Оригинални научни рад 343.533:004.056.5

Др Љубомир Стајић, редовни професор
Правног факултета у Новом Саду

Мр Горан Ј. Мандић, асистент
Факултет безбедности у Београду

СОЦИЈАЛНИ ИНЖЕЊЕРИНГ КАО ОБЛИК УГРОЖАВАЊА ПОВЕРЉИВИХ ПОСЛОВНИХ ИНФОРМАЦИЈА

Сажетак: *У многим пословима, поготово тамо где треба доћи до поверљивих информација у контакту са другим људима, присутне су поједине форме социјалног инжењеринга. Социјални инжењеринг је облик говорне и гестикуларне манипулације појединцима са циљем да се наведу на испуњење неких захтева постављених од стране нападача.*

Проблеми који се јављају у области заштите поверљивих информација налазе се у чињеници да иза сваког компјутера, стоји човек као јединка са свим својим добрим и лошим особинама. Социјални инжењеринг је техника у којој се убеђивање и/или обмана користе да би се добио неовлашћен приступ компјутерским системима. Ово се обично постиже разговором или неким другим облицима интерактивне комуникације.

Противмере у борби против социјалног инжењеринга су врло сложене. Усложава их чињеница да свако ко има приступ било ком делу информационог система представља могућу мету напада социјалним инжењерингом.

За разлику од осталих напада на компјутере, социјални инжењеринг се не односи на технолошку манипулацију и коришћење рањивости хардвера или софтвера. Поред тога и не захтева посебне техничке вештине и знања. Ова врста напада експлоатише људске слабости, као што су немарност или жеља за кооперативношћу, како би се добио приступ поверљивим документима који се налазе на компјутеру.

Циљ социјалног инжењеринга може бити стицање профита, сајбер тероризам или приступ интерним системима и поверљивим информацијама. Мете напада су, најчешће, провајдери телекомуникационих услуга, мултинационалне компаније, финансијски установе, болнице, владине агенције, војска и други.

***Кључне речи**: социјални инжењеринг, безбедност информација, безбедносни системи, компаније, хакери, компјутерски криминал*

1. Појам социјалног инжењеринга

Историјски посматрано вештина уверавања супротне стране да поступи по нечијем захтеву није концепт који је својствен само савременом добу. Прве корене вештине уверавања срећемо у форми реторике на тлу Грчке Сицилије, негде око 485. године пре наше ере, где је на настанак ове вештине пресудну улогу имала судска пракса. Реторика је од самог почетка сматрана техником уверавања.[1] Циљ уверавања био је убедити судије и поротнике у кривицу коју је доказивао оштећени реториком са позиције тужиоца, односно у невиност коју је говором бранио оптужени. Само од вештине говора зависила је процена веродостојности њихових тврдњи и исказа. Писани трагови из тог времена потврђују значај смишљеног уверавања са унапред дефинисаним циљем, иако је јасно да је уверавање одувек било присутно у комуникацији између људи.

Од тренутка кад се говор претворио у технику уверавања, постоје два начина његовог коришћења. Први, за који можемо рећи да је опстао до данас, у коме се истиче свемоћ језика као средства за уверавање, а с друге стране (према Аристотелу) саветује се да употреба тог средства мора бити у сагласју са посебном етиком, макар то довело до одустајања од непрестане, често безуспешне потраге за делотворношћу.[2] За њега, убеђивање је вештина. То је „вештина навођења људи да учине нешто што они обично не би учинили ако ви то не затражите“.[3]

Манипулација и уверавање, као претпоставка успешног социјалног инжењеринга, у свом основном појавном облику, користи говор са циљем уверавања супротне стране у неке чињенице, на начин где се заобилази истина, уз употребу свих расположивих средстава уверавања у изречено.

У многим пословима, поготово тамо где треба доћи до поверљивих информација у контакту са другом страном, или пак стићи до неког циља, присутне су модификоване форме социјалног инжењеринга. Можемо рећи да полицајци у свом оперативном раду скоро свакодневно користе социјални инжењеринг са циљем да открију и ухвате извршиоце кривичних дела. Без обзира да ли је циљ позитиван и исправан, или не, приступ је исти, манипулише се другом особом да би се постигао неки крајњи циљ. Могли бисмо рећи да је то један од најстаријих начина стизања до неког циља пу-

[1] Breton, F.: *Izmanipulisana reč*, Clio, Beograd, 2000, str. 56.
[2] Breton, F: *Izmanipulisana reč*, Clio, Beograd, 2000, str. 60.
[3] Borg, DŽ.: *Ubeđivanje: umetnost ubeđivanja ljudi*, IPS Media, Beograd, 2008, str. 4.

тем интерактивног односа две или више особа, иако се његова форма мењала временом.

Из претходно наведеног можемо закључити да скоро свако људско биће поседује потенцијале за покушај напада социјалним инжењерингом. Једина разлика је у потреби, мотивацији и нивоу вештине потенцијала који се користе.

Интересантно је напоменути да је још 1997. године, за ову врсту говорне манипулације употребљен појам социјални инжењеринг где се каже да је он у основи „уметност и наука навођења људи да вам испуне жеље. То није начин контроле ума и неће омогућити да наведете људе да обављају задатке много ван њиховог нормалног понашања и далеко од сигурног".[4] Најкраће речено, социјални инжењеринг је облик говорне и гестикуларне манипулације појединцима са циљем да се наведу даураде нешто што иначе не би урадили, а односи се на испуњење неких захтева постављених од стране нападача.

Проблеми који се јављају у области безбедности компанија или владиних установа и агенција и заштити поверљивих информација налазе се у чињеници да иза сваког компјутера, био он самосталан део мреже или сервер стоји човек као јединка са свим својим добрим и лошим особинама. Није важно које генерације су компјутери, који је оперативни систем инсталиран и који хардвер и софтвер се користи за заштиту поверљивих информација на њему, јер се у свом раду сви ови системи ослањају на човека. Јасно је у овом случају да та јединка представља најслабију карику безбедносног ланца којим се штите информације.

Социјални инжењеринг је техника у којој се убеђивање и/или обмана користе и да би се добио приступ компјутерским системима.[5] Ово се обично постиже разговором са људима или неким другим облицима интерактивне комуникације.

Најслабија карика у систему обезбеђења увек ће бити људи, а најлакши начин да се продре у систем обезбеђења је планирање упада користећи се људима.[6] Постоји размишљање да је најсигурнији и једини безбедан компјутер онај који је искључен из извора напајања. Ова тврдња је на први поглед тачна, али само постојање могућности да неког убедите да га укљу-

---

[4] *People Hacking: The Psychology of Social Engineering*, Text of Harl's Talk at Access All Areas III, 05/07/97, http://packetstormsecurity.nl/docs/social-engineering/aaatalk.html, pristupljeno 28.03.2010.

[5] Gattiker, U. E.: *The information security dictionary*, Kluwer Academic Publishers, Boston, 2004, str. 306.

[6] Rittinghouse, J.; Hancock W. M.: *Cybersecurity Operations Handbook*, Elsevier Digital Press, Oxford, str. 298.

чи у извор напајања и потом активира оперативни систем, довољно говори да је претходна тврдња илузија.

Социјални инжењеринг се дефинише и као „добијање поверљивих информација средствима људске интерактивне комуникације." (Business Wire, August 4, 1998.).[7]

Тако на пример претварајући се да је особа на високом положају нападач може својим захтевом и ауторитетом да заплаши мету напада (новозапослену радницу) негативним последицама ако не испуни његов захтев. Важан фактор који помаже овом приступу је веровање да се ауторитети обично не смеју проверавати. Људи ће испунити неке веома необичне захтеве за особе за које верују да су на значајној позицији.[8]

Колеге из друге организационе целине или другог града, као и новозапослени се, такође не одбијају, поготово ако им је потребна нека врста хитне помоћи да не би трпели последице због необављеног посла. Ову колегијалност веома вешто користи нападач да би дошао до информација. Кевин Митник познат као „Кондор," је био први хакер који је доспео на листу најтраженијих особа Федералног истражног бироа. На овај начин упао је у многе организације међу којима су Digital Equipment Corp, Motorola, Nokia Mobile Phones, Fujitsu, и многе друге.[9]

Оно што је чињеница и што усложава противмере у борби против социјалног инжењеринга је сазнање да свако ко има приступ било ком делу информационог система, (физички, или електронски посредством компјутерске мреже) представља потенцијални ризик по безбедност информација. Било која информација до које се може доћи представља корак ка следећој информацији и тако док се не стигне до оне информације која је циљ напада. То указује на чињеницу да и запослени који се не сматрају безбедносно угрожени и нису укључени у мере безбедносне заштите, могу бити мета напада социјалним инжењерингом.

За разлику од осталих напада на компјутере, социјални инжењеринг се не односи на технолошку манипулацију и коришћење рањивости хардвера или софтвера и поред тога не захтева посебне техничке вештине и знања. Ова врста напада експлоатише људске слабости, као што су немарност или жеља за кооперативношћу, како би се добио приступ легитимним документима који се налазе на компјутеру.[10] Најтеже је бранити се од напада социјалним инжењерингом, јер га не могу зауставити самостално ни

---

[7] Shinder, D. L.: *Scene of the Cybercrime: Computer Forensics Handbook*, Syngress Publishing, Inc., Rockland, 2002, str. 313.

[8] Gregg, M.: *Certifie Ethical Hacker Exam Prep*, Que Publishing, 2006, E-book.

[9] Gregg, M.: *Certifie Ethical Hacker Exam Prep*, Que Publishing, 2006, E-book.

[10] Shinder, D. L.: *Scene of the Cybercrime: Computer Forensics Handbook*, Syngress Publishing, Inc. 800 Hingham Street Rockland MA 02370, USA, 2002, str. 313.

хардвер ни софтвер.[11] Примера ради лице које користи социјални инжењеринг за напад може убедити оператера корисничког сервиса да му открије неопходне детаље како би се повезао на информациони систем. Касније, нападач поново назове другог оператера жалећи се да његова шифра из неког разлога не ради и убеђује кориснички сервис да му промене шифру. На тај начин та особа добија неовлашћени приступ компјутерском информационом систему.[12]

2. Профил лица које извршава социјални инжењеринг

Раније смо видели да је основни циљ социјалног инжењеринга неовлашћен приступ компјутерским системима или поверљивим информацијама и по томе он је сличан циљу хакера. Након што је добило приступ информацији, лице које користи социјални инжењеринг може да је користи или за друге нападе, или да би пореметио систем и изазвао штету. Социјални инжењеринг може бити организован због профита, сајбер тероризма или за приступ интерним системима и поверљивим информацијама. Такође може бити примењен и ради едукације и обуке запослених корисника за контра мере. Најчешће се нападају велике организације које скупљају и складиште осетљиве податке, као што су провајдери телефонских услуга, мултинационалне компаније, финансијски ентитети, болнице и војска.[13] Наравно поред наведених напад може бити усмерен и према било ком предузећу или владиној установи или агенцији.

Одређивање прецизно дефинисаног профила лица која спроводе социјални инжењеринг је врло тешко. Може се само рећи да су то углавном лица мушког пола, мада се у пракси срећу и жене које су биле веома успешне.

Тако на пример прва позната жена хакер, која је радила под псеудонимом Сузан Тандер, била је специјализована за упаде у војне компјутере и компјутере телефонских компанија. Била је повезана са познатим хакерима, браћом Роном и Кевином Митником. Посматрајући њену прошлост, прошла је кроз разне фазе развоја и постала врстан телефонски и компјутерски хакер.[14]

---

[11] Thomas Mathew: *Ethical Hacking and Countermeasures [EC-Council Exam 312-50]—Student Courseware*, OSB Publisher, International Council of Electronic Commerce Consultants, New York, 2004. elektronska forma.

[12] Gattiker, U. E.: *The information security dictionary*, Kluwer Academic Publishers, Boston, 2004, str.306.

[13] Janczewski, J. L.; Colarik, M. A.: *Cyber Warfare and Cyber Terrorism,* Information Science Reference, Hershey - New York, 2008, str. 184.

[14] Shinder, D. L.: *Scene of the Cybercrime: Computer Forensics Handbook*, Syngress Publishing, Inc., Rockland, 2002, str. 107.

Старосну структуру као елемент профила починиоца, такође је тешко одредити. Креће се од тинејџерског узраста до зрелог доба. Може се рећи, да су нападачи најактивнији у периоду од двадесете до тридесете године живота. Лица која га спроводе у позитивној конотацији (да би проверили безбедност правног ентитета) припадају нешто старијој животној доби.

Ова лица су иначе веома интелигентне и изузетно креативне особе. Поседују добре комуникацијске и манипулаторске вештине, добри су познаваоци психологије и углавном имају довољно техничког знања. Могу да наступају тимски и самостално, с тим што је тимски напад много опаснији јер удружују своја знања и умећа поштујући се међусобно и уважавајући хијерархију.

Често тимски напад резултира дозволом за улазак у компанију и на крају стицање жељених информација.[15]

Поставља се питање које све категорије људи и у којим све приликама, могу да користе социјални инжењеринг. Подела може бити направљена у односу на мотив који их покреће и циљ који се жели постићи.

Те групе су:

1. хакери,
2. крадљивци идентитета,
3. лица која се баве индустријском шпијунажом,
4. лица која прибављају информације о раду конкуренције,
5. незадовољни запослени,
6. разне врсте криминалаца,
7. терористи,
8. приватни детективи,
9. лица која проверавају функционисање система обезбеђења,[16]
10. лица која раде у обавештајним агенцијама државе и полицији,
11. грађани у својим свакодневним активностима.

Код свих поменутих група људи које користе социјални инжењеринг, заједничко је само то да га користе, док су мотиви углавном различити. Са аспекта безбедности треба се фокусирати на оне категорије људи који га користе у деструктивне сврхе са циљем да дођу до одређене користи, без обзира да ли је она материјална, или се огледа у остварењу одређених идеја и жеља.

---

[15] Rittinghouse, J.; Hancock W. M.: *Cybersecurity Operations Handbook,* Elsevier Digital Press, Oxford, 2003, str. 299.

[16] Лице које проверава функционисање система обезбеђења коришћењем социјалног инжењеринга проверава интегритет запослених у компанији, као и функционисање контроле приступа покушајем уласка у рестриктивни - штићени простор. Интегритет запослених се проверава покушајима неовлашћеног доласка до информација које поседују.

У даљем тексту приказаћемо предуслове које треба да испуни особа која користи социјални инжењеринг. За те предуслове можемо рећи да представљају криминогене факторе у ужем смислу и односе се на мотив, спремност и могућност извршења социјалног инжењеринга.

Наиме, да би се неке конкретне илегалне активности могле реализовати, неопходно је да се у одређеном временском тренутку код потенцијалног извршиоца истовремено стекну три предуслова:

- Мотив због ког би потенцијални извршилац предузео криминалну радњу,
- Спремност извршиоца да због тога прихвати одређени ризик и
- Могућност да се криминална радња изврши.[17]

Поред овако дефинисаних криминогених фактора у ужем смислу, у литератури проналазимо навођење и других предуслова како би нападач остварио свој циљ.

Ти предуслови су:

- метод (мора имати вештине, средства и остале неопходне ресурсе за извршење напада),
- могућност (извршилац мора имати време и приступ како би обавио и успео у нападу) и
- мотив (мора постојати разлог због кога ће извршилац извести напад.).[18]

Анализом наведених предуслова долазимо до закључка да је и једна и друга класификација предуслова непотпуна када говоримо о нападима на компјутере. Наиме, у првој не постоји метод као важан предуслов испуњења напада, док се у другој не помиње спремност, без које нема испуњења криминалне активности. Из тог разлога прихватљивије је рећи да су предуслови представљени кроз четири категорије или фактора и то:

- мотив,
- спремност,
- могућност и
- метод.

Мотив је психолошки фактор који се дефинише као процес који изазива, усмерава и одржава одређене активности које лице доводе до пројектованог циља.

Мотиви могу бити различити. Неки изводе нападе како би украли новац, или специфичне податке. Други то чине као изазов или из заба-

---

[17] Petrović, R. S.: *Kompjuterski kriminal,* Ministarstvo unutrašnjih poslova Republike Srbije, Beograd, 2000, str. 108.

[18] Pfleeger P. C.: *Security in Computing*, Fourth Edition, Prentice Hall, Pearson Education, Inc., Upper Saddle River, 2006, електронско издање.

ве. Остали, пак, из освете.[19] При томе, сваки криминалац има своје сопствене мотиве који се могу мењати, могу трајати годинама, а могу да се јаве и изненада.[20]

Примарни пројектовани мотиви код социјалног инжењеринга су у основи исти, долажење до употребљивих и квалитетних информација, док секундарни мотиви могу бити различити у зависности од профила нападача и наводе се као изазов, новац, такмичење са другима и самодоказивање и слично.

Спремност представља свесно прихватање одређеног ризика по нападача, који неминовно постоји као последица његовог деловања. Спремност може бити иницирана различитим карактерним особинама починиоца и условљена мотивом.

Могућност означава квантитет и квалитет лакоће и извесности којом особа може да почини штетно, забрањено, противзаконито и/или кривично дело, а да не буде откривена.

Као и све друге појаве, преступ је стицај прилика и околности у датом времену и простору.[21] Стицај прилика и околности означава и могућност да се преступ изврши.

Метод представља начин напада који је условљен и детерминисан вештинама, степеном комуникације, посебним знањима, потребном опремом (хардвером и софтвером) и неопходним пратећим ресурсима, који једино збирно омогућавају успешно остварење циља нападача.

Уколико један од четири поменута фактора не постоји, напад се неће десити. Чињеница је да се на мотив и спремност не може утицати јер су објективно ван контроле лица које штити систем. У функцији проактивног деловања на могућност се може утицати њеном елиминацијом или умањењем и на тај начин се може спречити и одвратити лице од чињења напада усмереног на неовлашћено прикупљање и добијање информација. Четврти предуслов, метод, у данашњим условима представља релативно лако савладиву препреку, поготово ако говоримо о социјалном инжењерингу. Проблем је у томе што су информације и знање о системима и методама напада лако доступни на Интернету.

Тако на пример, утврђено је да су десетине хиљада интернет страница садржавале софтверске алате и упутства корисна за сајбер напад и да су

---

[19] Pfleeger P. C.: *Security in Computing*, Fourth Edition, Prentice Hall, Pearson Education, Inc., Upper Saddle River, 2006, електронско издање.

[20] Petrović, R. S.: *Kompjuterski kriminal,* Ministarstvo unutrašnjih poslova Republike Srbije, 2000, str. 110.

[21] Крстић, О.: *Примењена криминалистика*, Завод за уџбенике и наставна средства, Београд, 1997, стр. 5.

милион корисника компјутера поседовали вештине да их искористе тако да проузрокују значајно оштећење на интернет компонентама и механизмима.[22]

Ако неко има мотив и спремност, без већих потешкоћа ће наћи потребна знања, алате у виду софтвера и начине како напасти одређене системе. Ако овоме додамо и релативно лак приступ компјутерским мрежама преко Интернета и незнање о социјалном инжењерингу, јасно је да се нападачима често указује прилика, односно да објективно постоји могућност за извршење напада.

Комбинација мотива, спремности и метода, с једне стране, и, с друге стране, евидентне и сталне или тренутне слабости у функционисању и организацији безбедности и заштите информација, намеће евентуалним извршиоцима питање и дилему колика је вероватноћа да ће успети, уколико почине (изврше) напад, и какве су могућности да почињено дело остане неоткривено?

Веома је важно знати да ће потенцијални извршилац инкриминисане радње ово питање поставити себи увек пре него што почини забрањено дело. Уколико су адекватним процедурама заштите елиминисане могућности и постоји велики број препрека до циља и ако је изузетно велики степен вероватноће откривања дела, односно извесно је да ће извршилац бити ухваћен, мали број потенцијалних нападача ће покушати да изведе инкриминисано дело.

3. Социјални инжењериг као облик претње штићеним информацијама

Смањити рањивости система који се штити није увек лако. Први корак у том процесу подразумева идентификовање врсте претњи које могу да се остваре. Идентификација противника, утврђивање његових особина и карактеристика и врста претњи је реална претпоставка успешном супротстављању кроз развијање система обезбеђења и заштите. Задатак менаџмента задуженог за обезбеђење и безбедност компанија је да схвате ко је, или шта је њихов евентуални противник. Често им то и не успева. Разлог је то што су недовољно едуковани, поготово кад је у питању социјални инжењеринг, те не могу исправно да идентификују или окарактеришу ову врсту претње.

Када нису у могућности да идентификују претње и противнике, лица задужена за обезбеђење имовине и пословања и безбедност генерално се уместо поменутог усредсређују на смањење рањивости, што је погре-

[22] Parker, T.; Shaw, E.; Stroz, E.; Devost, G. M.; Sachs, H. M.: *Cyber Adversary Characterization: Auditing the Hacker Mind,* Syngress Publishing, Inc., Rockland, 2004, str. 221.

шна логика из разлога што је рањивост у узрочно-последичној вези са претњом.

Са умањењем или уклањањем претњи и сходно томе са смањеном рањивости, претње се не могу испољити саме од себе. Након свега, ако један систем није рањив на напад, онда не може бити штете од напада. Организације са одбрамбеним положајима које се оријентишу на претњу, пре него на рањивост или изложеност, оријентисане су често на несхватање овог једноставног правила.[23]

Из тог разлога неопходно је утврдити ко представља претњу по безбедност информација и сходно томе развити систем адекватне заштите који узима у обзир претње и рањивости на које су оне усмерене.

Критичне информатичке инфраструктуре су рањиве на нападе на много начина из многих углова, укључујући и нападе физичким приступом и нападе изведене преко компјутерске мреже. Међузависности између елемената инфраструктуре чине ризичним све елементе, тако да ће успешан напад на један део система сигурно утицати на друге делове система који нису директно нападнути, али су међусобно повезани.[24]

Компјутерски криминалитет представља облик криминалног понашања, код кога се коришћење компјутерске технологије и информационих система испољава као начин извршења кривичног дела, или се компјутер употребљава као средство, или циљ извршења, чиме се остварује нека, у кривично-правном смислу, последица.[25]

Компјутерски криминалитет можемо класификовати кроз следеће типове који донекле осликавају мотиве као и мете напада и то на:

- војне и обавештајне нападе,
- пословне нападе,
- финансијске нападе,
- терористичке нападе,
- осветнички напади и
- напади забаве ради.[26]

У свим овим нападима, поред осталих техника, присутан је и социјални инжењеринг.

---

[23] Parker, T.; Shaw, E.; Stroz, E.; Devost, G. M.; Sachs, H. M.: *Cyber Adversary Characterization: Auditing the Hacker Mind,* Syngress Publishing, Inc., Rockland, 2004, str. 229.

[24] Parker, T.; Shaw, E.; Stroz, E.; Devost, G. M.; Sachs, H. M.: *Cyber Adversary Characterization: Auditing the Hacker Mind,* Syngress Publishing, Inc., Rockland, 2004, str. 229.

[25] Kukrika, M.: *Upravljanje sigurnošću informacijama*, Infohome, Beograd, 2002, str.66.

[26] Stewart, M. J.; Tittel, E.; Chapple, M.: *CISSP - Certified Information Systems Security Professional Study Guide,* 3rd Edition, SYBEX Inc, 1151 Marina Village Parkway, Alameda, CA 94501, 2005, str. 606.

3.1. Војни и обавештајни напади

Мотив војних и обавештајних напада се огледа првенствено у жељи да се дође до информација који представљају тајну од значаја за функционисање војске, полиције, државних институција или одређених процеса који се спроводе под окриљем државе. Обелодањивање и откривање овог типа информација може да компромитује одређене истраге које спроводи полиција, пореметити функционисање војске и да представља претњу националној безбедности државе.

Због своје осетљивости, значаја и природе ових информација, оне су често атрактивна мета напада поготово за искусне нападаче. Овакве нападе спроводе лица која су изузетно мотивисана, спремна и лица способна да истраже и пронађу могућност за напад и која имају веома развијене методе за ове врсте напада. По завршетку ове врсте напада иза нападача остаје веома мало или нимало доказа који говоре да се напад уопште и десио и можемо рећи да су напади у овој категорији веома успешни када се изведу до краја.

3.2. Пословни напади

Пословни напади су усмерени на откривање и експлоатацију поверљивих информација производних, услужних или научноистраживачких организација. Те информације су од кључне важности за функционисање организације. То су на пример: стратегијски планови развоја и усвајања новог производа, анализа конкуренције, информације маркетиншке и финансијске природе које нису намењене јавности, услови послова који се договарају и подаци о клијентима и запосленима. Мотив је остваривање материјалне добити или наношење штете и уништавање репутације мете напада.

Прикупљање поверљивих информација, представља индустријску шпијунажу и као појава није нова. Пре појављивања Интернета, ово прикупљање информација захтевало је дуготрајну обуку појединаца и значајна материјална средства. Данас је то промењено коришћењем софистицираних облика прикупљања информација као и количином информација доступних на Интернету. Ова техника делује само против мете напада која активно складишти и чува своје информације на компјутерима. Прикупљање пословних података и информација само по себи неће имати физички деструктивни или разорни ефекат на критичке инфраструктуре власника информација.

Компаније широм света шпијунирају једни друге из различитих разлога. Већина шпијунских операција се усредсређује на прикупљање обавештења о активностима конкуренције да би се погодио његов следећи потез или за рано откривање нових технологија. Други разлози укључују праће-

ње пословних потеза конкуренције везених за уговоре са конкуренцијом на тржишту.

Институционализацијом заштите информација које објективно представљају тајну, кроз њихову класификацију и доношење одређених интерних аката организације, само се донекле решава овај проблем. Ако се и заштите информације које су степеноване као тајна и спроведу адекватне мере заштите долазимо до новог питања: „Да ли су само подаци проглашени пословном тајном предмет индустријске шпијунаже?“ Одговор на постављено питање је да је то само део интересовања индустријске шпијунаже. Остало се односи на радне навике запослених, њихову стручност, продуктивност, интерперсоналне односе у предузећу, врлине и слабости руководилаца, списак добављача, клијената, односно на све оне информације које могу допринети долажењу до информација које су степеноване, или које могу конкурентском предузећу да помогну да оствари бољи и успешнији положај на тржишту или да преузме најзначајније кадрове са готовим знањима у које је улагано годинама много новца.

С обзиром да сви ови подаци не могу бити пословна тајна, законом и нису заштићени од неовлашћеног прикупљања. Организацији остаје да сама изнађе најбоље начине и методе заштите од индустријске шпијунаже, како од оних облика који су законом санкционисани, тако и од оних који нису, али објективно могу нанети штету.

3.3. Финансијски напади

Финансијски напади се спроводе са циљем директног незаконитог долажења до новца или неких других финансијских вредности или неких услуга. Ови напади су најраспрострањенији тип компјутерског криминала и с обзиром на то да је о њима много писано нећемо их шире елеборирати.

3.4. Терористички напади

Ослањање на компјутере и информационе системе у свим сферама функционисања друштва чини ову инфраструктуру све више и више привлачном за терористичке нападе. Такви напади се суштински разликују од војних и обавештајних напада јер је сврха терористичког напада да ширењем страха код ширег круга људи натерају власт да промени понашање у односу на терористе и да на тај начин оствари политичке циљеве терористичких организација. Код војних и обавештајних напада циљ је само долажење до поверљивих информација. Прикупљање почетних информација неизоставно претходи било којој врсти терористичког напада. Значи да су мете физичког терористичког напада по правилу прво биле мете напада социјалног инжињеринга чији је циљ био долажење до почетних информа-

ција. Халид Ибрахим (Khalid Ibrahim) члан Пакистанске терористичке групе Харкат-УлАнсар (Harkat-UlAnsar) је познат по томе што користи методе социјалног инжењеринга како би дошао до информација које му омогућавају неовлашћен улаз у војну компјутерску мрежу Сједињених Америчких Држава.[27]

Као што је Долан рекао: „У социјалном инжењерингу све је у томе да се користе други да би се сакупиле информације и на тај начин остварио напад“. У периоду после 11. септембра 2001, социјални инжењеринг је део добро организованог сајбер напада који је усмерен тако да изазове панику заједно са физичким нападом на критичну инфраструктуру и постројења, као што су разне јавне структуре и компаније за снабдевање водом, енергијом и друге.[28]

Могуће мете напада могу бити системи који контролишу рад система производње и дистрибуције електричне енергије, системи телекомуникација и веза, здравствени системи, системи снабдевања водом, као и остали системи чијим нефункционисањем би били изазвани страх и паника.

Чак и ако се не спроведу овакви деструктивни напади остаје проблем који се огледа у томе да терористичке групе искоришћују комплексност Интернета за прикупљање средстава и прање новца, као и размену информација и координирање напада.

3.5. Осветнички напади

Осветнички напади се по правилу спроводе на штету неке организације владиних агенција или појединих особа. Штета се може огледати у губитку информација, немогућности њихове даље обраде или уништавању угледа одређених особа. Мотив који стоји иза ових напада обично је осећај љутње и беса и нападач би могао да буде садашњи или бивши запослени или неко од конкуренције.

3.6. Напади из забаве

Основни покретачки мотив овог напада је лично задовољство и узбуђење остваривањем упада у штићени систем. Ови нападачи по правилу преузимају готове програме са Интернета који им користе у овим нападима. Жртве ових напада углавном имају проблем приступа својим сервисима и подацима. Иако нападач који користи ову врсту напада може да уни-

---

[27] Colarik, A,.M.: *Cyber Terrorism: Political and Economic Implications*, Hershey, PA, USA: Idea Group Publishing, 2006, str. 35.

[28] Janczewski, J. L.; Colarik, M. A.: *Cyber Warfare and Cyber Terrorism,* Information Science Reference, Hershey - New York, 2008, str. 183.

шти податке, његов основни мотив је да компромитује систем заштите, а самим тим и организацију која га је поставила, као и да упад искористи за покретање напада на друге жртве.

Класификација претњи усмерених ка компјутерима може се извршити и према томе ко стоји иза напада и где је усмерен напад. Напад може бити усмерен на макро плану где је предмет напада држава са институцијама које је представљају и ресурсима који су значајни за њено функционисање. Друга врста напада је претња усмерена ка микро плану према појединим привредним друштвима, компанијама, банкама или институцијама.

Интересантни су подаци наведени у САД, где су проучаване и анализиране специфичне врсте група или организација које би могле да изврше напад на критичне инфраструктуре државе или владине компјутерске мреже. Утврђено је да преко 100 земаља има технолошке и информационе предуслове за ову врсту напада. Најмање 20 земаља има САД као мету, а неколико њих је има исте могућности информационих технологија и знања као и САД.[29]

По тој класификацији као претње су означене следеће групе:

- Националне државе (најређа претња, али у случају остварења могућност највеће штете),
- Терористи,
- Шпијуни, укључујући и корпоративну шпијунажу,
- Организовани криминал,
- Инсајдери[30] и
- Хакери (најчешћа претња, али најмања могућност за оштећење).

Технике и алати које користе свих ових шест група су обично исте, али мотивације и намере увелико варирају.[31] Из тог разлога и када се утврди напад, не може се са сигурношћу рећи ко стоји иза њега док се не ухвати извршилац, што је веома често неизводљиво. Ово указује на значај схватања борбе против социјалног инжењеринга који се користи код свих поменутих напада, јер се углавном не зна ко стоји иза претње.

Хакери представљају сталну претњу усмерену ка компјутерским системима. У почетку мотив је био проширивање знања и показивање рањивости

---

[29] Parker, T.; Shaw, E.; Stroz, E.; Devost, G. M.; Sachs, H. M.: *Cyber Adversary Characterization: Auditing the Hacker Mind,* Syngress Publishing, Inc., Rockland, 2004, str. 220.

[30] По овој класификацији инсајдер је лице које није нужно запослено у правном ентитету који је мета напада. У контексту ових претњи, инсајдери су сви они који имају приступ рачунарима и рачунарским мрежама и имају знање о вредности информација које се налазе у правном ентитету. Овој групи припада већина запослених, али такође могу да припадају и чланови породице запослених, пословни партнери, купци, добављачи и у ретким случајевима конкуренција.

[31] Parker, T.; Shaw, E.; Stroz, E.; Devost, G. M.; Sachs, H. M.: *Cyber Adversary Characterization: Auditing the Hacker Mind,* Syngress Publishing, Inc., Rockland, 2004, str. 221.

система. У следећој фази циљ је био прикупљање информација, а у фази у којој смо данас циљ је углавном неки облик финансијске добити. Промена циљева такође је значила промену извршиоца. Роџерс је дао своју класификацију 2000. године, а она је допуњена код Вилсона (Tim Wilson) 2007. године, где он писује осам категорија хакера.[32]

1. *Новајлија*: често назван и скрипт клинац. (script kiddies). Припадници ове групе су млађе особе, ограничених способности. Њихова примарна мотивација је потрага за узбуђењем и подизање сопственог ега. У жељи да докажу своје вредности упадом у системе, углавном користе софтвер који је неко други развио.

2. *Сајбер силеџија* (cyber punk): најближи су традиционалном изгледу хакера. Млади, обично мушког пола, са одређеним способностима и знањима у програмирању. Мотив им је, углавном, жеља да скрену пажњу на себе, а понекад и материјална корист. Обично бирају високо профилисане мете и обично се опредељују за вандализам уместо крађе информација.

3. *Интерни* (internal): запослени који користе своје интерне могућности приступа информацијама, коришћењем привилегија које имају. Могу се класификовати у две категорије. У прву улазе они који су незадовољни из било ког разлога и на овај начин се свете и другу они који имају финансијски мотив.

4. *Мали лопов* (petty thief): класични криминалци који у склопу своје криминалне каријере покушају да овладају нападима на компјутерске системе да би проширили поље свог криминалног деловања. У почетку нису довољно способни, али временом постају квалификовани. Основни мотив им је финансијска добит.

5. *Стари чувар* (old guard): Ова категорија види хакерство као ментални изазов и веома су радознали. Често су врло способни и имају потребна знања за писање компјутерских програма. Прихватају идеологију прве генерације хакера и обично немају криминалне намере. Деле са другима своје искуство, односно програме које су развили и написали.

6. *Писац вируса*: углавном млађе особе мушког пола, мотивисани пре радозналошћу или осветом, него озлојеђеношћу.

7. *Професионални криминалац*: у ову категорију се убрајају високо обучени ИТ стручњаци који користе своје вештине и знања за стицање финансијске добити. Они никада не желе да скрећу пажњу на себе. Раде за организоване криминалне групе.

8. *Информатички ратник*: мотивисани су патриотизмом, користе своје вештине да поремете системе „непријатељских земаља“. Обично су

---

[32] Wilson, T.: *Eight Faces of a Hacker*, 2007. http://www.darkreading.com/security/perimeter/showArticle.jhtml?pgno=1&articleID=208804443, преузето са сајта 21.09.2010.

добро обучени и високо квалификовани по знањима и вештинама којима располажу.

Најчешћа и највидљивија претња за компјутере и компјутерске мреже повезане на интернет је злонамерна хакерска субкултура. Нажалост, администратори система и напредни корисници компјутера сматрају себе члановима опште хакерске сцене. Због тога их је тешко разликовати од оних који имају зле намере и оних који то немају. Алатке које користе „бели шешир“ (незлонамерни), „црни шешир“ (злонамерни) идентичне су. На пример, хакери белих шешира користе скенере рањивости да пронађу или поправе безбедносне рупе да би спречили неовлашћен приступ, док хакери црних шешира користе исте алатке да пронађу и искористе безбедносне рупе да добију неовлашћен приступ.[33]

Следећи корак у заштити од социјалног инжињеринга је идентификација извора претњи, које могу да користе социјални инжењеринг као начин долажења до информација и података и да на тај начин угрозе безбедност информационих система. Деле се на *унутрашње, спољашње, и комбиноване претње.*

Унутрашња претња - инсајдери представљају лица која су запослена у предузећу, компанији и институцији без обзира на њихов радни статус. Унутрашња претња је претња која има извор унутар компаније, владине агенције или институције и обично представља незадовољног запосленог који није унапређен или је обавештен о отказу. Напад социјалним инжењерингом може да покрене и нападач који је тражио привремено запослење.[34]

Претње изазване инсајдером су или намерне или ненамерне, а унутар ове две групе оне могу (али не морају увек) бити деструктивне. Пример ненамерне и потенцијално деструктивне претње је када запослени прослеђује осетљиву електронску пошту на кућни налог да би радио на њој. Нормално да ови запослени не изгледају као да могу да нашкоде, али им нико није објаснио колики је ризик по губитак информација који они стварају прослеђивањем унутрашње електронске поште сами себи, путем јавног и незаштићеног система, коришћењем Интернета.

Ненамерне и потенцијално деструктивне претње инсајдера укључују запослене који инсталирају неки софтвер на компјутерима компаније иако знају да је то противно политици компаније.

Намерни и деструктивни инсајдер може бити, на пример, незадовољни администратор система који брише важне податке са сервера непосредно пре него што прекине радни однос.

---

[33] Parker, T.; Shaw, E.; Stroz, E.; Devost, G. M.; Sachs, H. M.: *Cyber Adversary Characterization: Auditing the Hacker Mind,* Syngress Publishing Inc., Rockland, 2004, str. 226.

[34] Schell, B.; Martin, C.: *Webster's New World Hacker Dictionary*, Wiley Publishing, Inc., Indianapolis, 2006, str. 169.

Неколико недавних истраживања сајбер криминала указује на инсајдера као претњу број један са којом се суочавају организације које користе компјутере и компјутерске мреже. С обзиром на комплексност компјутерских мрежа и обично мали број особља које даје подршку корисницима, инсајдери имају много могућности да изазову озбиљна оштећења. Злонамерни инсајдери јесу, а и остаће, највећа претња за поуздан рад критичних инфраструктура.[35]

Спољашњу претњу представљају лица која немају заснован радни статус са метом напада. Мотиви који покрећу спољашње претње су различити и зависе од тога који је разлог напада и према чему је усмерен. У ову групу можемо укључити категорије у коју се убрајају пословни партнери, чланови породице, купци, добављачи и конкуренција, као и тотално непозната лица, са којима организација није имала званичних контаката, али због онога чиме располаже, представља интересантну мету напада.

Социјални инжењеринг помаже злонамерним лицима да добију унутрашњи приступ поверљивим подацима код организација са софистицираним техничким безбедносним системима. Претварајући се да су легитимно запослена или да имају овлашћени приступ, лица која спроводе социјални инжењеринг користе рањивост у људским обичајима и учтивости пријатељског помагања некоме ко има неки проблем очекујући за узврат исто тако понашање када то њима затреба. Ако су способни да убеде легитимног запосленог неке организације да им се омогући физички приступ компјутерским ресурсима или приступ преко мреже, они су тада подигнути на статус инсајдера, јер сада имају две кључне ствари - приступ и знање.[36]

Комбинована претња се остварује заједничким и координираним нападом на информације, коју свесно и са намером спроводе лица која су запослена у неком правном ентитету, без обзира на облик правно-радног односа, заједно са лицима која нису запослена. По категоризацији степена опасности може се рећи да је ова претња најопаснија, с тим што, по досадашњим искуствима, није често остваривана.

4. Закључак

Најслабија карика у систему обезбеђења увек су људи, а најлакши начин да се продре у заштићени систем је планирање упада користећи се људима и њиховим слабостима. Тврдња да је једино безбедан компјутер онај који је искључен из извора напајања само је делимично тачна. Постојање

---

[35] Parker, T.; Shaw, E.; Stroz, E.; Devost, G. M.; Sachs, H. M.: *Cyber Adversary Characterization: Auditing the Hacker Mind*, Syngress Publishing, Inc., Rockland, 2004, str. 225.

[36] Parker, T.; Shaw, E.; Stroz, E.; Devost, G. M.; Sachs, H. M.: *Cyber Adversary Characterization: Auditing the Hacker Mind,* Syngress Publishing, Inc., Rockland, 2004, str. 225.

могућности да неког убедите да га укључи у извор напајања и потом активира оперативни систем, довољно говори о значају социјалног инжењеринга.

Социјални инжењеринг је техника у којој се убеђивање и/или обмана користе да би се добио приступ компјутерским системима.

Оно што усложава противмере у борби против социјалног инжењеринга је сазнање да свако ко има приступ било ком делу информационог система представља потенцијални ризик по безбедност информација. Било која информација до које се може доћи представља корак ка следећој информацији и тако док се не стигне до оне информације која је циљ напада. То указује на чињеницу да и запослени који се не сматрају безбедносно угроженим и нису укључени у мере заштите, могу бити мета напада социјалним инжењерингом.

За разлику од осталих напада на компјутере, социјални инжењеринг се не односи на технолошку манипулацију и коришћење рањивости хардвера или софтвера и поред тога не захтева посебне техничке вештине и знања. Ова врста напада експлоатише људске слабости, као што су немарност или жеља за кооперативношћу, како би се добио приступ легитимним документима који се налазе на компјутеру.

Социјални инжењеринг може бити спроведен због профита, сајбер тероризма или за приступ интерним системима и поверљивим информацијама. Најчешће се нападају велике организације које обрађују и складиште осетљиве податке, као што су провајдери телекомуникационих услуга, мултинационалне компаније, финансијски установе, болнице и војска или владине установе или агенције. Наравно, поред наведених напад може бити усмерен и према било ком предузећу.

Лица која спроводе социјални инжењеринг су веома интелигентне и изузетно креативне особе. Поседују добре комуникацијске и манипулаторске вештине, добри су познаваоци психологије и углавном имају довољно техничког знања. Могу да наступају тимски и самостално, с тим што је тимски напад много опаснији јер удружују своја знања и умећа поштујући се међусобно и уважавајући хијерархију.

Из тог разлога прихватљивије је рећи да су предуслови представљени кроз четири категорије или фактора и то: 1) мотив, 2) спремност, 3) могућност и 4) метод. Уколико један од четири поменута фактора не постоји, напад се неће десити.

Критичне информатичке инфраструктуре су рањиве на нападе на много начина укључујући и нападе физичким приступом и нападе изведене преко компјутерске мреже. Међузависност елемената инфраструктуре чине ризичним све елементе, тако да ће успешан напад на један део система сигурно утицати на друге делове система који нису директно нападнути.

Технике и алати који се користе обично су исти, али мотивације и намере увелико варирају. Из тог разлога и када се утврди напад, не може се са сигурношћу рећи ко стоји иза њега док се не ухвати извршилац, што је веома често неизводљиво. Ово указује на значај схватања борбе против социјалног инжењеринга који се користи код свих поменутих напада, јер се углавном не зна ко стоји иза претње.

Инсајдери се наводе као претња број један са којом се суочавају организације које користе компјутере и компјутерске мреже. С обзиром на комплексност компјутерских мрежа и обично мали број особља који дају подршку корисницима, инсајдери имају много могућности за изазивање озбиљних оштећења. Злонамерни инсајдери јесу, а и остаће, највећа претња за поуздан рад критичних инфраструктура.

Социјални инжењеринг помаже злонамерним лицима да добију унутрашњи приступ поверљивим подацима код организација са софистицираним техничким безбедносним системима. Претварајући се да су легитимно запослени или да имају овлашћени приступ, лица која спроводе социјални инжењеринг користе слабости у колегијалним обичајима и учтивости. Способни су да лако убеде запосленог неке организације да им се омогући физички приступ компјутерским ресурсима или приступ преко мреже и тада имају две кључне ствари - приступ и знање.

Ljubomir Stajić, Ph.D., Full Professor
Faculty of Law Novi Sad

Goran Mandić, LL.M.,Instructor
Faculty of Security Studies University of Belgrade

Social Eengeneering as the Form of Endangering Confidential Business Information

Abstract

In many jobs, especially the ones where you need to get some confidential information in contact with other people, there are some forms of social engineering. Social engineering is the form of oral and gesture manipulation with individuals, aiming to impose them fulfill a kind of demands, made by the attacker.

The existing problems in the confidential information protection sphere appear in the fact that behind each computer, there is a human being, as an individual, with own good and bad characteristics. Social engineering is a technique where persuading and/or delusion are used for getting the access to the computer systems. This is usually accomplished by conversation or some other forms of interactive communication.

Countermeasures in fighting against social engineering are getting more complicated due to the fact that anyone who has the access to any part of the information system represents a potential risk to information security.

Unlike other attacks on computers, social engineering does not refer to technological manipulation or the use of hardware and software vulnerability. Besides that, it does not demand any special technical skills and knowledge. This kind of attack exploits human weaknesses, as negligence or cooperation wish, in order to get an access to the confidential documents existing in the computer.

Social engineering can be organized for the sake of profit and cyber terrorism or for the access to internal systems and confidential information. Big organizations that process and save sensitive data are the most often attacked and among them are telephone services providers, multinational companies, financial entities, hospitals, Government agencies, military service and others.

Key words: social engineering, information security, security systems, companies, hackers, computer crime.