

Viestintävirasto, *Näin meitä huijataan! Verkossa yleisesti tavattuja huijausmenetelmiä.*
2015

Hämtad: 24.11.2016

Tillgänglig:

https://www.viestintavirasto.fi/attachments/cert/certiedostot/Nain_meita_huijataa_n.pdf

Yadron, D 2015. The wall street journal Five simple steps to protect corporate data; what companies should be doing to protect their computer systems- but aren't

Hämtad: 25.04.2018

Tillgänglig: <https://www.wsj.com/articles/five-simple-steps-to-protect-corporate-data-1429499477>