# Social manipulering och IT-säkerhet

# Abstrakt

Det här kandidatarbetet ser på datasäkerhet och social manipulering och vilka IT-implementationer som finns för att förhindra eller försvåra kringåendet av säkerhetssystemen med hjälp av social manipulering.

Först förklaras kort vad ”social manipulering” är och vilka former det kan ta inom IT-branschen samt varför de är ett problem/problematiska. Sedan ser vi på allmänna metoder som används för indentifiering av social manipulerings försök. Till sist tas upp hurdana IT-implementationer för datasäkerheten som gjorts för att förbättra säkerhetsåtgärderna mot kringgåendet av dem.

# Innehållsförteckning

# 1.Inledning

Den digitala säkerheten utvecklas konstant. Den ställs på prov och då brister upptäcks täpps de till. Den tekniska delen av system kan uppdateras både med programvaruutveckling och med specialiserad hårdvara. För att bryta sig in i ett system krävs det tid och expertis. Oftast är de svagaste länkarna i systemen människan.

Därför har dessa säkerhetsåtgärder börjat försöka kringgås genom att utnyttja och manipulera människans natur och personlighetsdrag. Den här processen kallas social manipulering.

I dagens digitala och internationella värld skall saker och ting ske snabbt. Det leder till att mindre tid lämnar kvar för att kunna kontrollera och pricka igenom varenda punkt och detalj i säkerhetsprotokoll då det kommer till kundservice eller byggnadssäkerhet. Det här kan bilda öppningar i säkerhetssystem som kan utnyttjas och på så sätt kan den digitala säkerheten kringgås totalt.

# 2. Social manipulering

## 2.1 Vad är social manipulering?

Social manipulering är ett begrepp som används om att kringgå säkerhetsåtgärder med hjälp av bedrägeri och manipulering av personers förtroende. Genom att manipulera personer kan man komma åt de eftersträvade resurserna, såsom känslig information eller begränsade områden. [1][7]

Det här åstadkoms med utnyttjande av mänskliga aspekter och beteende. Exempelvis är offret en användare i ett system. För att komma åt information om användaren i systemet kan sociala manipulatorn låtsas vara användaren i ett samtal med systemets hjälpcentral och på så sätt komma åt offrets användarrättigheter genom missbruk av förtroende och bedrägeri. Metoden kan beskrivas som efterliknande eller maskerande.

Alternativt kan en betningsmetod användas. Det går ut på att ett USB-minne med skadlig mjukvara användas. USB-minnet lämnas oskyldigt på en plats där offret vistas i hopp om att offret är nyfiken på innehållet och därmed tar med sig USB-minnet och koplar den i sin dator.

Ett e-post meddelande kan också användas. Meddelandet kan innehålla något som väcker offrets intresse och ber dem att följa en länk till en webbsida. Där bes offret ladda ner mjukvara eller bes att mata in sina bank- och socialskyddsinformation för att få det som meddelats om. Efter det har sociala manipulatorn fått tillgång till offrets dator eller bank. Det här är en kombination av en Phishing och socio-teknisk attack.

### 2.1.1 Varför social manipulering?

Dagens säkerhets åtgärder är väldigt robusta och det krävs oftast mycket tid och energi för att kunna bryta sig igenom dem. Genom social manipulering kan man totalt kringgå dessa försvar och snabbare komma åt det eftersträvade målet, vare sig det är åtkomsten till något fysiskt rum i någon byggnad eller användarrättigheterna till en specifik persons användarkonto.

Exempelvis kan det vara så pass enkelt som att enbart behöva maskera sig som en gårdskarl för att få fritt inträde till någon byggnad eller ringa ett telefonsamtal med användarstödet i något företag och låtsas vara offret vars konto man vill komma åt.

### 2.2 Social manipulering och IT-säkerhet

Experter inom it-säkerhet har skapat pålitiliga metoder för att kunna identifiera risker, upptäcka sårbarheter och få tag i information gällande sårbarheter i sina system, för att kunna fortsätta utvecklingen av riktade motåtgärder baserade i riskbedömning. [3]

Med hjälp av dessa åtgärder kan systemens säkerhetsåtgärder förbättras effektivare. Trots det är de fortfarande sårbara på grund av den mänskliga faktorn.

De som vill komma åt informationen, föremålet eller utrymmet behöver nödvändigtvis inte kunna så mycket eller något alls om it-säkerhet. De behöver enbart lära sig förstå och kunna utnyttja kunskapen om hur mäniskor fungerar och reagerar i olika situationer.
I dagens värld har den sociala manipulatorns anfall, tack vare internet och annonymiteten det ger, en väldigt låg chans att bli upptäckta av offret och råka ut för följdföreteelser.

### 2.3 Kategorier, faser och former av social manipulering

Som vi tidigare nämnt kan social manipulering ta flera former. Den kan även delas upp i två kategorier och vissa angreppsmetoder kräver förberedande faser. Till näst tar vi upp vad de är och förklara kort hur en del av dem fungerar. I kapitel 3 beskrivs olika bekämpningsmetoder. [1]

Ett angrepp kan klassas antingen som jakt eller som kultivering av förtroende. Jakt metoder är de som vanligen används och de går ut på att angriparen med minimal växelverkan med offret åstadkommer det som angriparen är efter. Nästan som regel är offret endast en gång i kontakt med angriparen. Kultivering av förtroende går ut på att angriparen bygger en relation med

offret och på såvis utvinner önskad information eller resurser under en längre tidsperiod. [1]

För att lyckas med sina angrepp behöver angriparen vara förberedd. Det åstadkommas genom att samla ihop all relevant information under en tid av spanande och studerande av offret. När det har blivit gjort kan angreppet börja. Kommunikation med offret etableras. Offret manipuleras att ge ut information eller att omedvetet äventyra systemet. När angriparen nått sitt mål slutförs växelverkan med offret, helst utan väckta misstankar, varefter angriparen försvunnit och sopat upp sina spår. [1]

Angreppsmetoder som social manipulatorn kan använda sig av är mångfaldiga och de bestämmer hur angriparen skall gå till väga för att nå sitt mål. Metoderna kan delas upp mellan två grupper. Socialt närmande och socio-tekniskt närmande. Till näst förklaras skillnaden mellan grupperna och några av angreppsmetoderna som används. [1]

### 2.3.1 Socialt närmande

De metoder som klassas som socialt närmande har alla gemensamt att angriparen har nära kontakt med offret och att offret är omedveten om den påkommande skadliga avsikten. [1]

”Tailgating” är en metod som ofta ses användas i filmer och serier. Det går ut på att angriparen följer offret igenom en låst dörr antingen genom att be offret hålla dörren åt angriparen eller genom att angriparen stoppar dörren från att stängas efter att offret passerat in. [1]

Efterliknande och imitering är också bekant från filmer och serier där angriparen med hjälp av en falsk identitet försöker skapa trovärdighet för at kunna komma åt sitt mål. Det kan ske t.ex. med en förklädnad av en städare, med efterliknande av företagets förman eller chef, eller med skapandet av ett falskt hot för att sedan efterlikna någon som har en lösning till hotet. [1]

Att tjuvlyssna på offret, se över offrets axel och att söka igenom offrets skräp är alla metoder som används för att komma åt information som kan användas för angriparens ändamål. [1]

Omvänd social manipulering är en metod där angriparen, med en falsk identitet, lockar offret att självmant kontaktar angriparen för att lösa ett problem som angriparen har skapat. I det här skedet tror offret att angriparen är en pålitlig person som kan hjälpa dem och är omedveten om att problemet är skapat av angriparen. [1]

Under det gångna året i samband med Covid-19 har vi hört om och stött på telefon samtal där personen på andra ändan påstår sig jobba som Microsoft tech support. Deras ärende gäller oftast att de har upptäckt att offrets dator blivit utsatt för ett virus eller blivit hackad. De ber sedan offret att installera mjukvara på sin dator som sedan tillåter tech supporten att hantera datorn på distans. Offret mister totalt kontrollen över sin dator ifall de installerar mjukvaran och sedan tillåter tech supporten att skapa förbindelsen mellan datorerna.

### 2.3.2 Sociotekniskt närmande

Sociotekniskt närmande skiljer sig från socialt närmande med att det inte använder sig av personlig eller nära kontakt av offret. Istället används olika sorter av IT-metoder för att kontakta, locka och lura offret. [1]

Troligen det verktyg vi är mest bekanta med som social manipulatorn kan använda är ’Phishing’. Phishing går ut på att angriparen skickar e-post åt sina offer. Först kan angriparen skapa en falsk e-postadress som är väldigt lik det som angriparen försöker locka offret med t.ex. ett meddelande från offrets bank. Sedan efterliknas det riktiga meddelande från banken så gott som möjligt. Därefter fylls meddelandet med information som skall få offret att ge ut sin information eller pengar till angriparen. Det kan t.ex. vara ett meddelande där angriparen ber offret att byta lösenordet för sitt konto på en websida som angriparen skapat som ser liknande ut som den riktiga sidan.

Det mest kända exemplet på Phishing är ”nigeriabreven”.

Det fina med phishing är att den sociala manipulatorn kan skicka ut dessa e-post åt flera tusental offer samtidigt.

### 2.3.2 Qrishing

Qrishing är ett relativt nytt fenomen som dykt upp. Det använder sig av QR-koder som kan skannas av maskiner med möjlighet för det och när de skannas förs offret vidare till en webbsida som ser ut att vara legitim. Dessa QR-koder kan hittas till exempel: i webbsidor som kan se ut att vara legitima, i kommentarer i olika sociala medier från personer eller grupper som låtsas vara någon person eller grupp, eller i e-postmeddelande i kombination med phishing. [5]

### 2.3.3 Clickbait

Clickbait är som namnet säger ett bet för att fånga klickar. Man hittar clickbait överallt på internet. Clickbait används för att förvirra offret att till att klicka på fel ikon och ha offret ladda ner ett program som offret inte hade tänkt ladda ner. Dessa program kan variera från trojanska maskar, för att få kontroll över offrets dator, till program som övervakar offrets alla handlingar och sedan sänder det vidare programmets tillverkare.

# 3. Åtgärder mot social manipulering

Det finns huvudsaklingen två sätt att försvara sig från social manipulering. Metoder som riktar sig på människan och metoder som riktar sig på system. I det här stycket går vi igenom vad som är skillnaden mellan dem och olika metoder som hör till dem.

## 3.1 Metoder med människan som fokus

Dessa är åtgärder som inte använder sig av en IT-relaterad lösning för att förhindra anfall genom social manipulering från att lyckas. De fungerar istället som modeller med instruktioner som skall följas vid olika serier av händelser.

### 3.1.1 Social Engineering Attack Detection Model (SEADM)

SEADM är en model som varit framgångsrik i stoppandet av social manipulering. SEADM är avsedd för att göra det lättare för organisationsspecifika förlängningar att gruppera liknande aktiviteter i olika kategorier, indelade i flera stater. SEADM tillämpas sedan på representativa social manipulerande scenarier med hjälp av använding av dubbelriktad, enriktad och indirekt kommunikation. Det här bör verifiera att alla aspekter har beaktats i modellen och bör också givit förbättringsförslag. [6]

## 3.2 Metoder med IT-lösningar som fokus

Dessa är åtgärder som har som mål att minska eller stoppa människan från att komma i kontakt med social manipulerings försök eller hindra ett lyckat fall av social manipulering från att åstadkomma sitt mål.

### 3.2.1 PhishLimiter

PhishLimiter är ett relativt nytt system som skapats för att lättar kunna upptäcka och mildra effekterna av phishing försök. PhishLimiter fungerar genom att den klassifierar phishing mönster i ett nätverk, med hjälp av sin

tillgång SDN, vart efter den sedan lätt och effektivt kan bestämma ifall något e-post är ett phishing försök eller inte. I en demonstration hade PhishLimiter en noggrannhet på över 98% i upptäckandet och hindrandet av phishing försök. [4]

### 3.2.2 Två vägs faktorisering

# 4. Diskussion

# 5. Sammanfattning

# References


[1] M. Jakobsson, "Social Engineering Resistant 2FA," in *Security, Privacy and User Interaction*, M. Jakobsson, Ed., Cham, Springer International Publishing, 2020, p. 113–121.

[2] T. Chin, K. Xiong and C. Hu, "Phishlimiter: A phishing detection and mitigation approach using software-defined networking," *IEEE Access,* vol. 6, p. 42516–42531, 2018.

[3] F. Mouton, A. Nottingham, L. Leenen and H. S. Venter, "Finite state machine for the social engineering attack detection model: SEADM," *SAIEE Africa Research Journal,* vol. 109, p. 133–148, 2018.

[4] F. Breda, H. Barbosa and T. Morais, "Social engineering and cyber security," in *Proceedings of the International Conference on Technology, Education and Development, Valencia, Spain*, 2017.

[5] R. Heartfield, G. Loukas and D. Gan, "You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks," *IEEE Access,* vol. 4, p. 6910–6928, 2016.

[6] F. Mouton, L. Leenen, M. M. Malan and H. S. Venter, "Towards an ontological model defining the social engineering domain," in *IFIP International Conference on Human Choice and Computers*, 2014.

[7] M. I. Mann, Hacking the human: social engineering techniques and security countermeasures, Gower Publishing, Ltd., 2012.

[8] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo and M. Yung, "Fourth-Factor Authentication: Somebody You Know," in *Proceedings of the 13th ACM Conference on Computer and Communications Security*, New York, NY, USA, 2006.

[9] E. Follett, "Discussing the impact that Social Media has on enterprise Cyber security.".

[10] D. Alharthi and A. Regan, "ALiterature SURVEY AND ANALYSIS ON SOCIAL ENGINEERING DEFENSE MECHANISMS AND INFOSEC POLICIES".