UDC: 004.491/.492-094.2

Социјално Инженерство

Марија Шандуловска, Ерол Максуд, Доц. Д-р Сашо Гелев
sandulovska.marija@live.eurm.edu.mk; maksud.erol@live.eurm.edu.mk;
saso.gelev@eurm.edu.mk

Абстракт— Иако повеќето организации од целиот свет моментално посветуваат поголемо внимание на обезбедување на информациските системи со помош на софистицирани сигурносни алатки, сепак тие системи се уште остануваат отворени и ранливи. Земајќи ја во предвид оваа реалност, напаѓачите (хакерите) се насочуваат кон употреба на социјалното инженерство, наместо користење на нивните технички вештини за да дојдат до саканите информации. Концептот на социјалното инженерство во суштина е да се манипулира со корисниците на системот, кои се сметаат за најслабите алки на синџирот, со цел да се добие одредена информација. Повеќето луѓе сметаат дека социјалното инженерство е дело на криминални умови кои користат психолошки трикови врз корисниците на целниот компјутерски систем. Нешто за што сите се согласуваат е дека социјалното инженерство е паметна манипулација на напаѓачот со природата на човековата доверба. Целта е да се добијат информации кои на социјалните инженери ќе им овозможат неавторизиран пристап до вредни системи и до информациите кои се наоѓаат во тој систем. Ова всушност значи дека искусен социјален инженер може да добие пристап до секој информациски систем, независно од хардверските и софтверските механизми имплементирани за заштита на системот. Овој труд ќе го опише социјалното инженерство и некои од најчестите техники применувани од социјалните инженери и ќе претстави некои од начините со кои може да и се спротивставиме на оваа закана.

Клучни зборови—*Безбедност, социјално инженерство, dumpster diving, fishing, shoulder surfing, vishing.*

I. Вовед

Социјално инженерство, честопати нарекувано како „хакирање на луѓето“, претставува користење на психолошки трикови врз легитимни корисници на компјутерски системи од страна на напаѓачи/хакери, за да се здобијат со информации (кориснички имиња, лозинки, лични кодови за идентификација - ПИН-ови, броеви на кредитни картички и сл.) потребни за добивање пристап до нивните системи.

Зошто некој би се обидувал да ги напаѓа технологиите за заштита како: „firewalls“, автентикација, техники за превенција од провала во систем и енкрипција, со цел да се пробие одреден систем или да се украдат информации, кога може да се насочат кон најслабата алка во синџирот – вработените? Такви реализации не претставуваат некаква тајна во самата заедница на напаѓачите/хакерите.

Всушност, Кевин Митник, еден од најпознатите хакери од 1980-тите и 1990-тите години, тврди дека најголем дел од успешноста на нападите се должи на неговата способност да манипулира со луѓе за разлика од неговите технички вештини како хакер. И самиот Митник забележува дека е многу полесно да излажеш некого да ја открие својата лозинка отколку да се преземе некој комплициран напад за истата цел [1].

Во февруари 1995 година, Митник беше уапсен за компјутерски криминал за кој што требаше да помине 4 години во затвор. Главната област од хакирањето на Митник беше социјалното инженерство. Откако беше ослободен, објави книга на тема Социјално Инженерство со наслов: „Уметноста на измамата“, во која тој го дефинира социјалното инженерство како: „Социјалното инженерство користи влијание и убедување за да се измамат луѓето така што ќе поверуваат дека социјалниот инженер е некој кој всушност не е, или истото тоа преку манипулација. Како резултат на тоа, социјалниот инженер е способен да ги искористи луѓето за да добие информации со или без користење на технологија“ [1].

Некои може да кажат дека социјалното инженерство е уметност или вештина која не може секој да ја има. Ова е делумно точно, бидејќи секој нема добри социјални вештини. Сепак, повеќето луѓе се програмирани да бидат социјални инженери уште од многу рана возраст. Како деца, луѓето учат како да го добијат она што тие го сакаат со користење на тактики од социјалното инженерство.

Со малку размислување и труд, социјалното инженерство може да биде лесен и ефикасен начин за одредено лице со злонамерни намери да го направи животот на било која организација тежок. Социјалното инженерство не бара високо ниво на техничко знаење, но бара поединецот да има солидни социјални вештини. Хакер кој поминува неколку часа во обид да ги пробие лозинките, може да заштеди драгоцено време со

што би им се јавил на вработените, претставувајќи се како техничка поддршка или вработен во ИТ одделот и истите да ги побара од нив.

Социјалното инженерство користи многу основни квалитети на човековата природа.

Според Peltier, социјалните инженери целат на луѓе кои по природа сакаат да помогнат, кои се плашат да западнат во неволја и кои сакаат да најдат пократки патеки да ја завршат работата [2]. Користењето на мааните на човечката природа е многу полесно отколку наоѓање пропусти во софтверот за енкрипција.

Социјалното инженерство најчесто следи некоја одредена шема. Оваа шема се состои од четири различни фази: собирање на информации, развој на односите, извршување и искористување [3].

За време на фазата на собирање на информации, истражувањето е спроведено за да се соберат колку што е можно повеќе информации за организацијата. Ова е важно со цел да научат кои или какви информации може да бидат насочени во рамките на една организација, кои слабости можат да се искористат со цел да се соберат саканите информации и да се најде начин како да избегнат да бидат фатени од организацијата. Втората фаза, развојот на односите, се фокусира на развој на односите и довербата, зависно дали е остварен контакт со еден или со повеќе вработени во организацијата. Во оваа фаза е потребно да се посвети внимание на ситни детали бидејќи погрешно толкување на истите може да доведе до неуспех. Третата фаза се фокусира на искористување на довербата со поигрување на емоциите на метата (вработениот) за да се побараат информациите. Ова е главниот дел од нападот и фазата во која се разменуваат информациите. Конечно, последната фаза е искористување на информациите. Понекогаш, информацијата добиена од лицето од организацијата често е лозинка или начин како да се пристапи до системот.

Мотивите на напаѓачот може да варираат од стекнување на финансиска корист, па до одмазда или некој друг емоционален импулс, но крајната цел е иста, да се компромитираат информации за организацијата или некој компјутерски систем, за постигнување на лична сатисфакција.

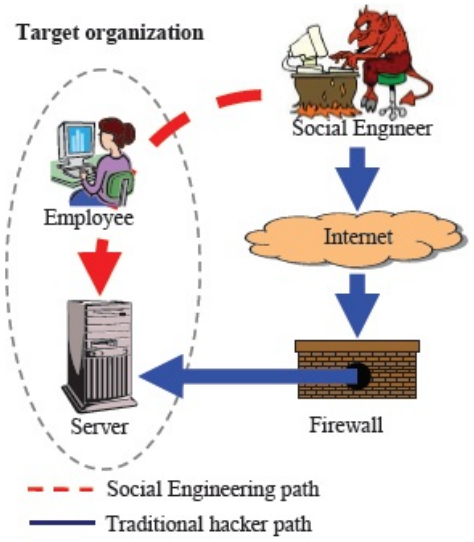
II. Методи на напади

Социјалното инженерство може да биде опишано преку две главни категории, технички базирани напади и човечки базирани напади.

Технички базираното социјално инженерство се потпира на техниките за измама на одредени поединци за обезбедување информации кои ќе му овозможат на напаѓачот да добие понатамошен пристап во мрежата.

Наједноставниот и најпопуларен начин на социјално инженерство се уште е човечко базирано. Човековиот пристап се прави преку измама, со искористување на незнаењето на жртвата и самата природа на човекот да помага во одредени ситуации. Се потпира на меѓучовечки односи и измама, применувајќи: ласкање, заплашување, деградирање, авторитативно поставување и омаловажување. „Секој медиум кој овозможува комуникација еден-на-еден помеѓу луѓето може да биде искористена, вклучувајќи комуникација лице во лице, телефонски разговор или електронска пошта. Се што е потребно, е да си добар лажго“ [4].

На пример ако напаѓачот се претставува како личност кој има голем авторитет, се јавува до техничката поддршка, претставувајќи се како главен раководител и тврди дека ја има заборавено својата лозинка, техничката поддршка може да ја ресетира истата и новата лозинка да му ја даде на напаѓачот. Во овој случај напаѓачот има отворени врати за да ги изведе своите злонамерни дејства.



Слика 1. Напад на социјално инженерство.

A. Технички базирани напади

Слика 2. Технички базирани напади.

1) „Phishing“

Овој термин се употребува во случај кога пристигнува електронска порака од некоја легитимна организација, како на пример банка. Во пораката има барање до корисникот да изврши верификација на информациите, во спротивно би се соочил со непосакувани последици. Пораката најчесто содржи линк до некоја веб страница која навидум изгледа како легитимна, со различни логоа на компанијата и содржина и се разбира има некаква форма во која треба да се внесе корисничко име, лозинка, број на кредитна картичка или детали за лични идентификациски кодови.

2) „Vishing“

Оваа техника е всушност иста како и претходната, но е изведена преку VoIP (Voice over IP). Ги користи предностите на довербата на јавноста во својата телефонска услуга. Хакерите кои користат VoIP манипулираат со системот за идентификација на повик со цел да го прикажат повикот дека доаѓа од некоја друга локација, а истите да се претстават како некој што не се. Ова го отежнува лоцирањето на ваквиот злонамерен повик.

Најчеста тактика на „vishing“ која се користи од измамниците е преку оставање на снимена порака, на пример од компанијата за кредитни картички, информирајќи го корисникот дека има некаков проблем со неговата картичка. Пораката исто така најчесто завршува со некакво итно барање за корисникот да повика телефонски број како би се решил проблемот. На овој начин корисникот на кредитната картичка својот број наместо на својата банка ќе му го пренесе на социјалниот инженер или на се позачестените крадци на идентитет.

3) Спам електронски пораки

Електронските пораки кои нудат пријателство, подароци, бесплатни слики или филмови ја искористуваат анонимноста и блискоста која ја овозможува Интернетот за да го достават својот злонамерен код.

Вработениот ќе ја отвори електронската порака преку која може да се пренесе тројанец, вирус или „црв“, наоѓајќи го својот пат до останатите системи или мрежата. Вработениот најчесто е мотивиран да ја отвори пораката бидејќи е привлечен од тоа што го нуди самата порака, како корисни информации, нотификации за некои безбедносни надградби, шеги, озборувања, фотографии, музика, филмови или софтвер. Резултатот може да биде различен, од непријатна ситуација, забавување на системот, па се до уништување на комуникацискиот систем или на записите.

4) „Popup“ прозорец

Злонамерната програма на напаѓачот, генерира popup прозорец, кажувајќи му на корисникот дека се појавиле проблеми со мрежната врска и дека е потребно повторно да ги внесе корисничкото име и лозинката за да ја продолжи сесијата. Корисникот веднаш без никаков сомнеж ќе ги внесе потребните информации за да ја продолжи својата работна задача. Откако ова ќе се случи информациите ќе бидат испратени назад до серверот каде што се наоѓа програмата на напаѓачот. Се разбира за ваков напад да може да се изведе напаѓачот мора да има одреден пристап до системот. По одредено време ќе се прочуе дека се случил напад врз системот, но многу често никогаш не се дознава кој ја отворил вратата за пристап на напаѓачот.

5) Занимлив софтвер

Во овој случај жртвата е убедена да превземе и инсталира некоја „корисна“ програма. Може на изглед да се прикаже прозорец како програма со која ќе се подобрат перформансите на компјутерот или софтвер со кој ќе можат бесплатно да се превземаат многу други софтвери. Во овие случаи најчесто се инсталира „Spyware“ или „Malware“ преку злонамерна програма претставена преку некоја занимлива порака.

6) „Baiting“ - Мамка

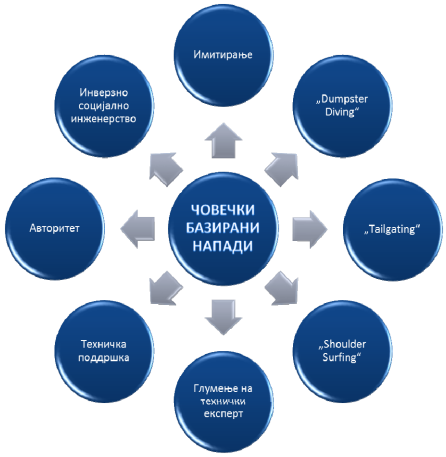
Во овој случај напаѓачот остава инфицирана дискета, CD или USB на некоја локација (лифт, ходник, паркинг) за која е сигурен дека некој ќе го пронајде. После тоа му преостанува само да чека.

На пример, напаѓачот може да креира диск на кој ќе биде отпечатено логото на компанијата и да напише дека го содржи целосниот извештај за работата на компанијата, ова сигурно звучи привлечно за секој вработен да го стави дискот во компјутер и да го стартува.

Последицата од ставање на ваквиот злонамерен диск е тоа што ќе се стартува инсталација на злонамерен код кој што потоа ќе го отвори системот за напаѓачот да пристапи до внатрешната мрежа.

Доколку компјутерот не го блокира овој инфициран софтвер, тогаш тој компјутер ќе биде почетна точка од каде што напаѓачот ќе може да ги напаѓа преостанатите компјутери. Анти-вирусните програми бараат злонамерен софтвер врз основа на веќе постоечки, но доколку тој софтвер е програмиран специјално за некоја цел, многу е тешко истиот да се открие.

B. Човечки базирани напади



Слика 3. Човечки базирани напади.

1) Имитирање

Имитирањето во главно значи креирање на некој вид на карактер и играње на таа улога. Некои најчесто креирани улоги се: ИТ техничка служба, инсталатери на телекомуникациска опрема, дури и колега/соработник. Креирањето на вакви карактери во големи компании не е воопшто тешко, бидејќи имаат голем број вработени и не постои начин да се знаат сите, а идентификациските картички можат да се фалсификуваат.

Ова е начин со кој се создава сценарио со кое се убедува жртвата да даде некоја информација или да изврши некаква активност и ова најчесто се изведува преку телефон. Ова е многу повеќе од едноставна лага бидејќи е потребно претходно истражување или планирање за да се искористат сите делови од добиената информација (датум на раѓање, адреса, начин на плаќање на сметки итн).

2) „Dumpster Diving“ - Барање по контејнери за ѓубре

Најчесто големите организации, во контејнерите на компанијата фрлаат работи како: телефонски именици, упатство за користење на системите, календари со датуми за одржани состаноци, печатени документи со важни податоци како кориснички имиња и лозинки, печатени документи со изворен код, дискови, компаниски писма, белешки, застарен хардвер. Напаѓачот може да ги искористи овие предмети за да добие голема количина на информации за организацијата на компанијата и мрежната структура.

Во интервју за BBC News Online, Кевин Митник објаснува: „како со малку знаење, хакерот кој звучи како вработен во фирмата, може да ги натера вработените непрекинато за него да обезбедуваат огромна количина на корисни информации“ [5].

Хакерот може да користи лист хартија на кој што стои заглавие со компаниското лого за да се прикаже како официјална кореспонденција. Хакерот може да извлече доверливи информации од хард дискот од компјутерот, иако корисникот мисли дека ги има избришано од дискот.

3) „Tailgating“

„Tailgating“ е кога неавторизирано лице следи некое авторизирано лице во обезбедена зграда. Кога напаѓачот кој што ја следи жртвата ќе влезе во обезбедената зграда, ќе може да изнесе вредни информации. Напаѓачот може да се движи насекаде и да собира информации како: имиња и телефонски броеви на вработените, за подоцна да ги искористи за имитирање на одреден вработен. Напаѓачите можат да украдат компјутери, PDA, дискови, документи или било што на кое може да се најде некоја доверлива информација. Овие напаѓачи може да пристапат до собите каде што се наоѓаат серверите и другата мрежна опрема.

Најголемата предност кај овој вид на напаѓачи е човековата природа. Во човековата природа е да ја држиме вратата отворена за оној кој што доаѓа зад нас, при тоа не знаејќи дали таа личност е вработен, дали е авторизиран да пристапи онаму каде што ние можеме, или е злонамерен напаѓач.

4) „Shoulder Surfing“

„Shoulder surfing“ е друга форма на социјално инженерство и се врши од страна на колеги вработени или имитатори. Ова се изведува така што се стапува во контакт со жртвата, на тој начин што ги забавува, а потоа прави ментални слики од она што го пишуваат на тастатура, во главно при внесувањето лозинки или пристапувањето до информацискиот систем. Друг метод е кога напаѓачот се движи низ некоја обезбедена област и ги набљудува компјутерски екрани и го меморира внесот на податоците.

Повеќето напаѓачи може да користат камера со која ќе го снимаат компјутерскиот екран од што подоцна ќе можат да извлечат податоци. Бидејќи камерите може да бидат многу мали и лесни за криење, за напаѓачите е многу едноставно да ја користат оваа техника без некој да ги забележи дека воопшто имаат камера. Тие исто така можат да користат разни оптички помагала (двогледи, телескопи итн.) за да ги прочитаат информациите од екранот. Ова најчесто би се случило доколку компјутерот се употребува на јавно место.

Постојат уште две други стратегии кои се поврзани со овој метод – прислушување и „snooping“/душкање.

Прислушувањето е слушање на некој разговор за да се извлечат некои информации; многу е слично на „shoulder surfing“, само што се користат ушите. Од друга страна, „snooping“ е пребарување низ датотеки и документи за да се дознаат информации. Во потрага по информации ваквиот напаѓач најпрво ќе побара под тастатурата, во белешките или на другите места каде што корисниците најчесто ги оставаат нивните лозинки.

5) Глумење на технички експерт

Ова е случај кога натрапникот се преправа дека е технички експерт кој работи на проблем со мрежата, барајќи од корисникот да му даде пристап до работната станица за да го „поправи“ проблемот. Корисникот, особено ако не е технички поткован, најверојатно нема да поставува прашања, дури нема ни да ја гледа поправката на компјутерот доколку е превземена од страна на техничар. Во овие случаи корисникот се обидува да биде корисен и ја врши својата улога со цел да се надмине проблемот со мрежата во компанијата.

6) Техничка поддршка

Во овој случај напаѓачот може да се претставува како вработен или придружен персонал и да го изведе својот напад. Човек облечен како чистач може да пристапи до работните простории, носејќи опрема за чистење. Во случајов не се појавува да ја исчисти вашата работна маса, туку тој ќе пребарува наоколу за да пронајде важни информации - како на пример лозинки, доверлива датотека или ако сте заборавиле да го заклучите вашиот компјутер. Исто така може да направи телефонски повик преставувајќи се како вас.

Може и да се претстави како техничка поддршка од вашата телефонска компанија и да каже дека треба да го поправи телефонскиот апарат. Наместо тоа може да постави уред за прислушување, па потоа да шпионира.

7) Авторитет

Напаѓачот може да се јави на компанијата за компјутерска поддршка и да се преправа дека има проблеми со пристапот до системот. При тоа да тврди дека е потребно многу брзо да пристапи до системот, барајќи од техничката поддршка да ја ресетира лозинката и да му биде пратена или дадена веднаш преку телефон. Ако напаѓачот е доверлив во својата приказна и додава информации кои укажуваат на вистинскиот корисник, техничката поддршка е се поверојатно да поверува и да го направи она што напаѓачот го бара.

8) Инверзно социјално инженерство

Инверзно социјално инженерство е кога социјален инженер дејствува како лице во позиција на авторитет на кое вработените ќе се обратат за помош. Тоа се нарекува инверзно, бидејќи жртвата е таа која иницира контакт, а не социјалниот инженер [6]. Овој пристап бара опширно истражување и подготовка за да успее. За социјалниот инженер треба да се создаде ситуација каде што жртвата ќе биде принудена да се поврзе со него за да се реши проблемот. Овој пристап може да се примени на два начина. Социјалниот инженер да изврши директен напад или да користи ситуација со која ќе воспостави доверба и добра врска со жртвата, од што во иднина можат да произлезат криминални активности [7].

Процесот на инверзно социјално инженерство се состои од три главни чекори. Сите три од овие чекори се неопходни за овој тип на напад.

Саботажа - првиот чекор вклучува компромитирање на целниот компјутерски систем, на пример преку инсталирање на злонамерен софтвер во него. Целта на оваа активност е да се добие ситуација во која корисникот верува дека постои вистински проблем со системот и има за цел да помогне да се реши овој проблем.

Маркетинг – социјалниот инженер мора да биде сигурен дека корисникот ќе го повика токму него за да го реши проблемот со системот. За да се осигура дека ќе го повика корисникот мора да се рекламира. Постојат неколку начини да се направи тоа. Поставување на визит-карта во близина на канцеларијата на корисникот. Друг начин на рекламирање е малициозниот софтвер кој содржи контакт информации во генерираната пораката за грешка.

Поддршка - Кога социјалниот инженер ќе стигне до овој чекор, главна задача е да се види дека корисникот останува несвесен за постоење на опасноста. Потоа социјалниот инженер пристапува кон поправање на системот. Ова е моментот кога тој треба да определи дали ќе ги побара информациите веднаш или ќе гради однос на доверба со жртвата. Најефикасен начин е да успее да ги изведе двете работи.

Рик Нелсон во неговиот труд на тема „Методи на хакирањето: Социјално инженерство“, вели дека: „Хакерите ја саботираат мрежата, предизвикувајќи појава на проблеми. Потоа напаѓачот рекламира дека тој е соодветен контакт кој може да го поправи проблемот, а потоа кога ќе дојде да го поправа проблемот со мрежата, тој ќе побара одредени делови на информации од вработените и го добива она за што тој навистина дошол. Тие никогаш нема да знаат дека тој е хакер, бидејќи проблемот ќе биде отстранет од нивната мрежа“ [8].

III. (Превенција) Заштита од социјалното инженерство

Едукацијата на корисникот е првата и најмоќната одбрана против социјалното инженерство, поткрепено со цврста, јасна (писмена) полиса која дефинира кога и на кого од корисниците им е дозволено да ги даваат нивните лозинки, кој може да ја отвори серверската соба, итн.

Мора да бидат утврдени строги процедури. Со спроведување на проверка на системот (смарт картички / токени, или, уште подобро, биометрика), може да се спречат многу обиди за социјално инженерство. Дури и ако социјалниот инженер успева да ја дознае лозинката, тоа ќе

биде бескорисно доколку постои некој друг фактор за проверка во другото ниво. Успешната одбрана против социјалното инженерство зависи од тоа дали компаниите имаат добри полиси и дали сите вработени ги следат. Социјалното инженерство има напади кои се доста моќни бидејќи се цели на човечкиот фактор, кој е понепредвидлив отколку софтверските системи. Сепак постојат неколку заштитни мерки за да се спречат некои од нападите.

A. Полиси

Добро дефинираните полиси се еден од основните темели на планот за безбедност. Тие треба да бидат напишани на јасен, концизен јазик, ослободен од ИТ стручни поими. Во нив исто така треба да се опише она што се очекува и да се наведе кој треба да се контактира доколку има некакви прашања.

Полисите имаат животен век, тие треба да содржат датум на преглед и секогаш да бидат ажурирани. За самиот процес на полисите во безбедноста да функционира, истите мора да бидат ревидирани најмалку на секои 5 години. Некои поклучни полиси можат да бидат ревидирани почесто, како што се откриваат нови закани и мора да бидат адаптирани, старите полиси да се ажурираат, а непотребните да бидат отстранети. Откако ќе се ажурираат полисите најдобро е да бидат поставени на компаниската мрежа, како би била достапна најновата верзија на полисата.

Полиси кои можат да се применат против социјалното инженерство се:

Објавување на информации

Безбедносната полиса треба да определи кој и под какви околности може да објавува информации. На пример, добро смислена полиса ќе одреди лице до кое би стигале сите анкети.

Одобрување на пристап

Безбедносната полиса треба да определи:

- Дали е потребно да се потпише некаков документ за да се одобри влез во компјутерски систем.
- Кој е овластен да даде пристап до системот и каков тип на пристап може да се даде.
- Определување на методите за креирање и поништување на кориснички сметки.
- Развој на посебни процедури за креирање на кориснички сметки за да се избегне забуна и грешки.

Промена на лозинки

Полисата треба да бара употреба на специјални знаци, бројки, мали и големи букви за да се добиваат цврсти лозинки. Исто така треба да се наведе и фреквенцијата со која треба да се врши промена на лозинките, како и да им се укаже на вработените да не ја запишуваат лозинката.

Корисничка поддршка

Треба да постои политика која ќе и забранува на корисничката поддршка да дава информации како лозинки, без претходно да ги провери податоците за вработениот:

- Да му се јави на корисникот за да ја потврди неговата локација.
- Преку користење на систем за идентификација на телефонски повици.
- Дигитален потпис на вработениот.
- Вработениот лично да ги бара информациите.

Идентификација на вработени

Организацијата мора да развие полиса и процедура за идентификација на вработените, како на пример носење на идентификациона картичка со фотографија.

Посетителите мора да бидат регистрирани и да носат привремена идентификациона картичка. На вработените треба да им се укаже да пријават кога некој се појавува без картичка.

Уништување на докуенти

Полисата треба да бара од вработените да ги уништуваат документите со важни информации, за да се избегне „dumpster diving“ нападот.

Физичка безбедност

Мора да бидат идентификувани чуствителните области и да бидат обезбедени од физички пристап на неовластени лица.

Пробивање на безбедноста

Потребно е да постои едноставен начин на кој вработените ќе можат да пријават сомнителна ситуација или активност.

Животен век

Животниот век на информацискиот систем, чувањето и уништувањето на податоците и хардверот мора точно да биде дефиниран и познат [9].

B. Едукација

Постојат неколку различни начини на едукација на вработените, сите со свое ниво на ефикасност. Популарно е компаниите да користат комбинација од следните алатки за образовни цели: видео, билтени, брошури, знаци, постери, screensaver-и, бележници, маици и налепници.

Проблемот со алатките кои корисниците ги гледаат секој ден е во тоа што тие стануваат запоставени. Затоа тие често треба да се разменуваат со цел да ги исполнат своите цели.

Кога се едуцираат корисниците, мора да се разбере дека не е доволно само да им се кажува како треба да се однесуваат. Важно е дека тие треба да бидат свесни за причините за едукацијата и целосно да разберат зошто треба да се однесуваат на одреден начин. За ефикасно едуцирање, важно е раководството, како и

остатокот од вработените целосно да се запознаат со едукацискатa програма.

Многу ефективна образовна техника е да им се укаже на вработените дека тоа што тие го прават не се однесува само на компанијата туку и на самите нив. Автентични приказни за напади од социјално инженерство, безбедносни совети и информативни приказни објавени во компаниската мрежа или во електронската пошта, се едни од најдобрите методи за едуцирање на вработените во поглед на ризиците на социјалното инженерство.

Исто така, овие приказни може да се искористат во обука за подигнување на свеста за безбедност на вработените. Користењето на автентични приказни при едукација на вработените го зголемува нивниот отпор кон експлоатацијата на социјалното инженерство [9].

Печатењето и објавувањето на безбедносните процедури на организацијата и претпоставувањето дека вработените ќе ги читаат и разбираат е малку наивна. Безбедносните процедури и практичниот тренинг треба да му се објаснуваат на секој нов вработен и да се повторуваат периодично. Постојаното обучување на вработените е важно за да се одржи нивната свест за социјално инженерство на високо ниво. Внатрешен веб сајт кој е посветен за безбедносни информации е добар начин да ги задржи вработените информирани и едуцирани [10].

Социјалните инженери се свесни дека вработените на најдолните слоеви се најранлива група на која целат социјалните инженери, бидејќи тие многу полесно можат да откријат информации.

Но, бидејќи социјалните инженери може да го нападнат секој вработен за да добијат информации, сите вработени треба да се загрижени за начините на напад и да знаат на кој да му се обратат доколку настанат проблеми. Градењето на тимови ја зголемува организираноста на компјутерската и организациската безбедност [11].

Недостатокот на безбедност е ретка причина за успешни напади. Причината е едноставно тоа што корисниците се само луѓе. Не само корисничката поддршка е цел на напади, туку секое ниво има одреден ризик од напад на социјално инженерство, што би резултирало со прекршување на процедурите и полисите. Најлоша претпоставка е дека секој може да биде имун на ваквите напади [6].

IV. Заклучок

Една компанија може да ги набави најдобрите безбедносни технологии, да ги обучи своите вработени како да ги извршат сите безбедносни мерки, и да ангажира луѓе од најдобрите фирми за обезбедување, но таа компанија се уште ќе биде целосно ранлива.

Социјалното инженерство е начин на кој натрапникот може да добие пристап до информационите ресурси, без да мора да биде технички, мрежен или експерт за безбедност. Напаѓачот може да користи многу тактики со цел или да ја измами жртвата за да му ги обезбеди информациите кои му се потребни за да добие влез или да ги добие тие информации без знаење на жртвата.

Социјалното инженерство не може целосно да се отстрани, тоа е сериозен проблем и е една од најголемите закани за безбедноста на организациите.Тоа е потценет безбедносен ризик кој многу ретко е опфатен од страна на компаниите.

Организациите може да го намалат влијанието на овие напади преку едуцирање на своите вработени. Организациите, исто така, треба да воспостават јасна полиса, која ќе вклучува стандарди, процеси и процедури за да се помогне во елиминирањето на заканите од социјалното инженерство.

Организацијата мора да обезбеди дека овие полиси и тренинзи се изведени соодветно од страна на корисниците, според тоа во текот на едукацијата треба да им се даде примери на вработените од последните напади на социјално инженерство.

Од ова може да се заклучи дека социјалното инженерство не може целосно да биде отстрането се додека е вклучена човековата природа, но може да се користи друга опција за да се минимизираат неговите ефекти врз организацијата, а тоа е континуирано да се обучуваат вработените да бидат претпазливи и способни да го препознаат нападот.

Библиографија

[1] Mitnick, K.D. and Simon, W.L. 2002. The Art of Deception: Controlling the Human Element of Security. Indianapolis, Indiana: Wiley publishing, Inc.

[2] Peltier, T. 2006. Social Engineering: Concepts and Solutions. EDPACS 33, 1-13.

[3] Allen, M. 2007. Social Engineering: A means to violate a computer system. SANS Institute.

[4] Denning, D.E. 1998. Information Warfare and Security, Addison-Wesley.

[5] Mitnick, K.D. October 14, 2002. How to Hack People. BBC NewsOnline.

[6] Gartner, M. Information Security Strategies Research Note TU-14-5662.

[7] Gragg, D. 2002. A multi-level defence against Social Engineering. SANS Institute.

[8] Granger, S. 2001. Social Engineering Fundamentals, Part I: Hacker Tactics. Retrieved December 8, 2005, from SecurityFocus web site:http://www.securityfocus.com/infocus/1527.

[9] Arthurs, W. 2001. A proactive defence to Social Engineering. SANS Institute.

[10] Tims, R. 2001. Social Engineering: Policies and education a must. SANS Institute.

[11] Nelson, R. Methods of hacking: Social Engineering. The Institute for Systems Research, University of Maryland.

Summary

SOCIAL ENGINEERING

Abstract:*Even though most organizations around the world currently pay more attention to the security of information systems with the help of sophisticated security tools, these systems still remain open and vulnerable. Taking into account this reality, the attackers (hackers) are directed toward the use of social engineering, instead of using their technical skills to get to the desired information. The concept of social engineering is to manipulate the users of the system, which are considered to be the weakest links of the chain, in order to obtain certain information. Most people believe that social engineering is the work of the criminal minds who use psychological tricks on the users of the target computer system. Something we all agree with is that social engineering is a smart manipulation of the attacker with the nature of the human trust. The aim is to obtain information that will enable the social engineers to have unauthorized access to valuable systems and the information in that system. This means that skilled social engineer can gain access to any information system, regardless of the hardware and software protection mechanisms implemented to protect the system. This paper will describe the social engineering and some of the most common techniques used by social engineers and will outline some of the ways in which we can stand against this threat.*

Key words: *Dumpster diving, fishing, security, social engineering, shoulder surfing, vishing.*