UDC: 343.533.9:004

Корпорациска истрага на компјутерски криминален инцидент

М-р Марјан Стоилковски, Зорица Каевиќ, Д-р Сашо Гелев
risto.hristov@eurm.edu.mk; saso.gelev@eurm.edu.mk

Апстракт- *Во овој труд обработена е проблематиката на спроведување на истражни постапки во рамките на институцијата во која се случил компјутерскиот криминален инцидент, односно опишана е таканаречената корпорациска истрага, почнувајќи од првите информации за случување на криминалниот инцидент, преку составување на корпорациски тим за истрага, извршување на истражните активности, собирање на дигитални докази, нивната припрема за презентација пред врвните менаџери на институцијата, па се до донесувањето на одлука дали е потребно истрагата да се предаде во надлежност на званичните истражни органи или не.*

На крајот е даден пример за спроведување на една ваква истрага.

Клучни зборови: *Компјутерски криминал, дигитален доказ, истрага на компјутерски криминал, корпорациска истрага, званична истрага*

ВОВЕД

1. Компјутерски криминал

Дигиталната ера се карактеризира со примена на компјутерско-комуникациската технологија како алатка за подобрување на традиционалните човечки активности. Со искористување на компјутерските системи во приватните, комерцијалните, едукациските, државните и останатите аспекти на модерниот живот, во голема мерка се подобрува и квалитетот на животот. Компјутерот ги прави човечките активности побрзи, поедноставни и поинтересни, Со негова помош се креираат нови модели на работните и останатите активности кои луѓето ги превземаат. Последиците на таквата состојба е континуирано генерирање нови идеи како и зголемување на бројот на можностите кои му се нудаат на на современиот човек. Меѓутоа, покрај добрите страни кои компјутерот ги донесе, постои и една темна страна која нуди можности за нанесување штети во општеството. Користењето на компјутерските системи нуди осет на анонимност, сигурност, а со тоа и намалување на можностите за откривање на неговите корисници. Овој последен факт може додатно да се потврди ако кажеме дека поголемиот број на компјутерски системи се и мрежни системи, односно се приклучени на некоја мрежа каде речиси е невозможно да се открие неговиот корисник. Со други зборови компјутерскиот систем иницира појава, изведување и усовршување на криминални дејанија.

2. Обезбедување на докази и Форензика на компјутерски криминал

2.1 Форензика на компјутерски криминал

2.1.1 Основни поими

Компјутерска форензика, или поточно кажано компјутерска форензичка наука, претставува спој на технологија и наука која се обидува да утврди на кој начин компјутерскиот систем учествуваат во одредено криминално дејство. Науката во компјутерската форензика ги опфаќа познавањето на методите и процедурите кои се применуваат при анализата и собирање на податоците (доказите). Технологијата претставува множество од различни алатки кои овозможуваат примена на методите и процедурите кои се предмет на научната страна на форензитиката.

Најсеопфатната дефиниција на поимот компјутерска форензика авторите на овој труд сметаат дека е:

„Компјутерска форензика е постапка на собирање и анализа на податоци на начин со кој не се влијае на нивната оригиналност или уништување, што е можно повеќе во насока на реконструкција на податоците или случките кои се случиле во минатото на некој компјутерски систем“ [1].

Компјутерски безбеден инцидент претставува користење на компјутерски или мрежни системи за различни нелегални, неприфатливи или неавторизирани активности [2]. Како случки за кои се сметаат дека причинуват повреди на компјутерската безбедност можат да се наведат следните:

- Неавторизиран пристап до компјутерските системи, со користење на различни видови модуси и облици на напад на компјутерскиот систем.
- *DoS (*Denial of Service*)* напади
- Испраќање на несакани електронски пошти *(*email spam*)*

- Било која незаконска активност која користи компјутерски систем.

2.1.2 Процедури за анализа на електронски криминал

Постапките во рамките на форензичката анализа можат да се поделат спрема работната состојба во која се наоѓа нападнатиот компјутерски систем. Секој систем има две основни состојби, вклучен систем (online) или исклучен (offline). Вклучен систем претставува состојба во која компјутерскиот систем е во работна состојба, односно извршува некоја задача.
Исклучен систем претставува состојба во која системот мирува, не извршува никаква задача, односно е исклучен од напонското напојување. Значи, форензичката анализа се дели на online и offline, односно на таканаречена live и post-mortem анализа. Таа се состои од идентификирање, издвојување и документирање на дигитални докази [4].

2.1.2.1 Анализа на компјутерскиот систем во работна состојба (live анализа)

Live анализа претставува анализа на компјутерскиот систем кога тој се наоѓа во работна состојба. Постапките при ваквиот тип на анализа овозможуваат проноаѓање на докази кои единствено егзистираат кога системот е во работна состојба. Во процесот на Live анализата се прави: Преглед на состојбата на процесите, преглед на отворените мрежни врски, на содржината на работната меморија, на содржината на цврстите дискови и слично. Целта на анализата е да се соберат докази кои потврдуваат дека инцидентот се случил, да се утврди распонот на нападот и да се донесе одлука дали е потребно да се направи offline анализа. Мнугу често live анализата претставува единствениот начин да се анализира системот. За тоа можат да постојат повеќе причини, а најчеста е таа што системот кој се анализира извршува важна функција поради што не смее да биде во offline состојба (сервер од кој зависи работата на институцијата) или пак со исклучувањето може битно да се промени неговата состојба, особено ако напаѓачот оставил замка која ќе ги избрише сите докази со исклучување на системот. Во тој случај податоците мораат грижливо и темелно да се соберат, бидејќи тие претставуваат единствен извор на докази. Овој начин на анализа е екстремно осетлив и бара сите форензички анализи пажливо да се селектираат и изведат бидејќи неповратно можат да ја променат неговата состојба. Во таа насока потребно е да се минимизира бројот на операциите кои се изведуваат, со цел нивното влијани на неговата состојба да биде што помало. Од друга страна мора да се внимава бројот на операции да биде доволен во насока на собирање задоволителна количина на информации која ќе биде во состојба да ја расветли почетната состојба на компјутерскиот систем [3].

Анализата на системот во работна состојба бара селекција на соодветни алатки со кои ќе се изведе анализата и селекција на соодветен начин на складирање на собраните податоци. Важно е да се спомни дека алатките претставуваат независни програми кои се изведуваат внатре во оперативниот систем. Во компромитираниот компјутер можат да постојат програми за ваква анализа, но не смееме да ги користиме бидејќи нивното потекло не е проверено или пак уште полошо напаѓачот дека може да подметне вакви програми со цел да ја одведе истрагата во погрешна насока и да ги прикрие доказите. Овие програми мораат да бидат статични, односно не смеат да ги користат библиотеките на компромитираниот компјутер од истите причини. Избраните алатки мораат да бидат сместени на некој независен преносен медиум. Видот на алатката зависи од оперативниот систем користен на компромитираниот компјутерски систем.

2.1.3 Видови на анализа на електронски криминал

Генерално, дигиталната форензичка истрага се дели на две основни категории [5]:

- Корпорациска (приватна) дигитална форензичка истрага
- Званична (јавна) дигитална форензична истрага.

Званичната (јавна) дигитална форензичка истрага ја изведуваат званичните истражни органи (полициските истражни органи, специјалното обвинителство и специјалното судство за борба против високотехнолошкиот криминал). Овие органи потребно е да работат во склад со позитивната законска легислатива, но и да ги почитуваат светските стандардни оперативни процедури за истражување, привремено одземање и испитување на компјутерските системи и другите мрежни уреди, аквизиција на дигиталните податоци/докази независно од оперативната платформа во насока на откривање на валидни дигитални докази. Тоа подразбира дека истражните органи мораат добро да ги познаваат постоечките закони и прописи кои се однесуваат на компјутерскиот криминал, но и добро познавање на стандардните локални процедури за истражување и утврдување на криминалните активности во областа на компјутерскиот криминал.

Во процесот на утврдување на карактерот на криминалното дејство, истражниот орган мора да одговори на многубројни прашања, како што се:

- Со кое средство е извршено кривичното дејание?
- Преку кои копјутерски системи, односно компјутерска мрежа е извршено криминалното дејство?

- Дали е во прашање извршена кражба, провала вандализам или тероризам во компромитираниот компјутерски систем?
- Дали напаѓачот загрозил нечија приватност и други права или некого вознемирувал?

2.1.4 Дигитални докази

Дигиталниот компјутерски доказ се состои од множество на посредни реални докази, од кои ниеден не смее да се исклучи поради било која причина. Доказите мораат да бидат потполни, меѓусебно да се потполнуваат (да се испреплетени) и да ја немаат таканаречената пукнатина за донесување на заклучок, односно за утврдување на цврст доказ.

Криминалниот акт може да се изврши на било кој компјутер поврзан во локална или светска мрежа независно од неговата географска положба. Исто така компјутерот-напаѓач географски може да биде лоциран во било која точка од земјината топка. Парот нападнат компјутер – напаѓачки компјутер може да биде во границите на една држави или пак да бидат сместени во различни држави. Тоа значи дека тие можат да бидат сместени во иста држава или во различни држави, односно форензичарите често се приморани собираат дигитални докази во едни држави, а да ги прикажуваат на суд во други држави. Самиот тој факт налага да се воведат одредени правила за прибавување, дистрибуција и презентација на дигитални докази кои ќе се релевантни за сите држави. Во таа насока, IOCE ги дефинира општите принципи за хармонизација на методите и праксата при работата со дигитални докази меѓу народите кои гарантираат прифатливост на дигиталните докази во една земја, ако тие се собрани во друга земја.

Светската судска практика ги прифаќа компјутерски генерираните и компјутерски меморираните докази под соодветно дефинирани услови. Овие услови мораат строго да се почитуваат, бидејќи трансформацијата на податоците од серија на кодирани битови во судски доказ е апстрактен процес кој може да предизвика сомнежи кај судиите и поротата и да ги доведе во прашање автентичноста и интегритетот на компјутерски генерираните судски докази. Тоа особено е изразено кај судиите/поротата кои се неедуцирани од областа на информатичко-комуникациската технологија. Затоа, потребно е да постојат процедури за ракување и чување, како и прописи за собирање, аквизиција и и анализа на дигиталните докази независно на каков медиум тие се запишани. Не смее податоците да се менуваат, да се оштетуваат или да се манипулира со нив во било кој чекор од истрагата [8].

Собирањето на докази започнува со реконструкција на хипотезата за случајот. Доказите треба да се собираат на местото на случување на криминалната случка (*на сцената на злочинот*), бидејќи тоа може да биде единствен директен контакт со реалните докази. Треба да се работи методично, полека и да се собираат клучните нешта. Користејќи ги заклучоците за случката, потребно е со критички поглед да се вратиме на поставената хипотеза, односно да си поставиме прашање како лично ние би ги прифатиле тие докази ако се наоѓаме на спротивната страна. Потребно е да ги пронајдеме причините за неквалитетниот доказ, односно да утврдиме: зошто доказот не е квалитетен, каде се изгубил некој важен факт, како да се пронајде доказен материјал кој ќе ја потпони празнината, што да направиме ако таков материјал се пронајде, итн. Во оваа фаза од истрагата од иста важност се докажувањето и негирањето на доказот. Заедничка одбрана во сите компјутерски ексцесни ситуации најчесто е тезата дека криминалниот акт никогаш не се случил, дека тоа е само нормална компјутерска аномалија итн.

Значи, потребно е да се соберат сите посредни докази од лице место, не само оние докази за кои дигиталните форензетичари мислат дека треба да се соберат, туку и се` она што може потенцијално да индицира што навистина се случило. Во процесот на аквизиција генерално е потребно да се снимаат листата на датотеки и логови како докази, дури и ако немаме никаква идеа што навистина се случило. Треба да се има во доказниот материјал секоја датотека која потенцијално може да содржи доказ, пред истата да се изгуби или промени. После иницијалната истрага (без запленување на компјутерот) потребно е да се свртиме кон првобитната хипотеза и да ја доградиме подетално со собраните докази. Голема веројатност постои да е испуштен некој значаен доказ, што претставува добар аргумент компјутерот да се заплени во текот на истрагата, но при тоа мораме да имаме на ум дека тоа не е секогаш лесно. Дигиталниот доказ е посреден доказ. Но, секој од посредните докази, кои заедно го градат доказниот материјал, треба да се третира како директен доказ кој води кон непобитно доказување на криминалното дејание. Сите посредни докази потребно е да се третираат како докази кои директно водат кон непобитно докажување на извршените криминални активности. Тие се сите важни и критички за конкретниот случај. Дури во тој случај почнува изградбата на доказ без пукнатини, односно изградбата на необорив доказ. Значи, потребен е голем посреден доказен материјал, за да се изгради еден мал цврст дигитален доказ.

2.1.5 Алатки за анализа на електронски криминал

Алатки кои се користат за анализа на веќе направениот електронски криминал би ги поделиле во два дела и тоа:

1. Алатки за анализа на компримитираниот компјутерски систем во живо,
   a. DEFT, Linux базирани сет на алатки компајлирани на CD,
   b. HELIX, Linux базирани сет на алатки,
   c. COFEE, Microsoft life forensic алатка за обезбедување на податоци/докази од вклучен компјутер
   d. FTK, software за правење на image (bit to bit copy) на RAM меморија или целиот file system на хард дискот.
2. Алатки/ софтвер за анализа на компјутер во лабараторија
   a. En Case, software за креирање на image и детална анализа на file system на хард дискот.
   b. FTK, софтвер за детална анализа на image file,
   c. X-way, софтвер за детална анализа на секој бит на хард диск.

2.2 Корпорациска истрага на електронски криминален инцидент

Корпурациската истрага претставува истрага која се спроведува во рамките на организацијата (корпорацијата) во која се случил компјутерскиот криминален инцидент. Започнува од моментот кога инцидентот е откриен. Таа се изведува со специјалисти од организацијата и према интерните правилата и процедурите кои се предвидени за вакви инциденти [9].

Во моментот кога се случува компјутерски инцидент најкритична е брзината на реакцијата. Во почетната пракса на форензичката истрага на компјутерските докази се покажало дека податоците откриени во текот на првите седум дена се критични за откривање на причинителот, односно за успешно заздравување на системот. Денес овој период е многу пократок. Се мери во часови.

Према праксата која се применува во FBI (САД) предистражната постапка се изведува во следните три фази:

- Покренување на истрага
- Одредување дали инцидентот претставува компјутерски криминал
- Анализа на доказите.

Првата фаза *покренување на истрага* опфаќа: обезбедување на местото на инцидентот, аквизиција на доказите, изработка на хипотеза за упадот и истражување на алтернативни објаснувања.

Втората фаза *одредување на карактерот на инцидентот* опфаќа: анализа на инцидентот, анализа на доказите собрани во првата фаза со алтернативни објаснувања, во насока на одредување дали инцидентот е криминален или е природна случка.

Третата фаза *анализа на доказите* опфаќа: анализа на доказите, припрема на презентацијата на инцидентот и наодите на органите на истрагата.

Процедурите кои се користат во текот на истрагата на компјутерскиот инцидент генерално ги содржат следните постапки:

- Проверка на евиденцијата, лог датотеката, како и останатите информации за сомнителните.
- Испитување на информантите (лицата од кои можат да се добијат било какви информации)
- Контрола на сите фази од истрагата
- Припрема на органите за пребарување (лоцирање на компримитираниот компјутер)
- Претрес на ресурсите на сомнителните
- Прибирање и анализа на доказите.

Главно тежиште на званичната корпорациска истрага секогаш се насочува на сведоците и сомнителните.

Најдобра комбинација во истрагата на компјутерскиот инцидент е заедничка тимска работа на званичните органи на истрагата одредени од страна на сопственикот на информацискиот систем и ИТ специјалисти. Не постои супервезда во истрагата. Секој учесник има своја задача соодветно на својата специјализација и своето знаење.

Генерално истражната постапка на корпорациско ниво се изведува со користење на моделот „чекор по чекор“ [5], [6]. Овој модел ги содржи следните чекори:

1. Иницијална истрага
2. Влез во трагата на напаѓачот
3. Откривање на инцидентот на напаѓачот
4. Апсење.

За приватниот сектор и за истрагата на корпорациско ниво клучни се првите три чекори.

Успехот на истрагата да биде успешен потребно е да се превземат следните шест поставени цели (*Rosenblatt*-ови цели):

1. Елиминирање на очигледните факти (факти кои сигурно не можеле да се случат).
2. Поставување на хипотеза за нападот
3. Реконструкција на криминалниот акт.
4. Откривање на траг до криминалниот компјутер од кој нападот е извршен
5. Анализа на изворните (нападнатите), целните (од кои нападот е извршен) и посредните (врски меѓу нападнатите и напаѓачките) компјутери.
6. Собирање на докази, ако е можно и од компјутерот од каде е извршен нападот.

Кон спомантите цели, во насока на поуспешно решавање на проблемот, може да се додаде и:

7. Предавање на доказниот материјал на истражните корпорациски органи или на званичните истражни органи за понатамошна постапка.

Истрагата започнува со утврдување дали постои компјутерски криминален инцидент или инцидентот настанал по природен пат.

Следниот чекор е *елиминирање на факти*, кои очигледно не можат да се случат во компјутерскиот инцидент во IKT системот (пр. Ако компјутерскиот систем не е поврзан со надворешна мрежа, тогаш се елиминира надворешен напад и се утврдува дека нападот е од внатре, односно од некој компјутер од локалната мрежа).

Потоа се анализираат патиштата од локалната мрежа кои водат кон нападнатиот компјутер, во насока на елиминирање на компјутерите од кои не бил возможен напад (пр. Компјутерите кои биле во тој момент исклучени од напонската мрежа, во просторијата немало никој, ...). Ако не се стесни векторот на можните напади, особено при мрежи со голем број компјутери, тогаш можностите да се открие напаѓачот во голема мерка се намалуваат.

Следниот чекор е анализа на човечкиот фактор, односно да се провери кој од персоналот, кој има пристап до мрежата, се исклучува од сомнителните (пр. бил во планина каде нема компјутерска мрежа, телефон, струја,...).

Се водат преелиминарни разговори со секој кој на било кој начин е поврзан со нападнатиот компјутер.

За водење на преелиминарни одговори е потребно:

- Да се соберат информации за опкружувањето на (мрежно, периферни уреди, просторно, луѓе, ...).
- Да се соберат детални информации за инцидентот од аспект на жртвата во нападот.
- Да се соберат докази за инцидентот директно од нападнатиот компјутер.
- Да се утврдат трагите и да се документира проценетата во парични единици.

Со процесот на стварање на хипотеза како нападот се случил, се обидуваме да го објасниме нападот, односно како напаѓачот влегол во системот.

Потребно е теоретски да го анализираме нападот со мапирање на сите можни вектори на напад (сите можни патишта кон компјутерот жртва), да ги анализираме контролните пристапи и лог датотеката на компјутерот жртва. Овие активности потребно е да ги изведуваме на исти тип на компјутер, со исти оперативен систем како нападнатиот.

Следниот чекор од изработката на хипотезата е тестирање на хипотетичките патишта (рутови) и ACL (контролните листи на пристап до нападнатиот компјутер) на сите корисници и суперкорисници кои имаат право на пристап со цел да се утврди дали некој од нив е потенцијален напаѓач. Се одредува точното време, дата и условите во кои се одвивал нападот.

Битно е да се потенцира дека во оваа фаза нападнатиот компјутер не смее да се вклучува или исклучува ако е вклучен, бидејќи не е препорачливо да се прават било какви промени во нападнатиот компјутер, особено ако тој користи *Microsoft* OS. Овие мерки се потребни, да се спречи уништувањето на можните докази кои постојат на цврстиот диск со предходно поставена замка.

Обавезна активност во оваа фаза е физичкото исклучување на нападнатиот компјутер од мрежата, во насока на спречување на повторен напад поради бришење на трагите и доказите.

Компјутерскиот криминал, за разлика од класичниот (убиство, кражба, ...), може да се реконструира со тестирање на створената хипотеза за нападот. Со реконструкцијата можеме да го откриеме патот по кој напаѓачот му пристапил на компјутерот.

Реконструкцијата се врши на форензички тест компјутер кој е од ист производител, ист модел со исти карактеристики. Тест компјутерот треба да се конфигурира колку е поможно поблиску до вистинската конфигурација на нападнатиот компјутер (се мисли на интерната конфигурација, логирањето, мрежните врски) во моментот на нападот. Ако нападнатиот компјутер е персонален компјутер, тестниот компјутер можеме да го бутираме од покретен медиум за DOS без *Windows*, со цел да се добие физичката слика на цврстиот диск со користење на соодветна програма каква е на пример *SafeBack (Sydex)*. Потоа физичката слика на цврстиот диск се реставрира на форензичкиот тестен компјутер со што се добива точна огледална (*miror)* слика на нападнатиот компјутер. Ако на тестниот компјутер се добијат исти резултати какви имал напаѓачот, тогаш почнува процесот на осознавањето како компјутерот жртва е нападнат. Тоа сознание не мора да не води кон напаѓачот, но сигурно ја намалува листата на сомнителни.

Реконструкцијата трага до сомнителниот компјутер од кој нападот е извршен. Поголемиот број на компјутерски криминалци се многу вешти, ретко прават грешки и паѓаат во замки. Но и тоа се случува. Секоја нивна грешка им ја олеснува работата на истражните органи. Затоа барањето на логички грешки е главниот вовед во откривање на трагата на напаѓачот.

Самиот компјутер остава трагови во многу пристапни, но и во непристапни зони на цврстиот диск. Компјутерските специјалисти ги знаат тие зони каде остануваат трагови. Тие зони не се секогаш сите познати и пристапни и за највештите хакери. Особено ако тие зони ги дефинирал IT специјалистот како превентивна мерка за полесно откривање на влезот и движење на напаѓачот во нападнатиот компјутерски систем.

Специјалистите, за соодветниот тип на компјутери каков што е нападнатиот, се во предност бидејќи го познаваат во детали функционирањето на оперативниот систем, хардверот, интерфејсот хардвер-софтвер-оперативен систем, го познаваат функционирањето на комуникациите во и надвор од компјутерот и филозофијата на функционирањето на хакерите, па затоа можат да постават замки и за највештите напаѓачи.

Секој компјутерски напаѓач има свои белези по кои може да се препознае. Чак и малициозните програми (пр. вирусите) кои програмерот ги напишал, можат да содржат индиции за неговиот идентитет. Не е редок случај кога хакерот, благодарение на својата суета, остава некаков белег за да ги одбележи своите програми. Вештината на аналитичарот е да ги открие тие белези.

Треба секогаш да се има на ум дека компјутерите се екстремно конзистентни и предвидливи во начинот на процесирање (обработка) на податоците. Ако компјутерот се владее невообичаено, тогаш постојат две причини:

- Аналитичарот не разбира како компјутерот се владее (функционира)
- Постои измена на стандардната програма.

Таа карактеристика е од голема помош за аналитичарот во текот на истражната постапка.

Пример: Да претпоставиме дека вршиме анализа на компјутерот кога изведува некоја апликација за процесирање на податоци. Процесирањето се изведува нормално на сите нивоа, освен во некои точки. Задачата на аналитичарот е, во соработката со систем програмерот, да ги пронајде причините за логичките грешки кои се откриени во истрагата, дали тие некоректности во заклучокот на истрагата се резултат на непознавање на работата на апликацијата од страна на аналитичарот или има измени во апликацијата.

Ако постои аномалија поради која доаѓа до пад на апликацијата, таа може да биде случајна или криминална. За да се открие нејзината природа мора да се анализира содржината на лог датотеката за периодот во кој претпоставуваме дека е направен криминал. Лог датотеката индицира преконфигурација на податоците, но програмските измени можат да бидат индицирани но и да останата нерегистрирани (измените во содржината на лог датотеката кои се направени програмски од страна на напаѓачот).

Пример: Напаѓачот влегол во нападнатиот компјутер. Ја вршел активноста за која и влегол во компјутерот. Но, на крајот го изменил времето на логирање во лог датотеката. Форензичарот воочил дека напаѓачот го посетил компјутерот, но бидејќи времето на настанатите криминални активности и времето на логирањето на напаѓачот се разликувале, иако се знаело дека тој го извршил делото бил ослободен бидејќи истрагата не можела да докаже дека тој го изменил времето на неговото логирање. Во таков случај доказот мора да се изведе со помош на други посредни докази.

Истрагата на компјутерскиот криминал не е само од техничка природа, но сепак нејзиниот технички аспект е доминантен и мора да има смисла. Игнорирањето на било која негова аномалија може да доведе до изведување на погрешни заклучоци.

Ако трагот води надвор од ИКТ системот на кој припаѓа нападнатиот компјутер, тогаш форензичарот мора да го реконструира трагот на Интернет.

Во овој чекор од истрагата форензичарот мора да се обиде да:

- Свати како напаѓачот влегол во информативниот систем.
- Собере потребни квалитетни информации кои ќе ги оправдаат мерките на поставување на замки и на навлегување во трагата на напаѓачот.
- Добие што повеќе докази за напаѓачот.
- Добие информации кои ќе ја стеснат листата на сомнители и ќе потврдат дека напаѓачот е интерен или надворешен.
- Собере доволно квалитетни информации со чија помош ќе донесе одлука да се обрати за помош до званичните органи за истрага.

Искусниот напаѓач никогаш не напаѓа директно од својот компјутер, туку користи посреден компјутер од други организации и од други мрежи. Тој поставува замка во компјутерот-посредник (*trap door- задна врата*) и користи наредби или програми од тој компјутер за да достаса до копјутерот-жртва. Географската одалеченост напаѓач-посредник-нападната компјутер воопшто не е важна.За да ја сокрие трагата напаѓачот (особено оние повештите) ја менуваат содржината кај сите компјутери кои се вмешани во нападот (напаѓачкиот, посредникот и нападнатиот).

Слична тактика може да примени и внатрешен напаѓач. За да ја измами истрагата може да нападне преку некој посредник кој се наоѓа на оддалечена локација.

Реконструкција на траговите на нападот подразбираат да се „знакови на или поред секој пат преку кој помионал напаѓачот“, односно логови за секој влез во серверот, рутерот, телефонската централа.

Во текот на реконструкцијата моѓе да се наиде на следните проблеми:

- Не постојат логови за временскиот период на нападот.
- Да се добијат несоодветни логови за периодот на нападот.
- Променети/избришани логови за периодот кога нападот е извршен.
- Испрекинати престои помеѓу изворот на нападот и компјутерот жртва, со што се маскира патеката на нападот.
- Администраторите на посредните компјутерски системи не се вољни за соработка.
- Лажни IP адреси (*spoofing* adresa).
- Директен конзолен пристап до нападнатиот компјутер прикривен со измена на содржината на лог датотеката.
- Маскирање на трагите од нападот со измена на содржината на лог датотеката.

Потрагата во нападнатиот компјутер најмногу зависи од лог датотеката. Ако во нападот се

вклучени повеќе компјутери, потребно е да се споредат лог датотеките од сите замешани компјутери. Основен проблем во тие активности е ако постојат намерни измени во нивните содржини, кои можат да предизвикаат погрешни заклучоци. Овој проблем особено се усложнува бидејќи тие промени можат да ги предизвикаат од невнимание или незнаење и форензичарите, односно другите субјекти кои доаѓаат во допир со споменатите компјутери. Затоа најдобро секогаш на лог датотеките да се прават две копии, едната да служи за реконструкција на настанот, а другата за доказ во судската парница.

Генерални проблеми при извршување на корпорациска истрага:

- Најчесто организациите немаат припремен план, ниту органи за истрага.
- Не можат да истражуваат надвор од својата организација.
- Мораат да водат сметка за угледот на фирмата, па затоа често не се обраќаат до званичните органи на истрага, ниту пак објавуваат информации за настанот.

2.3 Пример за корпорациска истрага за електронски криминален инцидент

Примерот за корпорациска истрага кој го избравме за анализа се однесува на истрага за промена на податоци во базата на податоци на системот на корпорацијата. Во овој пример се работи за банка која има над 500 вработени и во рамките на централниот менаџмент има одделение за Информатичка поддршка кое покрај основната функција за одржување на системот на банката и грижата за безбедноста на системот, има капацитети за мониторирање и истрагана инциденти или злоупотреби на системот.

Имено, при редовна месечна анализа на резултатите од работењето воочена е трансакција на 1 (еден) милион евра за кои нема потврда за причината на трансакцијата, но средствата се префрлени на банкарска сметка на друга банка во друга држава. Менаџментот на банката дефинира тим кој ќе истражува кој на има направено трансакцијата и на кој начин, сомневањата на почетокот се дека е можен влез во системот од надвор. Со цел истражување на злоупотребата или неовластеното користење на системот превземени се следните мерки:

1. Одредување на точно време на одобрување на трансакцијата,
2. Одредување на клиентот/ компјутерот од кој е направено одобрувањето
3. Анализа на сите процеси на компјутерот,
4. Анализа на event логови на компјутерот,
5. Анализа на моменталната и минатата комуникација на компјутерот,
6. Анализа на компјутерот, со цел да се види дали постои некој malware code во компјутерот,
7. Анализа на безбедносните логови на системот
8. Анализа на апликациските логови
9. Анализа на event логовите на системот
10. Анализа на моменталните сетирања на firewall и безбедносните параметри кои се поставени на системот.

Од резулатите од предходните анализи и проверки укажуваат дека ситемот е комплетно безбеден, сите непотребни порти се затворени, од безбедносните логови и од другите анализи се гледа дека нема обиди и нема успешни логирања со default account и нема логирања на системот со не domain корисници. Исто така од логовите на компјутерот заклучено е дека на истиот е користен регистриран domain. Од анализата конечно е воочено дека domain корисникот А кој има привелегии за одобрување на трансакции и кој ја има одобрена трансакцијата е логиран на анализираниот компјутер на службеникот Б кој со својот domain корисник нема привелегии за одобрување на ваков вид на трансакции. Исто така во разговор со двајцата службеници потврдено е дека службеникот А не бил на работа во периодот кога е одобрена трансакцијата.
Од анализата на сите електронски докази и разговори со службениците, утврдено е дека службеникот Б ги има злоупотребено корисничките привелегии кои ги имал службеникот А и во негово отсуство ја одобрил трансакцијата од својот компјутер.

3. Заклучок

Брза реакција, уште при првите индикации дека нешто нелегално се случува со нашиот компјутерски систем, е императив. Таа е неопходно од повеќе причини: Да се спречи нанесување штети од било која природа, да се намалат штетите ако веќе се нанесени и да се донесе одлука дали корпорацијата е сама способна да го реши проблемот, ако не е способна дали да повика истрага на званични органи или пак да го премолчи инцидентот бидејќи тој може да го компромитира угледот на корпорацијата. Брза реакција е можна единствено ако таа има екипа на специјалисти кои се способни да спроведат почетна истрага. Токму тоа е и целта на овој труд, да ги потсети компаниите дека, при денешниот развој на криминалот преку електронските комуникациски уреди, мораат да имаат екипа од специјализирани луѓе кои се способни да извршат истрага веднаш по индикацијата дека нешто незаконски се случува во рамките на нивните информациски системи.

4. Библиографија

[1] Farmer, Venema, " Forensic Discovery": The spirit of forensic discovery, Addison-Wesley, 2003
[2] K. Mandia, C. Prosise, M. Pepe, " Incident Response and Computer Forensics": , McGraw-Hill.

[3] K. Mandia, C. Prosise, M. Pepe, " Incident Response and Computer Forensics": Investigating Windows Systems, McGraw-Hill, 2003
[4] J. Philip Craiger, " Handbook of information security": Computer forensics procedures and methods, Wiley, 2006
[5] Bruce J. Nikkel, The Role of Digital Forensics within a Corporate Organization, BSA Conference, Vienna, May 2006.
[6] http://www.ncjrs.org, *Electronic Crime Scene Investigationon: A Guide for First Responders*, 2001.
[7] Icove D., Segar K., VonStorch W., *Computer Crime, A Crimefighter's Handbook,* O'Reilly & Associates, 2004.
[8] Australian Communications, *Electronic Security Instruction 33,* ACSI 33 Standard, 2002.
[9] Р. Христов „Детективска информатика“, ЕУРМ, 2010