УНИВЕРСИТЕТ ПО БИБЛИОТЕКОЗНАНИЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

КАТЕДРА „НАЦИОНАЛНА СИГУРНОСТ“
СПЕЦИАЛНОСТ „ИНФОРМАЦИОННА СИГУРНОСТ“

ДИПЛОМНА РАБОТА

на тема:

МЕТОДИ ЗА КОМПЛЕКСНА ЗАЩИТА НА ИНФОРМАЦИЯТА

Дипломант:
Пенчо Минков Василев
задочно обучение
Ф. №: 155-СЗ

Научен ръководител:
(проф. д. т. н. Атанас Начев)

София
2018

РЕЗЮМЕ

Василев, П. Методи за комплексна защита на информацията. Научен ръководител проф. д. т. н. Атанас Начев. С. 2018. Катедра „Национална сигурност“. Факултет „Информационни науки“. УНИБИТ. 86 стр. Брой източници – 16.

Цели на дипломната работа са: да бъдат описани и анализирани различните начини за нерегламентиран достъп до информация, както и да бъдат разгледани различни методи и направления за защита на информацията и информационните системи.

В първа глава са описани основните методи за нерегламентиран достъп до некомпютърно обработвана информация с използване на технически средства и е направен анализ на тяхното действие и употреба.

Във втора глава са описани методите за неоторизиран достъп до компютърно обработвана информация, като е обърнато внимание и на социалния инженеринг като средство за достъп до чувствителни данни.

В третата глава са разгледани различни методи за защита, разделени в 18 направления, като е обърнато внимание и на възможностите, които предоставя оценката и управлението на риска и са разгледани и системите за откриване и предотвратяване на атаки.

Ключови думи: достъпност, заплаха, защита, информационна сигурност, информация, конфиденциалност, сигурност, уязвимост, цялостност.

СЪДЪРЖАНИЕ

УВОД

Още от втората половина на XX век информацията започва да придобива значение, което далеч надхвърля дотогавашната ѝ същност. Това особено важи в наши дни, когато тя се възприема като жизненоважен актив за всяка организация, била тя от държавния или от частния сектор, което обуславя и необходимостта от нейната адекватна защита и опазване. Осигуряването на информационната сигурност започва още на най-ранен етап – от проектирането и създаването на една информационна система, като тук става въпрос за информацията във всичките ѝ форми и проявления: на хартиен, цифров или друг носител; предавана устно, електронно или по друг комуникационен канал; събирана, съхранявана, обработвана, разпространявана и унищожавана за нуждите на съответната организация. Загубата или липсата на информация може да доведе както до финансови, материални и/или човешки загуби, така и до загуба на имидж и репутация, което, в някои случаи, може да е много по-неблагоприятно.

Защитата на информацията се осъществява основно в три направления – конфиденциалност, цялостност и достъпност – като всяко едно от тях има своя роля в комплексното ѝ изграждане и осъществяване:

- *Конфиденциалност.* Управлява достъпа до информацията (нейната поверителност, тайна) – недопускането на достъп до информацията от потребител, процес или нарушител, който не е определен да има такъв.
- *Цялостност.* Защитата по това направление се изразява в осигуряването и гарантирането на това, че информацията не е компрометирана – неправомерно (предумишлено или по случайност) променена или изтрита.
- *Достъпност.* Гарантира, че информацията ще е достъпна в необходимия обем, по всяко време и от всеки, който има право на това.

Постигането на тези три цели до известна степен е процес на компромиси между тях. Например: прекалено лесната достъпност увеличава вероятността от нарушаване на конфиденциалността и/или цялостността; налагането на „тотална“ конфиденциалност би довела до затруднения в достъпността и т. н. Затова, в зависимост от конкретната ситуация и нужди, се търси необходимия баланс между тях.

Всяка информационна система притежава обекти и субекти. Обектите са файлове, директории и т. н., докато субектите са потребители, процеси и програми. След като обектите и субектите са идентифицирани трябва да има един набор от правила (политика за сигурност), съгласно който системата да определя кога даден субект може да получи достъп до определен обект. Изпълнението на тези правила се осъществява посредством различни методи и способи, работещи като единно цяло за осигуряване сигурността на информационната система. Нещата, които могат да окажат негативно влияние на работата на системата се обобщават до:

- *Уязвимости.* Слабости (пропуски, грешки, дефекти) на информационната система и/или защитните ѝ механизми, които при случайно или предумишлено използване могат да доведат до нарушаване на конфиденциалността, цялостността и/или достъпността на информационните обекти или до нарушаване работата на субектите.
- *Заплахи.* Това са всички възможни опасности за информационната система и нейните ресурси, които могат да произтекат от дадена личност, предмет или събитие.

Уязвимостите могат да са: физически; природни; софтуерни и хардуерни; медийни (на носители на информация); комуникационни; експлоатационни и т. н. Заплахите могат да се класифицират в две основни групи: случайни (неволни) и преднамерени (умишлени). Пробив (инцидент) в информационната сигурност има, когато дадена заплаха „съумее да се

възползва“ от една или повече уязвимости, като по този начин доведе до загуба на конфиденциалност, цялостност и/или достъпност на определен информационен ресурс. Основна задача при защитата на информацията е предотвратяване на инцидентите, като се ограничават и опознават заплахите и се премахват уязвимостите.

Предвид казаното дотук, може да се обобщи, че:

- ***Целта*** на защитата на информацията е осигуряването и гарантирането на нейната конфиденциалност, цялостност и достъпност.
- ***Задачите*** при осигуряването на защитата на информацията са идентифициране и ограничаване на заплахите и откриване и премахване на уязвимостите на информационната система.
- ***Методите*** за постигането на целта и изпълнението на задачите могат да са: технически; програмни; програмно-технически; физически; организационни и др.

ГЛАВА I: АНАЛИЗ НА СПОСОБИТЕ И МЕТОДИТЕ ЗА ДОБИВАНЕ НА ИНФОРМАЦИЯ

Способите и методите за неоторизиран достъп до информация са изключително разнообразни по своята същност и приложение. Затова, при разглеждането им, ще ги разделя на две големи групи:

- методи и способи за добиване на информация, която не се обработва компютърно; и
- методи и способи за добиване на компютърно обработвана информация (които ще бъдат разгледани във втора глава на настоящата дипломна работа).

Един от основните видове некомпютърно обработвана информация, която често се превръща в обект на нерегламентиран достъп, е акустично предаваната информация. Носител на тази информация са акустичните вълни, които могат да се разпространяват както във въздушна, така и в твърда и течна среда. Това означава, че при разпространението си, акустичните колебания могат да бъдат регистрирани от трети лица и така да бъде получен достъп до провеждани разговори, било то на открито или в затворени помещения.

На база методите за достъп до акустичните (звуковите) колебания, предизвиквани от акустичните вълни, могат да се специфицират следните акустични канали за неоторизиран достъп:

- въздушни канали – образуват се при разпространението на акустични вълни във въздушна среда;
- структурни канали – образуват се при разпространение на акустични вълни в конструктивните елементи на сградите, като стени, врати, тръби на различни инсталации и др.;

- електроакустични канали – образуват се при преобразуване на акустични сигнали в електрически (например, при микрофонен ефект, предизвикан в електронни устройства);

- оптикоелектронни канали – образуват се, когато вибриращи под въздействието на акустични вълни обекти биват облъчвани с кохерентни електромагнитни вълни от видимия или инфрачервения спектър и същите, след отразяване, биват уловени обратно. При демодулацията на отразените електромагнитни вълни могат да се отделят честотите на акустичните вълни;

- параметрични канали – образуват се при въздействието на акустични вълни върху електронни средства, генериращи високочестотни сигнали.

Следва разглеждане на някои от най-популярните методи за достъп до некомпютърно обработвана информация с помощта на технически средства, като при анализа им предимствата и недостатъците ще бъдат разглеждани от гледна точка на нарушителя.

1.1. Неоторизиран достъп до акустична информация с използване на подслушващи устройства.

В основата на този метод стои залагането и използването на скрит микрофон в помещението, който улавя и предава акустичната информация към нарушителя. Честотната лента на звука е от 20 Hz до 20 kHz, но за нуждите за прихващане на речева информация е достатъчно микрофонът да е чувствителен към диапазона от 70 Hz до 7 kHz, а ако няма изисквания за улавяне на спецификите на тембъра и емоциите в гласа на говорещите е достатъчно от 200 Hz до 5 kHz. Обикновено се използват електродинамични, кондензаторни или пиезокерамични микрофони, които имат обхват с радиус до 10÷15 m и чувствителност към честоти от 100 Hz до 5÷20 kHz.

Тъй като методите за отвеждане на информацията от микрофона до нарушителя са много разнообразни и разнородни, ще разгледам най-често използваните и ще направя съответните анализи на тази основа. Общото за всички тях е необходимостта от предварителен достъп до подслушваното помещение и възможност за скрито (незабелязано) инсталиране на съответните технически средства.

1.1.1. Прихващане на акустична информация чрез проводникови микрофони.

При този метод в подслушваното помещение се залага микрофон, от който посредством проводници сигналът се отвежда до вторичен акустичен преобразувател (слушалки или усилвателно стъпало с високоговорител) и/или записващо устройство. Допустимата дължина на проводниците е до 20÷30 m, но с използване на усилвател може да достигне до 120÷500 m.

Предимства на метода: не се изискват високи технически познания за монтажа и експлоатацията на необходимите технически средства; реализацията е проста, евтина и надеждна.

Недостатъци: наличието на проводници, които отвеждат сигнала от микрофона до крайното устройство, е силен демаскиращ признак, който може да разкрие не само наличието на микрофона, но и местоположението на нарушителя, в случаите, когато не се използва записващо устройство, а прослушване в реално време.

1.1.2. Прихващане на акустична информация чрез цифрови диктофони.

При този метод се използват цифрови диктофони, които се прикриват в подслушваното помещение, като това може да стане чрез маскиране в декорации, книги, произведения на изкуството и т. н. Съвременните цифрови диктофони разполагат със система за автоматичен пуск на записа при наличие на

говор в обхвата им, като същевременно, благодарение на вградения им таймер, има и стриктно позициониране на всеки запис по времевата ос. Имат нисък разход на енергия, което позволява направата на десетки часове чист запис. Обхвата им на слушане е с радиус около 8÷10 m и нямат движещи се части, което ги прави устойчиви на температурни колебания, механични въздействия и прах.

Предимства на метода: реализацията е сравнително евтина; устройството, при добър камуфлаж, е трудно за откриване; не се изискват технически познания за използването му.

Недостатъци: необходимост от периодичен достъп до подслушваното помещение за подмяна на паметта и енергийния източник (или на цялото устройство); разговорите не могат да се слушат в реално време.

1.1.3. Прихващане на акустична информация чрез радиомикрофони.

Радиомикрофоните са устройства, които препращат прихванатият акустичен сигнал до нарушителя по радиоканал. Приемането може да се извърши от съседно помещение или сграда, както и на улицата или в превозно средство. Това е най-използвания метод за неоторизиран достъп до информация с помощта на технически средства, като на него се падат около 60% от общия дял[1]. Основните характеристики на радиомикрофоните са:

- габарити и тегло – в зависимост от изпълнението радиомикрофоните могат да са от няколко кубични дециметра и няколко стотин грама до един кубичен сантиметър и няколко грама, когато става въпрос за неспециално изпълнение; при специализирано изпълнение за професионална употреба размерите могат да намалеят до 1.5 x 1.5 mm;
- продължителност на работа – зависи основно от типа на захранващия източник, който може да е автономен (батерия или друг,

[1] Цитираните данни са взети от печатно издание: Атанас Начев, „Технически средства и системи за защита на информацията“, страница 70.

вграден в устройството, източник на енергия) или да се използва електропреносната или телефонната мрежа (което на практика е неизчерпаем източник);

- скритост на работа – осигурява се основно от три показателя:

    1) избрания честотен диапазон – обикновено от 27 MHz до 1.3 GHz, в зависимост от конкретното решение и изпълнение;

    2) използвания режим на работа – радиомикрофонът може да работи в различни режими, като: непрекъснато предаване; предаване при гласова активация; предаване на компресирана дигитализирана информация през определени периоди от време или при поискване от приемащата страна и т. н.;

    3) използвана мощност за предаване;

- акустична чувствителност – това е способността на радиомикрофона да приема акустичните сигнали; за добра се счита чувствителност в рамките на радиус от 5÷12 m;
- далечина на свръзката – условно по този показател радиомикрофоните се подразделят на три групи:

    1) с малък радиус на действие – до няколко десетки метра;

    2) със среден радиус на действие – до няколкостотин метра;

    3) с голям радиус на действие – над 1000 m.

Предимства и недостатъци на метода: Най-общо казано, основното предимство на радиомикрофоните е възможността за предаване на нерегламентирано придобитата информация по безжичен канал на сравнително голямо разстояние, докато основния недостатък е факта, че активния радиоканал се явява демаскиращ признак, по който може да бъде установено наличието и използването на това техническо средство.

От тук насетне анализът не може да се прави общо, поради огромното разнообразие от реализации на радиомикрофоните. Затова ще продължа анализа на база основните им характеристики. Намаляването на габаритите е основно предимство по отношение възможността радиомикрофона да бъде добре скрит и маскиран, но с намаляването на размерите цената започва значително да нараства, а при специализираните изпълнения за професионална употреба има и определен контрол на пазара в някои държави. По отношение продължителността на работа, радиомикрофоните със собствено захранване имат определен времеви ресурс на използване, докато тези, подключени към енергийната или телефонната мрежа водят след себе си два проблема: първо, това значително намалява броя на местата, където радиомикрофона може да бъде търсен; и второ, изискват се определени технически познания и умения, за да се привърже устройството към мрежата, докато тя е под напрежение. При избор на диапазон за предаване трябва да се избягват стандартните честоти, които биха могли да бъдат прихванати случайно от трети лица. От мощността на предаването зависи разстоянието, на което може да бъде приет сигнала, така че трябва да се търси балансът между нуждата от дистанция и рискът, който може да бъде поет, понеже колкото е по-висока мощността, толкова е по-лесно да бъде засечен предавателя. Последния недостатък може частично да се компенсира при използване на предаване с гласова активация, а при използване на цифрови радиомикрофони, които компресират и излъчват записаната акустична информация за много кратък период от време този недостатък на практика е почти изцяло преодолян. При предаването в компресиран вид на порции има друг недостатък – също като при цифровите диктофони информацията се прослушва с известно закъснение.

1.1.4. Прихващане на акустична информация чрез микрофонни устройства и предаването ѝ по инфрачервен канал.

При този метод прихванатият акустичен сигнал се преобразува в електрически и се предава до нарушителя посредством оптичен канал от инфрачервения диапазон.

Предимства на метода: инфрачервеното излъчване не може да бъде открито, поради липсата на демаскиращо радиоизлъчване.

Недостатъци: необходима е пряка видимост между предавателя и приемника; нужни са определени технически познания.

1.1.5. Прихващане на акустична информация чрез микрофонни устройства и предаването ѝ по електропреносни или телефонни линии.

При този метод, прихванатата акустична информация се предава по проводниците на електропреносната инсталация на сградата или по линиите на телефонната мрежа. При използване на силовата мрежа модулацията се извършва при честоти от 40÷600 kHz (в редки случаи – 5÷10 MHz), като максималното разстояние между предавателя и приемника може да е 300÷500 m. При използване на телефонните линии с модулация на високи честоти това разстояние може да нарасне до няколко километра. Тези устройства, наричани още електромрежови микрофони, могат да се монтират в контакти, розетки, удължители и т. н.

Телефонните линии могат да се използват като преносна среда също и от устройства, които се активират чрез набиране на определен телефонен номер. Те предават сигнал само когато са активирани, което ги прави много трудни за откриване, като в същото време разстоянието за подслушването е неограничено, понеже може да се използва системата за международни или мобилни телефонни връзки.

Предимства на метода: изисква еднократен достъп до помещението и е с перспектива за дългосрочно използване.

Недостатъци: при използването на електромрежови микрофони в силовата и/или телефонната мрежа могат да се засекат високочестотните модулирани сигнали, което се явява ясен демаскиращ признак за наличието им; изискват се определени технически познания и умения.

1.1.6. Прихващане на акустична информация чрез пасивни радиоизлъчващи устройства.

Известен още като метод на високочестотното активиране. При него е достатъчно в помещението да има предмет (обект) с нелинейна характеристика. За осъществяването на метода помещението се облъчва с високочестотни радиовълни, които, на практика, карат обекта да ги преизлъчва. Ако в същото време до този обект достига акустична вълна, породена от разговор в помещението, то тази вълна ще предизвиква промени в характеристиките на обекта, което ще породи модулация на акустичната вълна върху честотата на облъчването. Тогава обекта ще излъчва именно този модулиран сигнал, който ако бъде уловен и демодулиран, ще предостави на нарушителя достъп до провеждания разговор. Като преизлъчващ обект може да се използва както предварително подставено пасивно радиопреизлъчващо устройство, така и случайни предмети в стаята, като рамки на картини и др.

Предимства на метода: изключително висока скритост.

Недостатъци: използване на високочестотни сигнали с висока мощност; чувствителна и сложна апаратура за улавяне и демодулиране на преизлъчения сигнал.

1.2. Неоторизиран достъп до акустична информация по структурни канали.

В основата на този метод стои прихващането на акустична информация, разпространяваща се по конструктивните елементи на сградите, като стени, тръби и други твърди тела. За целта се използват т. нар. стетоскопи (контактни микрофони), които преобразуват механични трептения, разпространяващи се в твърди тела, в електрически сигнали. Ако средата е течна (например, вода) се използват хидроакустични преобразуватели. Затихването на звуковите вълни във вода е минимално, което дава възможност за подслушване от голямо разстояние, но то все пак е ограничено от степента на шумовото замърсяване.

Електронния стетоскоп се монтира извън подслушваното помещение и притежава чувствителност от порядъка на 50÷100 μV/Pa, което е достатъчно за улавяне на звукови вълни през бетон с дебелина до 100 cm, врати, рамки на прозорци и т. н., като монтажът му се извършва директно върху тях. Честотният диапазон на електронните стетоскопи е от порядъка на 300÷3000 Hz и тежат от няколко десетки до няколко стотин грама. Може да се реализират и в радио вариант (принципът на предаване по такъв канал вече бе описан при радиомикрофоните).

Предимства на метода: не изисква директен достъп до подслушваното помещение; няма разкриващи признаци за използването му (устройството трябва да бъде открито визуално); малки размери и възможност за монтиране на скрити места и дори от външната страна на сградите.

Недостатъци: силно влияние на страничните шумове; може да се реализира активна защита срещу такъв тип подслушване с помощта на контактни акустични шумови генератори.

1.3. Неоторизиран достъп до акустична информация с използване на насочени микрофони.

Този метод е приложим при необходимост от подслушване на разговори на открито, в помещения с отворени прозорци и пр. За целта се използват микрофони с насочено действие (наричани още насочени микрофони), характеризиращи се с остра диаграма на насоченост. Честотният им диапазон варира от 30÷500 Hz до 12÷20 kHz, а максималната дистанция на прослушване е 50÷100 m при помещения с отворени прозорци и 100÷150 m на открито в извънградска среда. Ако нивото на страничните шумове е достатъчно ниско може да достигне и до 500 m.

Съществуват следните типове насочени микрофони:

- Насочен микрофон с параболично звуково огледало. При него, за постигането на насоченост се използва микрофон, разположен във фокуса на параболично звуково огледало. Благодарение на това, всички звукови сигнали, разпространяващи се перпендикулярно на сечението на огледалото се концентрират в неговия фокус (в микрофона), докато идващите по други направления се разсейват. Нещо повече – концентриращите се във фокуса сигнали са във фаза, докато разсейваните са дефазирани, което допълнително увеличава чувствителността. Чувствителността, също така, е право пропорционална и на големината на използваното огледало. Този тип микрофони се характеризират с висока чувствителност, но слаба насоченост.

- Насочен микрофон, тип „бягаща вълна“ (тръбен микрофон). Той представлява тръба с диаметър 10÷30 mm и с дължина до 1 m. Самият микрофон е монтиран в дъното на тръбата, на която са направени множество отвори, покрити с плат (или друг порест материал), като акустичното съпротивление намалява с отдалечаването от микрофона.

Когато бъдат прихванати звукови вълни, разпространяващи се по оста на микрофона, те проникват в тръбата през отворите и благодарение на равната си скоростна разпространение вътре и извън нея, при достигането си до микрофона са във фаза. Когато, обаче, звуковата вълна не е успоредна на оста на тръбата, съставната на скоростта ѝ по оста вън и вътре в нея ще се различават, което ще доведе до дефазиране.

- Насочен микрофон, тип „микрофонна решетка“. Представлява плоска решетка, към отворите на която са прикачени звуководи, които водят до микрофона. При достигане до решетката на звукова вълна, разпространяваща се перпендикулярно на нейната повърхност, тя достига по звуководите до микрофона във фаза. Колкото ъгълът на разпространение на звуковата вълна е по-малък от 90 градуса, толкова по-голямо става дефазирането на сигналите, достигащи до микрофона по отделните звуководи.

- Насочен резонансен микрофон. Състои се от много на брой тръби с еднакъв диаметър (от порядъка на 10 mm) и различни дължини, разположени пред параболично огледало, в чийто фокус се намира микрофона. Дължината на всяка тръба се определя спрямо нейната резонансна честота.

Предимства на метода: осигурява голяма дистанция между подслушваните обекти и нарушителя.

Недостатъци: необходима е пряка видимост между микрофона и източника на сигнала; изисква прецизно насочване, което при движещ се обект може да е проблем.

1.4. Неоторизиран достъп до акустична информация с използване на лазерни микрофони.

С помощта на лазерен микрофон също може да се осъществи отдалечен достъп до акустична информация, но за разлика от насочения микрофон, тук принципа на действие е съвсем различен. Когато акустичната вълна достигне до даден обект (прозорец, електрическа крушка и пр.) тя предизвиква в него микроколебания, чиито амплитуда и честота съответстват на амплитудата и честотата на звуковата вълна. Това дава възможност, чрез използването на електромагнитна вълна, същия обект да бъде облъчен, като отразената електромагнитна вълна ще бъде модулирана с трептенето, предизвикано от звуковата вълна. При обратното ѝ улавяне и демодулиране, нарушителят може да получи неоторизиран отдалечен достъп до модулиращия сигнал, който е пропорционален на сигнала, разпространяван от звуковата вълна.

Може да се реализира с отделни предавател и приемник, като в този случай те трябва да са от двете противоположни страни на обекта (обикновено стъкло на прозорец) и разположени под един и същ ъгъл (за предпочитане около 45 градуса) или да са обединени в едно устройство, но тогава трябва да се използва оптичен сплитер.

За да може да се осъществи отразяване на електромагнитната вълна е необходимо да бъдат изпълнени две условия:

- Дължината на облъчващата вълна да е съизмерима с амплитудата на предизвиканото от звуковата вълна трептене в облъчвания обект. Обикновено става въпрос за части от милиметъра, което попада във видимия и инфрачервения спектър на оптичния диапазон. За предпочитане е използването на инфрачервен източник, понеже освен, че е невидим за човека, това осигурява и по-слабо разсейване в условия на мъгла или силна запрашеност на въздуха.

- Честотата и амплитудата на облъчващата електромагнитна вълна да са фиксирани и неизменни във времето (кохерентни), което става чрез използването на лазерен лъч (от където идва и името „лазерен микрофон“).

С лазерен микрофон може да се засече реч от 250 m, като в някои професионални изпълнения това разстояние може да надвиши и 1 km.

*Предимства на ме*тода: осигурява значително разстояние между нарушителя и подслушваното помещение, без да е необходим предварителен достъп до него; методът е скрит и труден за демаскиране.

Недостатъци: изисква определени технически познания; в случай на отделни предавател и приемник изисква фина настройка на апаратурата; оборудването е скъпо.

1.5. Неоторизиран достъп до акустична информация с използване на възникваща паразитна електромагнитна индукция.

При този метод, вместо да се поставят микрофони в подслушваното помещение, се използват вече монтирани електромеханични устройства, в които, под въздействието на акустичните вълни се индуцират електродвижещи напрежения на магнитната индукция, изменящи се пропорционално на честотата на звука. Такива устройства могат да са различни електрически звънци, високоговорители, стъпкови електродвигатели и др., които имат в състава си бобини. По този начин тези устройства изпълняват функциите на електромагнитни микрофони, а каналът за отвеждане на сигнала са проводниците на слаботоковата система, към която са свързани. Така на нарушителя не се налага нито да монтира микрофони, нито да осигурява канал за пренос на данните, а само са се свърже към слаботоковата инсталация на използваната система и да усили сигнала до необходимите нива.

Предимства на метода: Не изисква достъп до подслушваното помещение; липса на демаскиращ признак; не изисква пряка видимост между нарушителя и обекта на подслушването; не изисква скъпа апаратура.

Недостатъци: може да се използва само при наличие в помещението на съответните системи и устройства, което е независещо от нарушителя обстоятелство; изискват се определени технически познания и умения.

1.6. Неоторизиран достъп до информация, разпространяваща се по телефонни линии.

Предвид своята глобална разпространеност и употреба, телефонната мрежа предоставя изобилие от методи за осъществяване на неоторизиран достъп до информация. Една телефонна линия е изградена от:

- телефонен апарат;
- разпределителна кутия и линията от телефонния апарат до нея;
- кабелна зона от разпределителната кутия до автоматичната телефонна централа (АТЦ);
- АТЦ;
- многоканална кабелна връзка между две АТЦ;
- радиоканал между две АТЦ (ако има такъв).

Всеки един от тези елементи е потенциално място, от което би могло да се извърши проникване и извличане на информация. Телефонната линия може да бъде използвана по различни начини за осъществяване на несанкционирания достъп до информацията:

- телефонния апарат, дори и при затворена слушалка, може да се използва за улавяне на акустична информация;
- телефонната мрежа може да се използва като нескончаем източник на захранване за различни подслушващи устройства;

- телефонната линия може да се използва за отвеждане на прихванатата акустична информация до нарушителя;
- възможно е подслушване на самата телефонна линия;
- не на последно място, възможно е използване на телефонната линия за провеждане на несанкционирани разговори по нея.

1.6.1. Подслушване на разговори, провеждани в помещение, в което има телефонен апарат.

При използването на телефонния апарат като микрофонно устройство, тази функция може да се осигури от веригите на звънеца или капсулите на слушалката и микрофона. В случай, че линията е затворена, то слушалката се отключва от веригата, но веригата на звънеца продължава да е активна. Така, индуцираните в нея електродвижещи напрежения, в следствие на провежданите в помещението разговори, протичат през телефонната линия и могат да бъдат уловени на разстояние от няколко десетки метра. Ефекта може да се подсили чрез използването на допълнително устройство, което анализира състоянието на линията и при липса на разговор по нея отключва телефона от АТЦ и включва нискочестотен усилвател.

Предимства на метода: не се изисква предварителен достъп до подслушваното помещение.

Недостатъци: приложим е само, когато линията е свободна; изискват се определени технически познания и умения.

1.6.2. Използване на телефонните линии за предаване на информацията от подслушваното помещение.

При този метод се използва устройство, наречено „телефонно ухо“. Предаването на сигналите може да се извършва както на ниски честоти (в диапазона на речевите сигнали), така и на високи. Самото устройство се състои от микрофон, подключен към нискочестотен усилвател. При предаване на ниски

честоти сигналът от усилвателя, посредством комутатор, управляван от устройство за анализ на телефонната линия, се подава през линията само в моментите, когато тя е свободна. При предаване на високи честоти между нискочестотния усилвател и комутатора се извършва модулация на сигнала. При използването на този метод предаването може да се осъществи на разстояние от няколко километра.

Предимства на метода: труден за откриване и надежден; възможност за продължителна във времето употреба.

Недостатъци: приложим е само, когато линията е свободна; изискват се определени технически познания и умения; необходим е предварителен достъп до подслушваното помещение за монтиране на устройството.

1.6.3. Подслушване на разговор, провеждан по телефонна линия.

За разлика от досега разглежданите методи, при този не се налага използването на микрофон или друг подход за преобразуването на акустичните сигнали в електрически, тъй като те, така или иначе, вече са преобразувани за нуждите на предаването им по телефонната линия. Възможни са два варианта за прихващането на сигнала: чрез непосредствено контактно подключване към телефонната линия или чрез подключване с помощта на индукционен датчик.

Непосредственото контактно подключване към телефонната линия обикновено се извършва с телефонна слушалка, като единствено е необходимо осигуряване на физически достъп до дадена част от линията. Освен слушалка, може да се сложи записващо устройство, радиопредавателно устройство и пр. Директното подключване внася допълнителен пад на напрежението в линията, което е силен демаскиращ признак. За да се намали неговото въздействие може да се използват високоомни слушалки или подключването да се извърши през съгласуващ трансформатор или с използване на компенсираща пада на напрежението схема със собствен енергиен източник.

При използването на индукционен датчик за включване към телефонната линия се избягва проблема с пада на напрежението в нея. За целта проводниците на усуканата двойка се отделят един от друг, за да се избегне ефекта на взаимното погасяване на предизвикваната от тях магнитна индукция и единия проводник се прекарва през затворен магнитопровод, който играе ролята на индуктивен датчик. Полученият от намотките на магнитопровода сигнал е пропорционален на сигнала, предаван по телефонната линия, и след съответното усилване може да бъде използван за прослушване на провеждания разговор. С цел усилване на сигнала, втория проводник може също да се прекара през магнитопровода, но в обратна посока – така сигналите в двата кабела ще текат в едно и също направление и вместо създаваната от тях магнитна индукция да се изважда, ще се сумира.

Предимства на метода: не сложна, но ефективна технология; наличие на множество места, от които може да се извърши интервенцията; за индуктивното подключване – не се нарушава целостта на проводниците на мястото на подключването, не внася пад на напрежение в телефонната линия, датчикът не може да се повреди при подаване на високо напрежение на линията.

Недостатъци: необходим е физически достъп до сегмент от телефонната линия; нужни са определени технически познания и умения; за контактното включване – нарушаване целостта на проводниците на мястото на подключването, внасяне на пад на напрежение в телефонната линия, апаратурата може да бъде повредена при подаване на високо напрежение; за индуктивното подключване – необходимост от усилване на сигнала.

1.7. Неоторизиран достъп до информация, разпространяваща се в системите за мобилна радиовръзка.

Предвид факта, че *GSM* технологията е открита технология, каквито и мерки за сигурност да бъдат предприети за защита тя винаги може да стане обект

на атака от страна на недоброжелатели. Възможностите за такава атака са много разнообразни и включват:

- достъп до разговорите, провеждани от абоната на *GSM* услугата, чрез прихващането им в участъка между *GSM* апарата и базовата станция;
- достъп до информацията, която се обменя между базовите станции;
- достъп до *SMS* съобщенията на даден абонат;
- използване на *GSM* апарата като радиомикрофон;
- използване на *GSM* апарата за локализиране местоположението на неговия приносител.

Подобно (несанкционирано от абоната) използване на *GSM* апарата може да се заподозре при проявяване на някои от следните демаскиращи признаци:

- апаратът излъчва радиосигнал дори и когато по него не се говори;
- постоянно греене на батерията;
- бързо изтощаване на батерията, без да има основание за това;
- нетипична активност на апарата;
- страничен шум в апарата;
- нетипични смущения, които апаратът предизвиква в други радиоелектронни устройства около него.

Предимства на метода: дава изключително големи възможности за достъп до информация; не се изисква пряк достъп до следеното лице.

Недостатъци: скъпо оборудване; необходими значителни познания за използването на метода; наличие на демаскиращи признаци.

1.8. Неоторизиран достъп до информация, чрез прихващане на паразитни електромагнитни излъчвания.

Всяко електронно устройство, което работи с променливи токове, излъчва в пространството паразитни електромагнитни вълни (ПЕМВ). В случаите, когато тези токове са информационно носещи, излъчените от тях ПЕМВ са преносители на същата информация, като токовете. Устройствата, които генерират такива излъчвания са: персонални компютри, телекомуникационно оборудване, компютърни мрежи, монитори и много други. С използването на съответна радиоприемна апаратура ПЕМВ могат да бъдат уловени и използвани за възстановяване на информацията и процесите, осъществявани в излъчващите ги устройства.

Тъй като ПЕМВ, при достигането си до телефонни линии, тръби на водопроводни и отоплителни инсталации, заземителни уредби и пр., предизвикват в тях паразитни електродвижещи напрежения (ПЕДН), то те също стават носители на информацията и могат да бъдат прихванати и използвани за несанкциониран достъп до информация.

Предимства на метода: силно прикрит; има възможност за прилагане от голямо разстояние.

Недостатъци: скъпо оборудване; необходими значителни познания за използването на метода.

1.9. Използване на скрито видеонаблюдение като средство за неоторизиран достъп до информация.

Поради бурното развитие на технологиите, видеокамерите стават с все по-малки размери, по-ниска енергийна консумация, по-добро качество на приеманата картина и по-ниска цена. Това, естествено, е предпоставка средствата и системите за скрито видеонаблюдение да имат широко приложение при неоторизираното придобиване на информация.

Камера (с или без микрофон) може да бъде скрита в почти всичко и навсякъде, стига нарушителят да си осигури достъп до мястото за наблюдение. Начините за отвеждане на сигнала от камерата до нарушителя са най-разнообразни, като например:

- използване на кабелна връзка;
- използване на радиочестота за предаване на данните;
- използване на *Wi-Fi* за предаване, приемане и управление;
- използване услугите на *GSM* оператор и т. н.

Предимства на метода: възможност за използване на всевъзможни обекти за камуфлаж; достъпна и нескъпа (в повечето случаи) технология; възможност за използване на инфрачервения диапазон.

Недостатъци: изисква се предварителен достъп до мястото, определено за наблюдаване; има ъгъл на насоченост на приемания образ.

Изводи от първа глава.

1) Методите за неоторизиран достъп до информация с използването на технически средства се характеризират с почти пълна насоченост срещу конфиденциалността (тайната) на информацията.
2) За реализиране на методите за неоторизиран достъп до определена информация в някои случаи се изисква физически достъп до съответни физически средства, или това се осъществява на логическо ниво.
3) Техническите средства за неоторизиран достъп до информация осъществяват този достъп най-вече в процеса на нейното предаване (разпространяване).

ГЛАВА II: ИЗПОЛЗВАНИ МЕТОДИ ЗА НЕОТОРИЗИРАН ДОСТЪП ДО КОМПЮТЪРНО ОБРАБОТВАНА ИНФОРМАЦИЯ

В тази глава ще бъдат описани основните методи за неоторизиран достъп до компютърно обработвана информация. Прието е, тези методи да се наричат компютърни атаки или просто атаки. Извършителите на тези атаки използват уязвимости в компютърните системи и мрежи. Обект на този тип атаки са самите компютърни системи и мрежи, както и информацията, услугите и ресурсите, които те предоставят. Целите на тези атаки са предимно получаване на несанкциониран достъп до различни информационни ресурси и мощности, предизвикване на отказ на услуга, уронване престижа и авторитета на организацията, чиято информационна система бива атакувана и др.

Средствата за осъществяване на компютърните атаки почти винаги също са компютърни системи и мрежи, но също така – различен приложен софтуер, напреднали информационни технологии, пропуски („бъгове“) в защитата на операционни системи, приложения и протоколи, недостатъци на системата за защита на информацията и др. По-популярните атаки срещу компютрите и мрежите са: *DoS* атака; *IP Spoofing*; физическо подслушване в мрежата; атаки, посредством вредни програми; атака тип човек по средата и много други.

2.1. *DoS* (*Denial of Service*, отказ на услугата) атака.

Атаките от този тип, независимо от подхода и начина на реализацията им, имат за цел прекъсването на нормалната работа на прицелната системата. Обикновено *DoS* атаката се осъществява, като „нападателя“ (хакера) „затрупва“ целта със заявки и по този начин системата (сървър, рутер, приложение, мрежа и др.), обработваща (или пренасяща) тези заявки, изчерпва целия си наличен ресурс. Така, при опит от страна на легален потребител да достъпи информацията, услугата и/или приложението, предоставяни от тази система,

същият няма да бъде обслужен, поради недостиг на ресурс, за да му бъде върнат отговор. Една разновидност на *DoS* атаката е *DDoS* (*Distributed Denial of Service*, разпределена атака за отказ на услугата), при която „затрупването“ със заявки се осъществява от много устройства. Те, обикновено, не са собственост на атакуващия, а са „заразени“ устройства на потребители, които не подозират, че някой ги използва за атака. Поради тази причина тези устройства се наричат „зомбита“, а мрежата от тях – „зомби мрежа“ (или още „зомби ферма“). Най-често използваните форми на *DoS* атака са: *Ping/ICMP* „наводнение“; смърф атака; *Ping of Death*; *SYN* атака; сканиране на портове. От гледна точка на направленията на сигурността, *DoS* атаката е насочена срещу достъпността на информацията/услугите, но ако тази атака е част от по-голяма серия от разнообразни атаки, то биха могли да бъдат засегнати и други направления (конфиденциалност и/или цялостност).

2.1.1. *Ping/ICMP* „наводнение“.

При този вид атаки се използва командата *ping* от протокола *ICMP* (*Internet Control Message Protocol*). Оригиналната ѝ функция е да провери дали даден *IP* адрес съществува, през колко на брой мрежови устройства се преминава, докато бъде достигнат и за колко време. Ако, обаче, към *IP* адреса започне постоянно да се изпращат *ping* запитвания от множество източници (например, зомби ферма), то това може да доведе до забавяне работата на устройството (компютър, сървър, рутер и пр.), а при достатъчно голямо натоварване и до пълен отказ на услуга.

2.1.2. Смърф атака.

Смърф атаката донякъде прилича на *Ping/ICMP* наводнението, но при нея запитванията се изпращат към бродкаст адреса (*broadcast address*) на локалната мрежа (*Local Area Network, LAN*). Това е последния адрес в мрежата и той не се дава на никое устройство, а стои свободен и се използва за реализиране на запитвания към всички устройства в *LAN*, т. е., запитване, изпратено към този

адрес е равносилно на запитване, изпратено до всички устройства в дадената локална мрежа.

Неудобството на този метод е, че не може да се реализира извън локалната мрежа, тъй като рутерите не предават заявки към бродкаст адрес. Но за сметка на това, ако нарушителят успее да си осигури достъп до локалната мрежа може да използва самата нея, за да се самонаводни, без да му е необходима зомби ферма.

Обикновено жертва на този вид атака стават доставчиците на интернет услуги (*Internet Service Provider, ISP*). Трафикът, генериран при един такъв процес, може лесно да забави работата на мрежи с ниска пропускателна способност и дори напълно да прекъсне работата им.

2.1.3. *Ping of Death*.

Ping of Death (от английски, „пинг на смъртта“) е атака, която използва ограничението, налагано от *MTU* (*Maximum Transmission Unit*, максимална единица за предаване) върху размера на пакетите, които могат да се предават в дадена мрежа. В случаите, когато бъде изпратен пакет с по-голям размер от максимално допустимия той се разделя на по-малки парчета, които се сглобяват при получателя. *IP* пакетът на командата *ping* по принцип е ограничен до 65’535 байта, но при намеса от страна на хакер може да се изпрати пакет надхвърлящ този обем. Когато системата-получател направи опит да сглоби този пакет, тя се срива.

2.1.4. *SYN* атака.

При този тип атака се използва синхронизиращата последователност за установяване на връзка между клиент и сървър на *TCP* (*Transmission Control Protocol*). Нормално тази последователност е следната:

- клиентът изпраща към сървъра *SYN* пакет;
- сървърът отговаря със *SYN/ACK* пакет;

- клиентът отговоря с *ACK* пакет и преносът на данни започва.

При *SYN* атака към сървъра се изпращат голям брой заявки за стартиране на сесия, на които той отговаря със *SYN/ACK* пакет и ги натрупва в опашката за изчакване на последния *ACK* пакет, който така и не бива изпращан. Ако заявките са достатъчно на брой и достатъчно често изпращани опашката се препълва и това пречи на отварянето на сесии на реалните потребители.

2.1.5. Сканиране на портове.

Сканирането на портове не води пряко до отказ на услугата, но спомага да се направи предварителен оглед за слаби места (уязвимости) в мрежата, преди да се осъществи същинската атака срещу информационната система.

За да може да работи и да бъде коректно разпознавано от системата на всяко приложение му се присвоява определен порт. Чрез сканиране на използваните портове може да се направи оценка на това кои приложения и мрежови ресурси са на разположение в прицелната мрежа.

2.2. *IP Spoofing* (подправяне).

Тази атака се изразява в промяна на хедърите на пакетите на съобщенията, които се изпращат. По този начин те изглеждат така, сякаш идват от друг *IP* адрес. В крайна сметка целия поток от данни към/от даден хост или даже мрежов сегмент се пренасочва да минава през компютър, контролиран от атакуващия. Това позволява информацията да бъде преглеждана, претърсвана и/или подправяна (изменяна). От гледна точка на елементите на сигурността, *IP Spoofing* атаката е насочена срещу конфиденциалността и/или цялостността.

2.3. Физическо подслушване в мрежата.

Принципът е следния – данните се прихващат и с помощта на декодер на *Ethernet* пакети шестнадесетичните данни се преобразуват във вид, разбираем за хора. За да може да се реализира физическо подслушване на пакети, е нужно да се постави устройство между източника и получателя на данните. Заради това

мрежите с общи среди са особено податливи на подслушване. От гледна точка на направленията на сигурността, атаката физическо подслушване в мрежата е насочена срещу конфиденциалността.

2.4. Атаки, посредством вредни програми (*malicious software, malware*).

Вредно програмно осигуряване е обобщен термин за софтуер, който целенасочено нанася вреда на компютърни системи и мрежи. Вредните програми се наричат още малуеър (*malware*), което идва от смесването на английските думи за „злобен“ (*malicious*) и „софтуер“ (*software*). В последно време, към него може да се причисли и т. нар. „шпионски“ софтуер (*spyware*). Шпионският софтуер е програма, която се инсталира тайно на потребителския компютър, за да следи и предава информация за начина на използване на Интернет и/или всякаква друга информация, като пароли, лични данни, банкови сметки и пр. Друга разновидност са адуеър (*adware*) програмите – те се инсталират без информираното съгласие на потребителя и генерират различни рекламни съобщения (*pop-ups*). Сред най-популярните видове вредни програми са: логическите „бомби“; люковете (*trap doors*); задните врати (*back doors*); компютърните „вируси“; компютърните „червеи“; файловите „червеи“; „бактериите“; троянските коне (*Trojan horse*) и др. От гледна точка на направленията на сигурността, атаката с вредни програми може да бъде насочена и/или срещу достъпността, и/или срещу конфиденциалността, и/или срещу цялостността на информацията/услугите на информационната система.

2.4.1 Логически „бомби“.

При логическите бомби вредния код се имплантира в легален програмен продукт, като е програмиран така, че да „избухне“ (да извърши вредното си действие) при удовлетворяването на определено условие (или комбинация от условия). Такова условие може да е настъпване на определена дата и/или час, логване на потребител, запис във файл и пр. При задействането

си, логическата бомба може да модифицира или изтрие файлове, да повлияе на определени процеси или да блокира работата на цялата операционна система.

2.4.2 Люкове (*trap doors*).

Люковете са тайни входни точки в програма или система, чрез които неоторизиран потребител може да получи достъп до защитаваните ресурси, без да премине през заложените процедури за сигурност. Официалното им предназначение е за коригиране на програмни грешки и извършване на тестове от страна на разработчиците на програмния продукт. Осъществяването на контрол върху подобни входове е изключително трудно.

2.4.3 Задните врати (*back doors*).

Задната врата е програма, чрез която нарушителя може безпрепятствено и по всяко време да получи достъп до атакуваната система. Обикновено се вмъква към start-up механизма[2] на операционната система (или на дадена програма) и така се задейства при всяко нейно пускане. Откриването и премахването им е изключително трудно, затова най-добрия начин за справяне с тях е преинсталация на операционната система и възстановяване на приложния софтуер и данните.

2.4.4 Компютърни „вируси“.

Компютърният вирус е фрагмент от програмен код, който се саморазпространява като модифицира кода на други програми. Сам по себе си той не е самостоятелна програма, а се изпълнява при изпълнението на програмите, които е „заразил“. Вирусът може да е настроен така, че да се задейства при настъпването на дадено събитие (например, на петък 13-ти).

[2] Поредица от действия, които се изпълняват при стартиране на операционна система или програма.

2.4.5 Компютърни „червеи“.

Компютърните червеи много приличат на вирусите, но за разлика от тях те са самостоятелни програми. Преминават от компютър на компютър, като използват уязвимости в мрежовите протоколи и обикновено не правят свои копия в постоянната, а заразяват само оперативната памет на компютъра/сървъра.

2.4.6 Файлови „червеи“.

Файловите червеи се разпространяват под формата на файлове, като използват възможностите на файловата система. Съществуват най-различни варианти за предаването и активирането им, като:

- използват се стандартни имена на системни файлове, като така потребителите по грешка може да ги активират;
- добавят се в архиви и се активират при възстановителните процедури;
- вмъкват инструкции за активирането си в различни изпълними файлове и скриптове;
- прикачат се към електронната поща;
- прикачат се като макроси в различни документи;
- прикачат се като скриптове в *HTML* страници и др.

2.4.7 „Бактерии“.

Бактериите, като вреден софтуер, не правят нищо друго, освен да се самовъзпроизвеждат. Всяка бактерия прави свой наследник и така се удвоява. Това води до експоненциално нарастване на броят им, като в същото време системата остава без свободна памет и процесорно време за своята легална работа.

2.4.8 Троянски кон (*Trojan horse*).

Троянските коне са програми, използващи прикритието на даден полезен софтуер. Те не разполагат със собствен механизъм за разпространение (като вирусите и червеите), а разчитат на некомпетентността и непредпазливостта на потребителите, за да бъдат инсталирани или активирани. Могат да бъдат скрити в инсталационните пакети на операционната система или приложен софтуер, прикачени към електронната поща и т. н.

Различават се следните типове троянски коне:

- Предоставящ отдалечена администрация – след инсталирането си предоставя на нарушителя отдалечен административен достъп до системата.
- Файлов сървър – при активирането си стартира в заразената система услугата файлов или *FTP* сървър. Обикновено се използва за последващо инсталиране на троянски кон, предоставящ отдалечена администрация. Размерите им са изключително малки (от порядъка на няколко килобайта), което позволява лесното им внедряване в различни инсталационни пакети, приложен софтуер и игри.
- Крадец на пароли – „краде“ паролите на потребителите на засегнатата система и да ги изпраща на определен адрес, където нападателят може да получи достъп до тях.
- *Key logger* – създава лог на всяко действие, извършено от клавиатурата на поразената система. В даден момент тези логове се изпращат на нападателя, който може да ги анализира за потребителски имена и пароли или друга чувствителна информация.
- *DDoS* – след инсталирането си превръща поразената система в „зомби“, което, в последствие, се използва, заедно с множество други заразени системи, за организиране на разпределени атаки за отказ на услуга без знанието на легалните потребители.

2.5. Атака тип човек по средата (*Man in the Middle, MitM*).

При атаки от този вид нападателят се позиционира между потребителя и сървъра, предлагащ определен ресурс/услуга. Хакерът създава две сесии – първата е към потребителя, а втората – към сървъра. При опит от страна на потребителя да достъпи ресурса, предоставян от сървъра, атакуващия се представя за него. Така той получава цялата информация, необходима му, за да изгради легална сесия към сървъра от името на потребителя. По този начин нападателят може да получи неоторизиран достъп до чувствителни данни. По-съвременен вариант на „*Man in the Middle*“ е „*Man in the Browser*“ (буквално – човек в браузъра). Подходът е много подобен – извършителят използва *malware* на компютъра на потребителя, който се изпълнява в браузъра. Той записва данните, течащи между потребителя и различни уебсайтове, които нарушителят е задал да бъдат следени. Използването на вреден код позволява едновременното прицелване в по-широка група потребители и не изисква физическата близост на нападателя до неговите жертвите. От гледна точка на направленията на сигурността, атаката тип човек по средата може да бъде насочена и/или срещу достъпността, и/или срещу конфиденциалността, и/или срещу цялостността на информацията/услугите на информационната система.

2.6. Социален инженеринг.

Социалният инженеринг е съвкупност от техники и средства за манипулиране на отделни хора или цели групи, с цел, да бъдат използвани пряко или косвено (чрез придобита от тях информация, достъп или друго) като входна точка за атака или нерегламентирано придобиване на информация или друг ресурс. Той може да има изключително разнородна насоченост и средства[3], но за целите на тази дипломна работа ще разгледам „фишинга“, като негова основна компютърна разновидност. Идеята е, чрез манипулиране на човешките емоции,

[3] Пример за некомпютърен социален инженеринг, който напоследък е много наболял в България, са т. нар. телефонни измами, където целта е кражба на пари и/или ценни предмети, а средствата за постигане на целта са телефонен разговор и заблуда.

да се накара обекта (човек или група хора) да направи нещо без да се замисля, което да доведе до разкриване на чувствителна информация или до допускане на нарушителя в информационната система.

2.6.1. Атака тип фишинг (*phishing*, зарибяване).

Фишинга (*phishing*, от нарочно промененото *fishing* – риболов) е, може би, най-често използвания метод за атака от социалния инженеринг. Нарушителят разпраща електронни съобщения или поща, като претендира, че е достоверен източник, и се опитва да убеди получателя да предприеме определено действие (да даде лична, служебна или финансова информация, да влезе уебсайт, да отвори прикачен файл и т. н.). Обикновено, фишинг атаките се реализират масово, към всякакъв тип потребители. Има и по-целенасочена атака чрез фишинг, която се нарича *spear phishing*, като при нея целта е конкретен човек или организация.

Съгласно изследване, проведено от *Intel Security* сред 19 хиляди потребители на *e-mail* услуги в 144 страни, едва 3% от хората съумяват да разпознаят *phishing* в кореспонденцията си[4].

Изводи от втора глава.

1) За разлика от методите, използващи технически средства, където основната цел е компрометиране на конфиденциалността, при атаките срещу компютърно обработвана информация цел са също така цялостността и достъпността на информационните ресурси.
2) В повечето случаи не се изисква никакъв физически достъп до информационната система, за да се реализира атаката. В редките случаи, когато това е необходимо, след първоначалната физическа интервенция атаката пак може да се осъществи от произволна точка на земното кълбо.

[4] Данните са взети от публикация в Интернет: Виктория Лазова, „Едва 3% разпознават фишинга в имейла си“, *http://cio.bg/7252_edva_3_razpoznavat_fishinga_v_imejla_si/*.

3) Компютърно обработваната информация е уязвима за атака във всяка фаза на нейното съществуване: създаване, съхраняване, обработване, предаване, унищожаване.

ГЛАВА III: ПОДХОДИ И МЕТОДИ ЗА ЗАЩИТА НА ИНФОРМАЦИЯТА. КОМПЛЕКСНА ЗАЩИТА НА ИНФОРМАЦИЯТА.

Методите за защита на информацията са не по-малко разнообразни от заплахите и средствата за атаки спрямо нея. Все пак, може да се направи класификация, на база средствата, чрез които се реализират. Според тази класификация те могат да са управленски, организационни, технически, програмни, физически, психологически и др., както и различни комбинации между тях.

Макар всеки един от методите да има своето приложение в защитата на информацията, истинската им сила е, когато се използват координирано и под общо планиране и управление. Една система за защита на информацията, която управлява комплексно всички използвани от организацията методи, има предимството да е много по-ефикасна и да има синергично действие – ефективността на цялата система многократно да надвишава сумарната ефективност на нейните съставни части по отделно.

В тази глава ще разгледам методите за защита на информацията разделени по направления, за да се демонстрира по-добре приносът на всеки от тях, но трябва да се има предвид, че при цялостното изграждане на системата за защита на информацията те следва да се разглеждат комплексно и в общ контекст. На различни места ще давам примери за това как използването на даден метод в комбинация с друг би повишило ефективността на защитата.

3.1. Документация.

Тук се включват всички документи (политики, договори и съглашения, декларации, заповеди, наръчници, указания, вътрешни правила и др.), създадени от и/или съвместно с организацията, които пряко или косвено са свързани със защитата, обезпечаването и работа на/с информационната система. Те могат да

са най-разнообразни като обхват, обем и тип. В тях ясно, конкретно и методично следва да са разписани: възможностите и начините на функциониране и използване на системата и нейните ресурси и услуги; правата и задълженията на всички, имащи достъп до информацията и процесите, обработвани в системата; административните санкции, на които подлежат евентуалните нарушители и др. Ще обърна по-подробно внимание на най-важния документ, свързан с информационната сигурност – политика за информационна сигурност.

3.1.1. Политика за информационна сигурност.

Политиката за информационна сигурност (ПИС) е основополагащият документ на организацията, свързан със защитата на информацията и системите, които я събират, обработват, предават и съхраняват. Тя представлява множество от правила, практики и указания, които предопределят начина, по който организацията управлява, разпределя и защитава информацията и свързаните с нея процеси и услуги. ПИС е една своеобразна рамка, която предоставя насоки за управление и поддръжка на информационната сигурност съобразно целите и дейността на организацията. Задължително се одобрява и налага от най-висшето ръководство (когато организацията е държавна структура, това е политическото ръководство на съответната административна структура), като по този начин се гарантира нейното безпрекословно изпълнение и се демонстрира ангажимент към сигурността на информацията.

В обхвата на политиката за информационна сигурност се включват: разпределението на, и работата с информационните ресурси и услуги, както и контролът на достъпа до тях; правилата за идентификация и автентификация (било то локално или отдалечено); условията за използване на криптографски методи и устройства при защитата на информацията; защитата от компютърни вируси и друг вреден софтуер; изготвяне на различни ръководства (за администраторите, потребителите и др.); каква трябва да е квалификацията на персонала и какви обучения следва да премине (еднократно, периодично, при

промяна на задълженията и отговорностите и др.) и т. н. Също така, тя трябва да бъде сведена до знанието на всички потребители, в подходяща, достъпна и разбираема форма.

ПИС следва да подлежи на преразглеждане на определен, планиран интервал от време, или при настъпване на сериозни изменения в средата/обстановката (в зависимост от появата на нови, или елиминирането на налични заплахи, уязвимости и рискове), целите или средствата за събиране, обработване, предаване и съхранение на информацията, за да се гарантира нейната адекватност, ефективност и ефикасност във всеки един момент.

В зависимост от конкретната организация и информационната система, която тя поддържа и следва да се защитава, политиката за информационна сигурност може да има различно съдържание и подредба. Все пак, стандартът *ISO/IEC 27003* препоръчва следната структура на ПИС:

- резюме – кратък преглед в няколко изречения;
- въведение – обяснение на нуждите от ПИС;
- обхват – описание на частите и дейностите на организацията, за които се отнася ПИС;
- цели – описание на намеренията на ПИС;
- принципи – описание на правилата, касаещи действия и решения за постигане на целите;
- отговорности – описание на това кой е отговорен за изпълнението на изискванията на политиката;
- ключови резултати – описание на очакваните резултати, свързани с поставените по-горе цели;
- свързани политики – описание на други политики, имащи отношение към постигането на целите ПИС.

3.2. Роли и отговорности.

Разделянето на ролите и свързаните с тях отговорности е важен подход при реализирането на информационната сигурност. Той позволява ясно да се дефинират длъжностите, които определят политиките при изпълнението на дадени процеси и/или услуги, длъжностите, които отговарят за изпълнението на тези процеси и/или услуги и длъжностите, които контролират дали тези процеси и/или услуги се реализират в съответствие с политиките за тях. При големи организации това разпределение не е особен проблем, но при по-малки структури, разполагащи с ограничен човешки ресурс, може да се наложи един служител да съвместява няколко роли и съответно да поеме свързаните с тях отговорности. Това е допустимо, но трябва да се внимава съвместяваните роли да не са в конфликт една с друга. Например, ако едно и също лице едновременно задава политиките за изпълнение на даден процес и в същото време отговаря за изпълнението (реализацията) на същия процес, то е възможно (дори несъзнателно), за да улесни изпълнението на процеса да занижи критериите в политиките. Също така, ако едно и също лице едновременно реализира процес/услуга и в същото време контролира изпълнението на този процес/услуга, е възможно да премълчи някои проблеми пред органа, пред който се отчита. Не е проблем да се съвместяват роли, които задават и контролират един и същ процес и/или услуга.

Ключовите роли, в базираните на информационните технологии системи, могат да се подразделят на четири основни групи: главен информационен мениджър; управление на информационната сигурност; системно и мрежово администриране; потребители на информационната система.

3.2.1. Главен информационен мениджър.

Главният информационен мениджър (ГИМ) е гарант за адекватността и актуалността на информационната сигурност в организацията. Ролята на ГИМ е свързана със следните отговорности:

- координира и съблюдава политиката за информационна сигурност на организацията, предлага варианти за развитие и промяна, в съответствие с променящата се среда;
- задава процедури за оценка на сигурността, които обхващат цялата организация;
- участва при разработката на методи за вземане на решения и при определянето на приоритетните системи на сигурността.

3.2.2. Управление на информационната сигурност.

Управлението на информационната сигурност се осъществява от служителите по информационна сигурност (СИС). Те отговарят за надзора на всички елементи на сигурността на информацията в рамките на конкретни структури на организацията. Следят за съответствието и прилагането на организационните стандарти, политики и процедури при реализирането на информационната сигурност. Имат следните отговорности:

- разработват процедури за сигурност в сферата на своите компетентности и отговорности;
- участват при прилагането и разработването на различни механизми и инструменти за сигурност;
- поддържат конфигурационните профили на системите, за които отговаря организацията (компютри, сървъри, портали и др.);
- поддържат оперативната цялост на системите.

3.2.3. Системно и мрежово администриране.

Системните и мрежови администратори (СМА) отговарят за конкретна система или подсистема и имат следните отговорности:

- провеждат мониторинг на системата, като следят за нейната цялостност и за свързани със сигурността събития в нея;
- отстраняват откритите при мониторинга грешки и несъответствия в системата;
- участват в провеждането на тестове за сигурност на системата;
- дават оценка на мерките за сигурност на системата.

3.2.4. Потребители.

Ролята на потребителите е най-широката и за разлика от останалите, тя няма отговорности към функционирането на системата. Техните отговорности са насочени към спазването на правилата и политиките за работа с информационната система и оборудване.

3.3. Идентификация, автентификация и оторизация.

3.3.1. Идентификация.

За да осигури безопасността на данните, информационната система не трябва да разрешава каквато и да било операции над тях (четене, копиране, изтриване и т. н.), ако потребителя няма съответните права за това. За всеки потребител, тези права се описват чрез серия записи в системата, описващи неговия профил. Преди да получи достъп, потребителят трябва да се идентифицира чрез съответен идентификатор (например, потребителско име). Така системата бива насочена към съответния потребителски профил. След това, потребителят трябва да потвърди своята идентификация (да докаже, че е този, за когото се представя) чрез автентификация.

3.3.2. Автентификация.

Процесът на автентификацията представлява проверка (сравняване) на данни, които потребителят предоставя на системата и които само той би следвало да притежава. Автентификацията може да е еднофакторна или многофакторна (двуфакторна, трифакторна и т. н.). Различните фактори на автентификацията се формират на базата на специфични за тях критерии, на които отговарят данните, предоставени от потребителя (ако данните отговарят на критерия на даден фактор – методът следва да се причисли към неговата група). Най-широко използваните фактори са три и имат следните критерии:

- Нещо, което знам. Тук влизат методи, като използване на пароли, пин кодове, отговори на тайни въпроси и т. н.
- Нещо, което имам. Това са физически устройства, които генерират данните на база своята функционалност: смарт карти, генератори на пароли и кодове и т. н.
- Нещо, което съм. Такива са биометричните данни, като пръстов отпечатък, карта на ретината на окото и т. н.

Важно е да се отбележи, че като се определя колко факторна е автентификацията, се броят чистите фактори, а не похватите. Например, ако вече се използват пръстови отпечатъци и се добави и сканиране на ретината, то броя на факторите не се увеличава.

3.3.3. Оторизация.

След успешна автентификация, системата извършва оторизация – предоставяне на потребителя на права за достъп до данни, ресурси и услуги, съобразно правата, които са зададени в неговия профил. Оторизацията може да бъде и по-сложна – когато освен успешната автентификация се правят и други проверки, например дали дадения потребител се опитва да влезе в системата в

рамките на работното си време, дали го прави от собственото си работно място и т. н.

3.3.4. Пароли – добри практики.

Факторът, отговарящ на критерият „нещо, което знам“, и по-специално, методът „двойка потребителско име и парола“ е най-масово използваният. Ето някои добри практики, при съставянето и използването на пароли:

- Използване на комплексна парола. Комплексната парола е съставена задължително от букви (малък и голям регистър), цифри и специални символи. Обикновено има и изискване за минимална дължина (брой символи) на паролата. Това значително намалява шанса паролата да бъде налучкана или отгатната от евентуален нарушител.

- Използване на генератор на случайни пароли. Това е устройство (или софтуер), което генерира случайна последователност от символи (обикновено отговаряща на изискванията за комплексност на паролата).

- Една и съща парола да не се използва за две различни системи. Това елиминира вероятността при „откradване“ на паролата за едната система, автоматично да се компрометира и другата.

- Паролата да се сменя на определен период от време (например 30 дни). Така, в случай на компрометиране на парола, след най-много един пълен период тя вече няма да е актуална.

- Да не се използва една и съща парола два пъти в една и съща система. Обикновена се прилага по-лек вариант – да не се използва някоя от последно използваните пароли (например, последните 10).

3.4. Управление на потребителите.

Под управление на потребителите на една информационна система се има предвид управлението на техните потребителски акаунти за достъп до нейните ресурси и услуги. Акаунтите условно могат да се разделят на четири големи групи: потребител по подразбиране (*default user*); гост (*guest*); потребител (*power user*) и администратор (*administrator*). Първите два почти не се използват, затова няма да се спирам на тях. Акаунтите тип *power user* са потребители със специфични привилегии, съобразно конкретните дейности на служителите. Администраторските акаунти имат значително по-големи привилегии. Техните собственици следва да познават много добре функционалностите на информационната система и да имат отговорности, свързани с нейната коректна и адекватна работа.

При конфигурирането на акаунтите следва да се спазва принципа на минимални привилегии, т. е. оторизация и привилегии трябва да се дават единствено и само въз основа на конкретните задачи, които имат потребителите. Това е еквивалент на максимата „необходимо да се знае“. Така се свежда до минимум възможността за неволна или предумишлена злоупотреба с информация и информационни ресурси.

Една от добрите практики е на потребителските акаунти да не се дават никакви права, а те да се задават на групи, към които акаунтите да се причисляват. Като членове на групата (един акаунт може да е член и на повече от една група) те наследяват всички нейни права (и ограничения). По този начин много лесно се променят и одитират привилегиите и няма опасност някой потребител да бъде пропуснат и по грешка да бъде с неправилни (било то по-големи или по-малки) привилегии.

Друг важен момент при управлението на потребителските акаунти е добрата комуникация между администраторите на информационната система и отдел „Човешки ресурси“. От критична важност е във всеки един момент да се

знае статута на всеки служител на компанията (новоназначен, повишен, преместен от един отдел в друг, уволнен, напуснал, пенсиониран и т. н.), както и на външните партньори, които имат достъп до информационната система на организацията, за да може своевременно да се реагира по отношение на техните права за достъп и привилегии в системата. В противен случай може да бъде създадена сериозна уязвимост, която при реализирана заплаха да компрометира информацията, процесите и/или услугите, предоставяни от системата. Например, ако акаунтът на един пенсиониран служител не бъде деактивиран, то той се превръща в една възможност за нерегламентиран достъп до системата за всеки, който по някакъв начин се сдобие с паролата му. Или пък един дисциплинарно уволнен служител може да се опита да си отмъсти на компанията, използвайки все още неотнетите му права. В този случай е желателно администраторите на системата да са уведомени още преди служителя, за да деактивират акаунта му предварително.

3.5. Контрол на сесията.

Съществуват редица добри практики по отношение контрола на сесиите на потребителите в информационните системи, спазването на които могат значително да намалят риска от нерегламентиран достъп и/или да увеличат шанса да бъде засечен опит за такъв. Ще разгледам по-популярните от тях.

3.5.1. Предупредително съобщение.

Добре е, когато няма отворена сесия, но компютърната станция е включена, на екрана на монитора да стои някакво съобщение. Тъй като то ще е достъпно за всеки в обсега на монитора, в него не следва да се поместват чувствителна информация. То може да съдържа части от (или цялото) „Съгласие за достъпа до компютрите и Интернет“, което потребителя подписва при назначаването си в организацията, или някаква друга обща информация, касаеща организацията и условията, при които се ползват нейните информационни ресурси.

След успешно отваряне на сесия (логване в системата) следва да излиза друго съобщение, което вече може да съдържа и по-конкретна информация, например кои ресурси и услуги на системата не са на разположение и до кога, новооткрити уязвимости и заплахи, с които потребителите трябва да се съобразяват и други.

И двете съобщения трябва да са добре композирани и информативни. Дори потребителите да не им обръщат особено внимание, тяхното послание, подсъзнателно, ще им оказва влияние.

3.5.2. Реакция при опит за нерегламентирано влизане в системата.

При наличие на няколко последователни неуспешни опита за отваряне на сесия системата трябва да предприема определени действия, за да намали вероятността неоторизиран потребител (нарушител), по метода на налучкването, да отгатне паролата на реален потребител и да влезе в системата, представяйки се за него. Например, би могло при три неуспешни опита за афтентификация да следва заключване на акаунта за 15 минуни. Освен това, ако в рамките на един астрономически час има, например, пет неуспешни опита, то акаунта да се заключва перманентно, като отключването да може да се направи само с намеса на системен администратор, който преди това да направи съответното разследване защо е имало толкова неуспешни опити за логване.

3.5.3. История на използване на акаунта.

Добра практика е при успешно логване на потребителя да му се показва кога последно е бил в системата и дали през времето от тогава е имало неуспешни опити за автентификация с неговия идентификатор (потребителско име). Така той би могъл да види, ако е имало опит (успешен или не) за неправомерно използване на неговите права от неоторизиран потребител и своевременно да съобщи на системните администратори, които да направят одит (преглед) на логовете от този период с цел анализ на евентуалните щети, нанесени от нарушителя.

Данните за последното успешно логване и за неуспешните опити за логване след него трябва да съдържат минимум следната информация:

- точни дата и час на началото и края на последната успешна сесия;
- точни дата и час на всеки неуспешен опит за логване с идентификатора на потребителя, ако е имало такива;
- работна станция (*IP* адрес), от която е станало последното логване и всеки от неуспешните опити, ако е имало такива.

Историята на използване на акаунта би могла да се предоставя на потребителя по най-различни начини, като: да е налична в началната страница на дадено приложение или вътрешен сайт на организацията; да е част от съобщението, което се показва след успешно логване в системата; да се изпраща като електронно съобщение на вътрешната поща на служителя и т. н.

3.5.4. Ограничения за влизане в системата.

Най-често ограниченията, които се налагат на потребителите по отношение на логване в системата, са по място и по време. Например, може да се направи така, че потребителите да могат да логват в системата само от работните станции на своя отдел, на своя сектор, или даже да се направи ограничение даден потребител да се логва единствено и само от едно конкретно работно място. Може политиките за логване да се конфигурират така, че да не позволяват локално логване, ако потребителя не се намира физически на територията на организацията (съответно, отдалечено логване, ако потребителя е на територията на организацията) и т. н. Пример за ограничение по време е, ако системата не допуска отваряне на сесия в извън работно време или на потребител, който се води в отпуск или временна нетрудоспособност.

За да може да се използва този похват за защита на информационната система е необходимо тя да може да комуникира (или да е интегрирана със) системите за контрол на физическия достъп до сградата и със системата на отдел „Човешки ресурси“, което е пример за значително повишаване на сигурността, в

следствие на комплексното (съвместното) използване на няколко метода за защита на информацията.

3.5.5. Временно спиране на сесията.

Най-добре е потребителят сам да приключи сесията си, ако се налага да напусне работното си място, но понякога обстоятелствата са такива, че може да пропусне или поради спешност да няма време за това. При продължително отсъствие (неактивност) на потребителя системата трябва да може да заключи сесията (без да я спира), като нейното отключване да става с повторна идентификация и автентификация. Времето, за което сработва механизма може да е най-различно, в зависимост от конкретиката на работния процес. Системата трябва да може и да закрие сесията, ако например, отсъствието на потребителя продължи повече от един час след изтичане на работното му време. В такъв случай е добре тя да изпрати уведомление за това до началника на служителя, за да може той да му потърси отговорност за това, че е оставил работното си място с активна връзка към информационната система, което е потенциален риск за сигурността и може да доведе до сериозни последици за организацията.

3.6. Външни връзки, свързване.

Всяка връзка на информационната система с външна мрежа, било то Интернет или друга корпоративна мрежа, е потенциален „вход“ за нерегламентиран достъп от страна на евентуален зложелател. Затова към тези точки следва да се подхожда с особено внимание и стриктност.

3.6.1. Рутери и защитни стени.

Рутерът (*router*) или още, маршрутизатор, анализира информацията от всеки пакет, за да го изпрати по възможно най-късия път до неговата дестинация. Почти винаги в него е вградена и защитна стена (*firewall*), която дава допълнителни възможности за филтриране на трафика. Има два подхода при настройването на защитните стени:

- чрез забранителни списъци – по подразбиране всички пакети се пропускат свободно, с изключение на тези, които отговарят на някой (или комбинация) от критериите, заложени в забранителния списък;
- чрез разрешителни списъци – по подразбиране всички пакети се спират, с изключение на тези, които отговарят на някой (или комбинация) от критериите, заложени в разрешителния списък.

Комбинацията рутер със защитна стена, когато са настроени правилно, е изключително мощно средство за контролиране на трафика в една мрежа. Когато трафикът през рутера е голям, не е желателно да се използва вградената в него защитна стена, защото тя използва оперативния ресурс на вградените в него процесор и памет, което при голям брой правила за обхождане може да доведе до забавяне изпълнението на основната функция на рутера. Затова се препоръчва използването на хардуерно реализирана защитна стена, работеща последователно на рутера.

Когато се настройва дадена мрежа е важно всички рутери в нея да се настройват съгласувано и от човек, който е много добре запознат с материята и с конкретния модел рутер. Неправилното конфигуриране може да доведе до проявата на сериозни уязвимости в сигурността на информационната система, които, ако бъдат установени от евентуален зложелател, могат да имат значителни последици за организацията.

3.6.2. Блокиране на неизползваните портове.

Компютърният порт е виртуална точка, с помощта на която се обработват данните (входящи и изходящи). Това прави портовете изключително важни от гледна точка на сигурността. Всеки един порт, който е наличен за използване, е потенциално слабо място в информационната система. Затова е изключително важно неизползваните портове да бъдат забранени (блокирани), а тези, които не са, да бъдат надеждно защитени срещу нерегламентиран достъп.

3.6.3. Комутируеми връзки по телефон.

Комутируема връзка (*Dial-up access*) е услуга, при която чрез използването на модем, един компютър може да се свърже с друг през телефонната мрежа, за предаване на данни (например, за достъп до Интернет). Характерно за нея е, че се осъществява тогава, когато е необходима и се разпада, когато връзката не се използва. Тя може да предостави абсолютно нерегламентиран и непроследим достъп до информационната система. Това може да стане дори още по-лесно със съвременните смартфони, които имат вградена еквивалентна услуга с много по-добро качество и параметри. Затова е абсолютно задължително да се вземат всички възможни мерки (технически, софтуерни, административни и т. н.) срещу създаването на подобни входно-изходни точки в информационната система.

3.6.4. Виртуални частни мрежи.

Виртуалната частна мрежа (*Virtual Private Network, VPN*) е технология, чрез която могат да се предават данни през публична мрежа по такъв начин, че за участниците това да изглежда сякаш се използва частна защитена локална мрежа. Тя се изгражда върху три основни стълба – тунелиране, криптиране и идентификация.

Тунелирането прави така, че цялата мрежова инфраструктура, намираща се между източника и получателя на данните, остава скрита

(невидима). Тунела предава пакетите между двата си края без да прави никакви промени в тях. Изграждането на такъв тунел е достатъчно, за да се свържат два мрежови възела по начин, по който за всеки софтуер те изглеждат като части от една и съща локална мрежа, въпреки, че данните преминават през неограничен брой междинни рутери на публичната мрежа. Освен това, тунелиращите протоколи осигуряват и криптиране на връзката, така че вероятността за загуба на конфиденциалност на данните, преминаващи през тунела, е значително ограничена (сведена почти до нула).

Сред основните предимства на виртуалните частни мрежи са:

- Спестяване на финансов капитал. С използването на *VPN* отпада необходимостта от използването на скъпи наети линии.
- Високо ниво на сигурност. Чрез използване на разширено криптиране и протоколи за оторизация, *VPN* осигурява най-високо ниво на сигурност и защитава данните от непозволен достъп.
- Мащабност. С помощта на *VPN* организацията може да достъпва свои отдалечени структури чрез услугите на най-обикновен доставчик на интернет. Това дава възможност за голям ръст на способностите, без да се налага добавяне на значителна инфраструктура.
- Мобилност. *VPN* технологията е съвместима с почти всяко съвременно преносимо компютърно и/или комуникационно устройство, което позволява защитена свързаност с информационната система от страна на служителите на терен.

3.7. Телекомуникации.

Защитата на телекомуникациите също е сред основните елементи на сигурността на една информационна система. Важни са подборът на технологиите, които ще бъдат използвани, както и тяхната реализация, последваща поддръжка, ъпгрейд, периодични тествания за уязвимости и анализ. На следващо място е важно да се използват, навсякъде, където това е

необходимо, защитени сесии, посредством криптиращи устройства и софтуер и протоколи с висока степен на надеждност и сигурност. Трябва да има стриктни правила за начините, по които се предава класифицирана и чувствителна информация с ясно разписани процеси, роли и отговорности.

Не на последно място, трябва да се обърне внимание и на защитата на служебната електронна поща. Нейното криптиране може да има огромно значение за информационната сигурността на компанията. Хората изпращат важни данни, без да осъзнават колко дълго те може да престоят в пощенските сървъри и какви може да са последствията, ако съобщенията попаднат в неподходящи ръце. Според водещата фирма в областта на сигурността *Kroll,* около 70% от електронните съобщения, изпратени от офиси, не съществуват на хартиен носител[5], което означава, че евентуалната им подмяна може да се окаже изключително опасна. За тази защита, обикновено, се използват цифрови сертификати (*Public Key Infrastructure*, *PKI*).

3.8. Наблюдение.

Тук се има предвид както физическото наблюдение, така и наблюдението на процесите, изпълнявани в самата информационна система, осъществявано чрез управлението на логовете.

И за двете е от особена важност да има ясна политика. Трябва да е разписана инструкция, която конкретно и методично да описва начините за събиране, съхранение, задържане и унищожаване на данните от наблюдението. Това е важно, тъй като в не редки случаи успешното разследване на различни инциденти минава именно през преглед на данните от физическото наблюдение и/или анализа на логовете от информационната система.

[5] Данните за цитираното изследване са взети от публикация в Интернет: SAGA Technology, „Защита на електронната поща“, *http://sagabg.net/item_5261.html*.

Също така трябва да се прави и периодичен преглед на данните (логовете) от наблюдението, защото така могат да бъдат уловени пропуснати преди това пробиви.

3.8.1. Физическо наблюдение.

Освен класическото видеонаблюдение, физическото наблюдение може да обхваща и проследяването на редица други фактори от физическо естество, като температура, влажност, налягане, електромагнитни излъчвания, радиационен фон, ниво на шума, сеизмична активност и т. н.

За да може да се използват пълноценно данните от физическото наблюдение трябва да има формализиран подробен план, в който да са описани точното местоположение на всеки сензор, датчик и камера, техния обхват (зона на действие), допустимо отклонение (допустима грешка) и други технически данни. Трябва, също така, да се извършва и периодично тестване, както на системата за наблюдение, като цяло, така и на отделните ѝ елементи. При необходимост, системата трябва да може да генерира и предупреждения за застрашаващи събития, ако контекста на дейността на организацията предполага възможността за възникването на такива.

3.8.2. Управление на логовете.

Средството, чрез което може да се направи преглед на отминали събития в информационната система е анализа на логовете, които тя генерира. Логът представлява единичен запис, в който са описани определени параметри на логваното събитие (точна дата и час, какво е самото събитие, обект и субект и т. н.). Кои събития и кои негови атрибути да бъдат логвани е обект на предварителна настройка на системата. Тук правила от рода „колкото повече, толкова по-добре“ или „колкото по-малко, толкова по-добре“ не са приложими, защото прекомерното натрупване на логове неимоверно затруднява тяхната последваща обработка, анализ и съхранение, а събирането на малко на брой и непълни логове може да доведе до недостатъчност на данните, за да се извърши

анализа. Също така, трябва да се има предвид, че обработката на логовете трябва да се извършва машинно, защото обикновено инцидентът, който се разследва (или за който се прави превантивна проверка) е скрит на два до три записа сред няколко стотин хиляди други записи. Затова, при анализ на логове трябва да се използва съответен софтуер, който да филтрира данните по различни критерии.

3.9. Защита от вируси.

Основната защита срещу вируси и други вредни програми се осъществява от така наречения антивирусен софтуер. Силно препоръчително е да се използва лицензирана версия с доказани качества, която да обхваща всички сървъри и работни станции в информационната система. Дефинициите за антивирусната защита следва да се качват автоматично, през определен период от време, но трябва да има възможност и за ръчен ъпдейт при необходимост.

В наръчника за използване на информационната система от потребителите трябва да бъде дефинирана последователност от действия, която да се следва в случай, че бъде открит вреден софтуер. Тя трябва да бъде кратка, ясна и недвусмислена, за да може лесно да бъде запаметена и изпълнена дори от служители с не до там висока компютърна грамотност. Също така е добре програмните продукти, необходими за дейността на организацията, да бъдат лабораторно тествани за вируси и друг вреден софтуер преди да бъдат инсталирани на работните станции и сървъри.

3.9.1. Функции на антивирусния софтуер.

Като цяло, антивирусния софтуер има следните основни функции:

- предпазване от проникване на вреден код – осъществява се постоянно върху всеки файл, който се изпълнява или отваря;
- търсене на вредно съдържание по конкретна заявка на потребителя или при планирано активиране – може да обхваща цялата файлова система, определена папка и нейното съдържание или конкретен файл;

- отстраняване на вреден код, открит в процеса на предпазване от проникване или при търсене – в случай, че антивирусната програма не съумее да възстанови заразения файл до първоначалния му вид то той се премества в така наречената карантинна зона.

9.3.2. Принцип на действие на антивирусния софтуер.

Съществуват множество и най-различни методи за откриване на вреден код, които се използват паралелно в антивирусните пакети. Безспорно, най-популярният от тях е методът на търсене по сигнатури (байтове с уникална последователност). Сигнатурите се конструират от производителя на антивирусния пакет и се предоставят на потребителите на услугата под формата на антивирусни дефиниции. Когато се окаже, че даден файл съдържа в себе си сигнатура на вирус се смята, че той е заразен. Поради непрекъснатата поява на нови и нови вируси и техни модификации се приема, че едно от основните качества на антивирусния софтуер е актуалността на разпознаваните сигнатури, което не рядко се превръща в основен критерий за избор на антивирусен софтуер.

Ето и някои от другите методи за откриване на вреден софтуер:

- Търсене по контролни суми. Това е модификация на търсенето по сигнатури. При него се взима не само сигнатурата, но и контролната ѝ сума и местоположението ѝ в тялото на заразения файл. Това намалява броя на фалшивите сработвания.
- Използване на редуцирани маски. Използването на маски често е усложнено, поради наличието на шифрован код в тялото на вируса.
- Статистически анализ. Анализира се честотата и вида на използваните команди и на база на това се прави извод за вероятното наличие на вирус в изследвания файл.
- Евристичен анализ. При него се използва набор от програми, анализиращи кода на изпълними файлове, макроси, скриптове и т. н.

- Емулация. В специално пригоден за целта буфер се прави емулация на изпълнението на заразената програма. След това от буфера се извлича разшифрованото тяло на вируса, което вече може да се изследва със стандартните методи за откриване на вреден код.
- Статичен метод. При този метод се търсят общи, кратки сигнатури, които са присъщи за големи групи от вируси (т. нар. „подозрителни команди“).
- Динамичен метод. Доста прилича на метода емулация. Прави се емулация на изпълнението на проверяваната програмата и се протоколират всички нейни действия. На база този протокол се преценява дали програмата е компрометирана.

3.9.3. Добри практики при антивирусната защита.

От страна на потребителите:

- Редовно актуализиране на софтуера. Вредните програми често използват уязвимости, които разработчиците на софтуер вече са коригирали.
- Файлове да се теглят само от надеждни сайтове (източници). Като допълнителна мярка, изтеглянето може да се прави на допълнително устройство, например *USB* флашка, след което да се подлага на проверка с антивирусна програма.
- Повишено внимание към неочаквани прикачени файлове или хипервръзки в електронни съобщения.
- Поддържане на добри архивни копия на данни. Като минимум, да се архивират файлове, чиято загуба би била критична.

От страна на администраторите на информационната система:

- Блокиране на определен вид съобщения или прикачени файлове.

- Блокиране на възможността за сваляне на файлове (музика, филми, програми и т. н.).

3.10. Планиране на случайността (непредвидените инциденти).

Планирането на случайни инциденти и редуцирането на последиците от тях е важен елемент от комплексното изграждане на сигурността на една информационна система. Самият израз „непредвидени случаи“ подсказва, че не могат да бъдат обхванати всички негативни сценарии, но все пак има определени групи от мерки, които биха могли да обхванат голяма част от тях.

3.10.1. Политика за резервни копия.

Резервните копия за възстановяване ще бъдат разгледани като отделен елемент на защитата, но тук само ги споменавам, тъй като те могат да изиграят важна роля при справянето с много от непредвидените инциденти.

3.10.2. Договори за поддръжка с доставчици и производители.

В много от случаите поддържането на склад на специфичен хардуер за бърза подмяна при необходимост не е рентабилно. От една страна, това е скъпа техника, която може и да не се наложи да бъде използвана, а само ще стои в склада и ще остарява морално. От друга страна, може да се окаже, че именно в тази техника е била открита уязвимост и тя трябва да бъде спешно заменена с друг модел, при който слабостта е коригирана, което ще утежни допълнително ситуацията, понеже ще трябва да бъдат заменени не само използваните устройства, но и резервните такива.

Нещата при поддръжката на специализиран софтуер (тук не става въпрос за стандартни операционни системи, офис пакети и друг приложен софтуер, чиято поддръжка под формата на регулярни пачове и сървис пакове е подсигурена от разработчиците им в замяна на закупения лиценз за използване, а за софтуер, разработен по поръчка специално за нуждите на компанията) стоят по сходен начин. Освен ако това не е част от основната дейност на организацията,

поддържането на екип от висококвалифицирани специалисти (програмисти), които да отстраняват новооткрити бъгове и слабости в програмния код на системата може да се окаже в пъти по-скъпо от наемането на фирмата-разработчик да извършва тази дейност под формата на абонамент. По този начин организацията ще има отговорности само по администрирането на системата, което така или иначе се извършва от информационния отдел.

С оглед на изложеното по-горе, в много случаи е рентабилно да се сключат договори за поддръжка с доставчици, производители и/или специализирани сервизи, които да обезпечат дейността по поддържането на специфичен хардуер и софтуер. В тези договори трябва да се направи ясно разграничение на поддържаните софтуер и хардуер по отношение на тяхната критичност. За тези с по-висока степен на важност следва да са заложени минимални срокове за реакция и отстраняване на проблема, докато при не толкова важните сроковете може да са по-големи. Така, от една страна се гарантира бързина при справянето с извънредната ситуация, а от друга – в някаква степен се редуцира стойността на поддръжката.

3.10.3. Непрекъсваемост на електрозахранването.

Предвид факта, че всичко в наши дни използва електричество, подсигуряването на неговата непрекъсваемост е жизненоважна по отношение работата на която и да е система. Мерките за постигането на това са много и разнообразни, като е препоръчително съвместното използване на колкото се може повече от тях. Обикновено използваните похвати, подредени в зависимост от тяхната мащабност, са както следва:

- Захранване от няколко външни източници. Сключването на договор за доставка на електроенергия от поне две различни подстанции на електропреносната мрежа ще подсигури непрекъсваемост на електроснабдяването случай на локална авария.

- Резервно захранване от вътрешен източник (генератор). Подсигуряването на непрекъсваемостта на електроподаването може да се реализира и с помощта на бързо сработващ агрегат. В случаите, когато използваните мощности са големи, е удачно да се направи разделяне на захранващата мрежа – критичната инфраструктура се включва към тази мрежа, която е подсигурена от агрегата, докато по-маловажните системи към мрежата, за която не е предвидено допълнително захранване от вътрешен източник.
- Използване на непрекъсваеми захранващи устройства (*Uninterruptible Power Supply, UPS*). Използването на *UPS* за работните станции и особено за сървърите и мрежовото оборудва дава най-малкото три сериозни предимства. Първо, може да подсигури работния процес за определен период от време (от няколко минути до часове, в зависимост от мощността на устройството и потреблението), докато електроподаването бъде възстановено, без това да се отрази на работата на апаратурата. Второ, в случай, че електроподаването не може да бъде възстановено в рамките на времето, за което е предвидено да го прави *UPS*-ът, има възможност за коректно изключване на софтуера и хардуера. Трето, когато електроподаването е налице, *UPS*-ът играе ролята на защита срещу токови удари, което намалява вероятността за отказ на захранващия блок на апаратурата.

3.10.4. План при бедствия и аварии.

Бедствията и авариите, които биха могли да се случат на територията на организацията, могат да са с най-разнороден характер: земетресения; наводнения; пожари; радиационно, химическо и/или бактериологическо замърсяване и т. н. За да може да се справи с подобни ситуации с минимални последствия, организацията трябва да разработи, одобри и сведе до знанието на служителите си План при бедствия и аварии.

Целите на плана са:

- Анализ и оценка на риска от възникване на бедствия и аварии на територията на организацията и около нея.
- Набелязване на необходимите превантивни мерки за редуциране на неблагоприятните последици от бедствията и авариите.
- Организиране и координиране на действия за предотвратяване/намаляване на последиците при вече възникнали бедствия и аварии.

Основните задачи на плана са:

- Анализиране на възможните бедствия и аварии в района на организацията и около него и прогнозиране на последиците от тях.
- Планиране на мерки за предотвратяване/намаляване на последиците от бедствията и авариите, касаещи организацията.
- Разпределение на задълженията и отговорностите между длъжностните лица за изпълнение на мерките за намаляване на рисковете и последствията от бедствията и авариите, засягащи организацията.
- Осигуряване на финансови средства и материални ресурси за ликвидиране на последиците от възникналите бедствия и аварии в района на организацията.
- Задаване на методите на взаимодействие с органите на изпълнителната власт, имащи отношение по предотвратяване на последиците от бедствия и аварии.
- Определяне на реда за навременно уведомяване на личния състав на организацията при възникване на бедствие или авария.

3.11. Поддръжка и експлоатация.

Поддържането на информационната система (софтуер и хардуер), както и правилната ѝ експлоатация, са ключов момент в сигурността. Промените в оборудването (мрежово, сървъри, работни станции и т. н.) трябва да става при обстойна проверка за съвместимост и наличие на скрити уязвимости при взаимодействието на новите елементи със системата. По отношение на софтуера е важно да има обособен полигон (лаборатория), където да се тестват новите продукти (както и актуализациите на съществуващите), преди да бъдат въведени за употреба в реалната информационна система.

Важно е да има разписани процедури за профилактика. Хардуерът трябва да бъде продухван от прах през регулярни периоди от време, да се прави оглед за настъпили продуктови дефекти (например надути кондензатори, наличието на които може да не спре работата на апаратурата, но води до влошаване на работоспособността ѝ) и т. н. По отношение на софтуера също може да се прави регулярна профилактика – проверка за качени ъпдейти и сървис пакове, почистване на темпоралните папки и др.

Също така трябва да се води стриктна документация за извършваната поддръжка. От една страна, тя ще помогне за правилното планиране на последващата поддръжка и профилактика. От друга страна, в случай на инцидент, може да хвърли яснота за това дали причината не е била в неправилна поддръжка и експлоатация. При това положение ще могат да се вземат мерки за избягване на подобен род инциденти в бъдеще.

3.12. Управление на конфигурацията.

Целта е да се определят и контролират компонентите на системата и да се поддържа точна информация за конфигурацията. Управлението на конфигурацията трябва да бъде планирано и разписано като правила (политики), които да обхващат всеки компонент на информационната система: мрежата,

сървърите, работните станции, операционните системи, приложенията, потребителските акаунти и т. н.

Информацията за конфигурацията подпомага планирането и контрола на промените в системата, когато се налагат такива. В тези случаи трябва да има ясно разпределени отговорности по отношение изпълнението на промените, записите на промените и резервните копия, в случай, че се наложи възстановяване на предишно конфигурационно състояние.

Също така, от особена важност е периодично да се извършва проверка на системата за настъпили нерегламентирани промени в конфигурацията ѝ.

3.13. Резервни копия за възстановяване.

Основната цел на резервните копия за възстановяване (*backup*) е да се гарантира, че в случай на загуба на данни и/или услуги, било то поради повреда в оборудването, случайна грешка, умишлена атака или настъпило бедствие, то те ще могат да бъдат възстановени в достатъчен обем и с достатъчна бързина. Нещата (обектите), които основно се архивират, са:

- данни – отделен файл, папка с нейното съдържание, цял логически или физически дял и т. н.; и
- конфигурации – на конкретен приложен софтуер, на операционни системи (на сървъри или работни станции), на мрежови устройства (рутери, интелигентни суичове и др.), на потребителски профили и активни директории и т. н.

Освен за възстановяване, резервните копия могат да се използват и за анализ. Например, ако се знае, че е имало успешна атака срещу информационната система и са били променени елементи от нейната конфигурация, може да се направи побитово сравняване между компрометираната конфигурация и нейния последен *backup*. Така много лесно и

нагледно може да се види какво е било променено и да се направи анализ на целта на атаката.

3.13.1. Политика за резервни копия.

Политиката за резервни копия е разписан от ръководството документ, регламентиращ всички дейности, свързани копията за възстановяване. В нея задължително са описани: точно кои данни и конфигурации подлежат на архивиране; графици за създаване на резервните копия; графици за проверка на възможностите за възстановяване (на какъв период и с използването на какви методи); колко на брой копия, на какви носители и в кои хранилища следва да се пазят; начинът, по който ще се документира всеки един процес, свързан със създаването, съхраненото, използването и унищожаването на копията; отговорните лица и длъжности, свързани с всяка една от изброените по-горе дейности.

Също така, в политиката за резервни копия следва да са разписани и различни планове за действие, даващи бързи и методични отговори на различни въпроси, като:

- Кой следва да извърши възстановяването на данните (конфигурациите) при проблем?
- Може ли лесно и бързо да се възстановят значителни масиви от данни от облака?
- Може ли да се възстанови дадена система на различна хардуерна конфигурация?
- В случай на възстановяване на конкретна система или сървър, има ли неща, които трябва да се донастроят ръчно?
- Възможно ли е възстановеното на няколко системи едновременно?

- Как се процедира, ако лаптоп (или друго преносимо устройство) на служител се повреди, докато е в командировка (извън физическия обсег на екипа по поддръжката)?
- Възможно ли е възстановяването на сървър на друго място? И т. н.

3.13.2. Методи за архивиране.

Методите за правене на *backup* са много и разнообразни, но ще се спра на някои от най-популярните и използвани.

3.13.2.1. Огледален архив (*mirror backup*).

При този метод към твърдия диск огледално се привързва втори. При запис, промяна или изтриване на данни на основния диск, същото действие паралелно се извършва и на втория диск. Като предимство може да се изтъкне скоростта (бърз *backup*, бързо възстановяване). Недостатък е не чак толкова намаления риск от загуба на информация, тъй като двата твърди диска работят едновременно и на едно и също място, което означава, че са подложени на едни и същи външни влияния. Освен това, в случай на грешка или умишлена манипулация, промяната веднага ще бъде отразена и в архивното копие.

3.13.2.2. Пълен архив (*full backup*).

При него се записва цялата информация от цялата система. Основното предимство е бързото и надеждно възстановяване на информацията. Недостатъците са, че архивирането е бавно, а съхраняването на чести пълни архиви изисква значителен обем от свободно пространство.

3.13.2.3. Частичен архив (*incremental backup*).

При него се записват само промените от последния направен архив (пълен или частичен), като през зададен период от време вместо частичен се прави пълен. Например, в неделя (в не работно време), поради ниската му скорост се прави пълен архив. В понеделник се прави частичен архив само на

промените спрямо неделя. Във вторник се прави частичен архив само на промените спрямо понеделник и т. н. до неделя, когато отново се прави пълен архив. Сред предимствата му са, че се прави бързо и не изисква много място. Недостатъците са бавно възстановяване и риска от загуба на информация в случай, че се загуби дори един от частичните архиви.

3.13.2.4. Диференциран архив (*differential backup*)

Много прилича на частичния архив, но със следната разлика: след като се направи пълния архив (в неделя, спрямо по-горния пример), всеки следващ ден се архивира цялата разлика от пълния архив до текущия ден, т. е. в понеделник се архивира разликата от неделя до понеделник, във вторник се архивира разликата от неделя до вторник и т. н. до следващата неделя, когато отново се прави пълен архив. Предимствата са следните: бързо архивиране, използва по-малко място в сравнение с пълния и по-бързо възстановява спрямо частичния архив. Сред недостатъците са по-бавното възстановяване спрямо пълния архив. Също така, ако пълния архив се прави прекалено рядко може да е необходимо значително пространство (не колкото, ако се прави само пълен архив, но доста повече спрямо частичния).

3.13.2.5. Стратегия 3-2-1.

Стратегията 3-2-1 не е метод за архивиране, а по-скоро добра практика, която придобива все по-голяма популярност. 3-2-1 означава, че трябва да се направят поне три копия на архива – едно работно и две резервни. Поне две от тях трябва да са записани на поне два различни типа носителя (външен диск, мрежови диск, *CD/DVD, USB* флаш памет и др.) вътре в организацията, а поне едно да е записано на място извън нея (облачна услуга, нает сървър в дата център и др.).

За това колко е важно да се прави архив говори и изследване, направено по данни на Американското Бюро по Заетост (*US Bureau of Labor*), според което

93% от фирмите, неглижиращи вътрешната си информация, фалират до 5 години[6].

3.14. Етикиране и класификация.

От особена важност за сигурността е как организацията управлява, защитава и разпределя чувствителната си информация. Рамката, в която информационната система осигурява защитата си, се гради на правилното описание на характеристиките на нейните обекти и субекти. Обекти са файловете, директориите и т. н., докато субектите са потребителите, процесите и програмите. След като са налице правилно идентифицираните обекти и субекти, следва да има една съвкупност от правила, която системата да използва, за да определи кога един субект следва (може) да получи достъп до даден (конкретен) обект. За целта се използват понятията:

- потребителски променлив етикет – специфицира нивото на сигурност за даден потребител (субект); и
- файлов чувствителен етикет – специфицира нивото на сигурност, което следва да притежава потребителя, за да има достъп до съответния файл (обект).

Чрез етикетната цялост се гарантира, че обектите и субектите са правилно представени спрямо нивата си на сигурност. В една защитена система трябва да е гарантирано, че информацията, създадена от нея, продължава да има присвоените ѝ защитни механизми през цялото време на нейното съществуване.

Етикети следва да имат още:

- носителите на информация – на един носител не може да се записва информация с по-висока степен на класификация от неговата,

[6] Данните за цитираното изследване са взети от публикация в Интернет: ЛИП Трейд ООД, „Препоръки за добър архив (*backup*) на информацията“, *https://liptrade.eu/препоръки-за-добър-архив-backup-на-информац/*.

както и не може до носителя да има достъп потребител с по-ниско ниво на класификация от това на носителя;

- мрежите, работните станции и сървърите;
- резервните копия за възстановяване; и др.

3.15. Носители на информация.

Организацията трябва да регламентира политика (правила) за начините на използване, съхраняване и унищожаване на носителите на информация. Носителите следва да бъдат надлежно класифицирани, етикирани и описани. Трябва да се водят точни регистри за това кога носителя е бил класифициран, кога и от кого е бил използван и кога е бил снет от употреба (и по какъв начин). Трябва да се следи също кога, как и при какви обстоятелства се правят копия на тези носители, като копията следва да се следят по същия начин, като оригиналите.

Когато един носител трябва да се снеме от употреба (поради морална остарялост, невъзможност за повторната му употреба или друга причина) има няколко подхода, които дават различна степен на гарантираност, че информацията, съхранявана на тях, няма да попадне в неподходящи ръце:

- Изхвърляне. При изхвърлянето на носители няма други съображения за разрушаване. Обикновено се използва за хартиени носители (които се дават за рециклиране), които не съдържат поверителна или чувствителна информация, но може да се използва и за други носители.
- Изтриване. Изтриването следва да защити информацията срещу опит за възстановяване. Обикновеното заличаване не е достатъчно за изтриване, понеже не може да гарантира, че информацията няма да бъде извлечена посредством специализиран софтуер за възстановяване на файлове.

- Прочистване. При прочистването носителите се обработват по начин, защитаващ конфиденциалността на информацията срещу лабораторни атаки. При определени носители, изтриването не е достатъчно за прочистване.
- Разрушаване. Става дума за физическо унищожение на носителите. Може да стане чрез дезинтеграция, изгаряне, разпрашаване, раздробяване, смилане и др.

3.16. Физическа среда и обкръжение.

Физическата защита на информацията има за цел предотвратяване на несанкциониран достъп до сгради, съоръжения и помещения, предотвратяване на кражби, повреждане или компрометиране на активи, както и осигуряване непрекъснатост на дейността на организацията. Тя се реализира чрез комплекс от технически средства и организационни мерки.

3.16.1. Организационни мерки за физическа защита.

Дефинират се зони като: периметър; сгради; паркинги; зони за посетители (приемни); зони за сигурност; помещения с ограничен (контролиран) достъп; входно/изходни точки (ежедневни и аварийни) и др. За всяка една от тези зони се регламентира кой следва да има достъп и по какъв начин ще се контролира този достъп.

За сървърите и мрежовото оборудване се определят: защитени помещения; зона за сигурност; мерки за ограничение и контролиране на достъпа; климатично и противопожарно оборудване и т. н.

Видеонаблюдението на различните зони и силите за охрана и реагиране също са неразделна част от мерките за осигуряване на сигурността.

Друг важен елемент от организационните мерки за физическа сигурност е работата с посетители (външни лица). Разрешенията за посещения следва да се издават на база заявки, имащи минимум следните атрибути: цел на

посещението; време; място; отговорник (за посетителя от страна на организацията); придружител (може да е същото лице, което е и отговорник). Трябва да се водят дневници на: заявките за влизане; разрешенията за влизане и самите посещения.

Трябва да има възможност за бързо и точно идентифициране (например посредством баджове или карти за достъп) на: персонал; посетители и сили за охрана и реагиране.

3.16.2. Технически средства за физическа защита.

Сред основните технически средства са физическа защита са:

- ключалки, шкафове, метални каси, сейфове и др.;
- оборудване в помещенията и зоните с контролиран достъп;
- различните устройства за контрол на физическия достъп;
- средствата за защита на периметъра;
- системите и средствата за предизвестяване и гасене на пожари;
- различни детектори за метали, химически вещества, взривни вещества и др.

3.17. Персонална сигурност.

Персоналната сигурност е комплекс от различни организационни мерки спрямо физическите лица, които обработват или имат какъвто и да е досег до подлежаща на защита информация, информационен ресурс или услуга.

3.17.1. Основни мерки за персонална защита.

- Познаване на нормативната уредба в предметната област – служителите трябва да притежават необходимите квалификация и опит за дейностите и отговорностите, с които са натоварени, по отношение опазването и сигурността на информацията.

- Познаване на политиката за сигурност на организацията, както и другите ръководства за защита – служителите следва да са се запознали с всички вътрешни документи, свързани със сигурността и защитата на информацията, преди да бъдат допуснати да работят с информационната система и нейните данни, процеси и услуги.
- Знания за опасностите за подлежащата на защита информацията – служителите на организацията трябва регулярно да бъдат осведомявани за новооткрити заплахи за сигурността и за мерките, които следва да предприемат, за да не станат тяхна жертва.
- Споделяне на критична информация между служителите – споделянето на критична и чувствителна информация (идентификатори, пароли, графици на охраната и др.) между служителите следва да е абсолютно забранено. Ако даден служител трябва да знае нещо, то той следва да бъде запознат по съответния ред.
- Съгласие за неразпространение на информация (включително за определен период след излизане на лицето от структурите на организацията) – възможността за търсене на наказателна отговорност заради издаване и/или разпространяване на чувствителна и/или класифицирана информация има силен възпиращ ефект срещу недоволни настоящи и бивши служители, които имат желание да уронят авторитета и престижа на организацията или да ѝ нанесат материални загуби, издавайки нейните тайни, тактики, методи и стратегии на конкурентни организации.
- Обучение и тренировка – това направление ще бъде разгледано като отделен метод за защита на информацията.
- Периодични проучвания на персонала – трябва да е съобразено с местното законодателство (например, в България лицето трябва да даде изрично писмено съгласие, за да бъдат проучвани банковите му сметки). Проучването може да разкрие различни факти за служителя,

които косвено или пряко да подсказват за съмнителни практики (например, наличието на необяснимо голяма разлика между доходите и стандарта на живот води до подозрения за корупция).

3.17.2. Основен принцип на персоналната сигурност.

Мерките за персонална защита гарантират достъпа до информация, подлежаща на защита, само на лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да се знае“.[7]

3.18. Обучение, тренировка и осъзнаване (убеждение).

Друг важен елемент на сигурността е квалификацията на служителите на организацията. Преди назначаването на всеки служител, отдел „Човешки ресурси“ трябва да изиска от него всички дипломи и сертификати, които се изискват за длъжността, за която той кандидатства, както и да провери тяхната легитимност. Вече назначените служители също подлежат на допълнителна квалификация и повишаване на уменията под формата на различни обучения. Те може да са в няколко разновидности:

- обучения под формата на курсове, целящи усвояването на определени знания и умения, свързани със спецификата на работата на конкретния служител, както и със сигурността на информацията като цяло;
- регулярни инструктажи, целящи периодичното припомняне и актуализиране на определени знания и умения (например, годишен инструктаж за прилагането на закона за защита на класифицираната информация);

[7]Дефиницията е взета от печатно издание: Веселин Целков и Орхан Исмаилов, „Сигурност на информацията“, страница 67.

- съобщения и инструкции, целящи уведомяване на служителите за новооткрити заплахи и уязвимости на информационната система.

Друга, нерядко използвана форма за придобиване и затвърждаване на умения, е тренировката. Симулирането на определена кризисна ситуация и обиграването на реакцията спрямо нея може да е много по-ефикасен метод за обучение от който и да е курс или инструктаж.

Не на последно място, вътрешната убеденост на всеки служител за необходимостта и правилността на мерките за безопасност и защита на информацията, които се изисква той да спазва и съблюдава, е от изключително значение. Може да са наложени и най-добрите световни практики, но ако персоналът не схваща тяхната необходимост и значимост то те, обикновено, са неефективни. Например, наложено е правило за използване на комплексни, машинно генерирани пароли. Ако служителят не разбира смисъла от това и не желае да се съобрази с изискванията за сигурност, той може да вземе комплексната си, машинно генерирана парола, да я запише лист хартия и да го залепи на стойката на монитора си. Това не само, че ще елиминира положителния ефект от използването на сложната парола, но и ще влоши още повече нещата, спрямо варианта, при който служителят използва за парола името на кучето си или рожденната дата на детето си, които би запомнил без проблем.

Организацията трябва да положи всички необходими усилия, за да обучава, тренира и убеждава своите служители в добрите практики, които е приела да следва и в правилата и политиките, които е наложила.

3.19. Управление на риска за информационната сигурност.

Управлението на риска за информационната сигурност е сложен и комплексен процес, в който участват както собствениците и висшето ръководство, така и обикновените служители на организацията. За да се реализира, трябва да бъдат установени: рамка на риска; оценка на риска; реакция на риска и наблюдение на риска.

3.19.1. Рамка на риска.

Основната цел на рамката е чрез нея да бъде създадена стратегия за управлението на риска, да бъдат определени отговорностите, свързани с него и риска да бъде контролиран. За да бъде рамката правдоподобна и реалистична, то организацията следва да идентифицира:

- предположения за риска – възможните уязвимости, заплахи, въздействия и последствия за организацията;
- ограничения за риска;
- допустимост на риска – до каква степен (ниво, праг) даден риск е допустимо да бъде приет;
- приоритети и компромиси.

3.19.2. Оценка на риска.

Оценката на риска трябва да бъде направена съобразно приетата рамка на риска. Следва (вече конкретно) да се идентифицират:

- кои са заплахите за организацията;
- кои са нейните уязвимости, било то външни или вътрешни;
- вредата, която организацията би понесла, ако дадена заплаха съумее да се възползва от една или повече уязвимости и каква е вероятността това да се случи;
- самото изчисление на риска, като степен на вреда и вероятност тя да бъде нанесена.

За да се направи изчислението е необходимо организацията да определи и да е наясно със:

- средствата, техниките и методологията, с които се оценява риска;
- възможните ограничения, свързани с тази оценка;
- ролите и отговорностите, свързани с риска;

- начините, по които необходимата за оценката на риска информация ще бъде събирана, обработвана и обменяна;
- как самата оценка ще бъде използвана от организацията;
- на какъв период от време и/или при какви конкретни обстоятелства ще бъде правена оценка на риска;
- какви ще са източниците и методите, които ще се използват, за определянето на заплахите.

3.19.3. Реакция на риска.

Това е начинът, по който организацията ще отговори на риска, когато той вече е идентифициран и му е направена оценка. Целта е осъществяването на систематизиран и широкомащабен отговор на риска, който кореспондира с рамката на риска чрез:

- изработване на алтернативни мерки за реакция на риска;
- оценка и сравнение на тези мерки;
- избиране на тези от тях, които не са в противоречие с приетия от организацията праг за допустим риск;
- прилагане на избраните мерки за отговор на риска.

За да е успешна реакцията на риска, организацията следва подробно да опише възможните видовете мерки за реакция. Също така средствата, техниките и методологията, чрез които тези мерки се разработват, сравняват и избират.

3.19.4. Наблюдение на риска.

Организацията трябва да осъществява непрекъснато наблюдение (мониторинг) на риска. Целите на това наблюдение са:

- да потвърди дали избраните мерки за отговор на риска са приложени и дали са спазени изискванията за информационна сигурност;

- да определи доколко избраните мерки са ефективни и ефикасни;
- да следи за промени в средата, които биха довели до промяна на резултатите от оценката на риска.

3.20. Системи за откриване и предотвратяване на атаки.

Системите за откриване и предотвратяване на атаки (*Intrusion Detection and Prevention Systems, IDPS*) не са метод за защита, а изключително мощно средство (инструмент), което може да обедини в себе си редица методи за защита и използвайки ги съвместно (комплексно) многократно да увеличи тяхното индивидуално действие (ефективност и ефикасност). По принцип това са две различни системи, които могат да работят по отделно, да работят заедно или да са интегрирани една с друга в един общ продукт.

3.20.1. Системи за откриване на атаки.

Системите за откриване на атаки (*Intrusion Detection System, IDS*) са инструмент за видимост (мониторинг). *IDS* наблюдава трафика от страната на мрежата и дава информация за състоянието на сигурността в мрежата. Тя се ползва от мрежовия инженер за задълбочен преглед на мрежата и дава възможност да се види какво се случва в нея в големи детайли. Информацията от *IDS* помага за разкриването на:

- Нарушения в политиката за сигурност на информацията (например, системи или потребители, които са стартирали непозволени приложения).
- Инфекции (вируси, троянски коне и др.), които имат частичен или пълен контрол върху вътрешни системи.
- Изтичане на информация (в следствие на инсталиран шпионски софтуер, записвачки на клавишни натискания и др.), както и случайно изтичане на информация от обикновени потребители.

- Грешки в настройките на конфигурацията, които намаляват производителността на мрежата, като и погрешно конфигурирани защитни стени.
- Неоторизирани клиенти или сървъри, както и инструменти за сканиране на мрежата.

3.20.2. Системи за предотвратяване на атаки.

Системите за предотвратяване на атаки (*Intrusion Prevention System, IPS*) най-лесно могат да се сравнят със защитна стена, но работеща не на принципа „пропусни, ако намериш съвпадение“, а на принципа „спри, ако намериш съвпадение“. *IPS* има правила (може да са стотици или дори хиляди), повечето от които са от вида „блокирай този познат проблем за сигурността“. Когато даден пакет достигне *IPS,* системата преглежда списъка си с правила в търсене на основание да го спре. Ако не намери такова, в края на списъка има правило „пропусни всичко“, което дава основание на системата да го пропусне през себе си.

IPS са контролиращи устройства и за разлика от *IDS*, те се намират на линията между две мрежи, като контролират трафика, обменян между тях, т. е. *IPS* е част от механизмите на политиката за сигурност. Те внедряват или налагат определена политика, според която не се позволява на определен трафик да премине.

Основната задача на *IPS* е да блокира познатите атаки в рамките на мрежата. Когато е налице нов начин за пробив, а системата все още не е пачната срещу този вид атака, *IPS* е добър инструмент за бързо блокиране на атаки и по-специално на тези, използващи базови и добре познати техники за пробив.

IPS могат да предлагат и други услуги, като: ограничаване на скоростта (което е полезно при справяне с атака за отказ на услуга); инструменти за налагане на политики; инструменти срещу изтичане на данни; инструменти за

откриване на аномалии и др., но винаги ключовата функция на *IPS* е да контролира.

3.20.3. Системи за откриване и предотвратяване на атаки.

Системите за откриване и предотвратяване на атаки (независимо дали са реализирани като две отделни, съвместно работещи *IDS* и *IPS* или една система, която интегрира в себе си и двете – *IDPS*) осигуряват: идентифициране на настъпили и потенциални инциденти; детайлното им описване и даване на справки, обобщаващи наблюдаваните събития; действия за неутрализирането и предотвратяването им; своевременно предоставяне на сведения за тези процеси на администраторите по сигурността и др. В допълнение на основните си функции, *IDPS* могат да служат и за идентифициране на проблеми, свързани с политиките за сигурност на организацията, документиране на съществуващите заплахи и, не на последно място, за обезкуражаване на лица, правещи опити за нарушаване на мерките за информационна сигурност. Освен това, те могат да се използват и за идентифициране на разузнавателни действия, което е сериозен индикатор за предстояща атака.

Изводи от трета глава.

1) Информацията е актив, който, като всеки друг актив, е от значение за организацията и трябва да бъде подходящо защитен, независимо от начина, по който се съхранява (дигитален, материален или под формата на знания и умения на персонала).
2) Съвместното (комплексно) планиране, внедряване, управление и използване на подходите и методите за защита на информацията значително повишава тяхната ефективност и надеждност.
3) Методите за защита трябва да се използват по начин, при който в случай на компрометиране на един от тях това да не води до компрометиране на цялата система за сигурност.

ЗАКЛЮЧЕНИЕ

Разгледаните методи за защита на информацията и информационните системи дават решения срещу различни групи заплахи за сигурността. Въпреки това, използването им по отделно (на парче) не би било особено ефективно, особено в случай на комбинирана атака, използваща повече от една уязвимост и група от различни по вид подходи за неоторизиран достъп. Методите за защита трябва да бъдат планирани и използвани заедно (комплексно) през целия жизнен цикъл на информационната система, като ключова роля за това играе политиката за информационна сигурност на организацията. Хората, изграждащи, внедряващи и поддържащи системата за информационна сигурност, трябва да са наясно, че една свързана инфраструктура предоставя много по-високо ниво на сигурност и при значително по-ниски разходи за поддръжка, отколкото покупката и инсталирането на отделни, независими решения, били те и най-добрите в своята област на действие и клас.

Изводи.

1) Извършен е анализ на способите и методите за несанкциониран информационен достъп. Дефинирани са особеностите на тези методи и са разкрити слабите им места от гледна точка на превенция и защита.
2) Изследвани са съществуващи методи за осъществяване на неоторизиран достъп до компютърно обработвана информация. Разкрити са техни особености от гледна точка на превенция и защита.
3) Анализирани са и са оценени съществуващи методи и подходи за осъществяване на комплексна информационна защита. Дадени са техни характеристики и са разкрити особеностите им от гледна точка на тяхното използване.

4) Разработена е методика за реализиране на комплексна защита на информацията. Предложен е качествен модел за оценка на реализираната информационна защита.

Препоръки.

1) При изграждането на системата за защита на информацията да се следват добрите практики, препоръчани в стандартите за информационна сигурност и управление на информационни системи и услуги.
2) Да се прави регулярен анализ на заплахите и рисковете за информационните ресурси и услуги, предоставяни от информационната система, за да може своевременно да се реагира на променящата се среда, в която тя функционира.
3) Системата за защита на информацията да се изгражда успоредно със самата информационна система и, когато е възможно, да бъде част от нея, като подсистема, за да се гарантира нейната съвместимост и безотказност.
4) Да има добра координация между отдел „Човешки ресурси“ и администраторите на информационните системи, за да може своевременно да се реагира при напускане/назначаване/преместване на служители по отношение на отнемането/предоставянето/промяната на съответните им права за достъп.
5) Да се следят световните новости в областта на защитата от нерегламентиран достъп, за да може да се вземат адекватни превантивни мерки срещу новите заплахи и уязвимости.
6) Да се правят периодични тестове на сигурността от независими специализирани органи и на база докладите от тях да се правят съответните промени за подобряване качеството на информационната защита.

СПИСЪК НА ИЗПОЛЗВАНИТЕ ИЗТОЧНИЦИ

Източници от печатни издания:

1. Йоцов, В. Изкуствен интелект и експертни системи. За буквите – О писменехь. София. 2014. 232 с. ISBN 978-619-185-033-4.
2. Начев, А. Технически средства и системи за защита на информацията. За буквите – О писменехь. София. 2014. 231 с. ISBN 978-619-185-126-3.
3. Семерджиев, Ц., Н. Митев. Информационна сигурност. Софттрейд. София. 2015. 316 с. ISBN 978-954-334-173-3.
4. Семерджиев, Ц., Н. Митев. Норми и стандарти за управление на информационните системи. Софттрейд. София. 2014. 304 с. ISBN 978-954-334-162-7.
5. Целков, В., Н. Стоянов, О. Исмаилов. Международни стандарти и добри практики за защита на информацията. За буквите – О писменехь. София. 2010. 235 с. ISBN 978-954-8887-68-7.
6. Целков, В., Н. Стоянов, О. Исмаилов. Управление на риска, тестване и оценка на мрежовата и информационна сигурност. За буквите – О писменехь. София. 2015. 250 с. ISBN 978-619-185-159-1.
7. Целков, В., О. Исмаилов. Сигурност на информацията. За буквите – О писменехь. София. 2017. 216 с. ISBN 978-619-185-253-6.

Уеб базирани източници:

8. Дончев, Румен. Политика за мрежова сигурност. *http://profisec.bg/484/politika-za-mrezhova-sigurnost/*. Посетен на 25 март 2018.
9. Михайлов, Иван. Класификация на мрежовите атаки. *https://ivodoc.wordpress.com/2010/01/25/класификация-на-мрежовите-атаки/*, 25 януари 2010. Посетен на 25 март 2018.

10. Лазова, Виктория. Едва 3% разпознават фишинга в имейла си. *http://cio.bg/7252_edva_3_razpoznavat_fishinga_v_imejla_si/*, 29 юни 2015. Посетен на 25 март 2018.
11. ЛИП Трейд ООД. Препоръки за добър архив (*backup*) на информацията. *https://liptrade.eu/препоръки-за-добър-архив-backup-на-информац/*, 10 октомври 2016. Посетен на 06 април 2018.
12. ESET Internet Security. *https://help.eset.com/eis/10/bg-BG/index.html*. Посетен на 03 април 2018.
13. Microsoft. Най-добри практики за защита от вируси. *https://support.office.com/bg-bg/article/Най-добри-практики-за-защита-от-вируси-d64131a8-b0ef-4bc5-9ba0-8a5cb42684dd*. Посетен на 04 април 2018.
14. PC WORLD. Що е то VPN. *http://pcworld.bg/12368_shto_e_to_vpn*, 30 април 2009. Посетен на 03 април 2018.
15. SAGA Technology. Защита на електронната поща. *http://sagabg.net/item_5261.html*, 10 февруари 2003. Посетен на 04 април 2018.
16. SAGA Technology. Знаем ли кога се нуждаем от IDS, IPS или от двете заедно. *http://review.sagabg.net/znaem-li-koga-se-nuzhdaem-ot-ids-ips-ili-ot-dvete-.html*, 12 август 2009. Посетен на 08 април 2018.

СПИСЪК НА ИЗПОЛЗВАНИТЕ СЪКРАЩЕНИЯ

Съкращения на български език:

АТЦ – автоматична телефонна централа;

ГИМ – главен информационен мениджър;

ПЕДН – паразитни електродвижещи напрежения;

ПЕМВ – паразитни електромагнитни вълни;

ПИС – политика за информационна сигурност;

СИС – служител по информационна сигурност;

СМА – системен и мрежови администратор;

Съкращения на английски език:

DDoS – Distributed Denial of Service (разпределена (атака) за отказ на услугата);

DoS – Denial of Service (отказ на услугата);

GSM – от названието на групата Groupe Spécial Mobile, по-късно преименувана на Global System for Mobile Communications;

ICMP – Internet Control Message Protocol (протокол за контрол на съобщенията);

IDPS – Intrusion Detection and Prevention Systems (системи за откриване и предотвратяване на атаки);

IDS – Intrusion Detection System (системи за откриване на атаки);

IP – Internet Protocol (интернет протокол);

IPS – Intrusion Prevention System (системи за предотвратяване на атаки);

ISP – Internet Service Provider (доставчик на интернет услуги);

FTP – File Transfer Protocol (протокол за прехвърляне (предаване) на файлове);

HTML – Hypertext Markup Language (език за маркиране на хипертекст);

LAN – Local Area Network (локална мрежа);

MitM – Man in the Middle (човек по средата);

MTU – Maximum Transmission Unit (максимална единица за предаване);

PKI – Public Key Infrastructure (цифров сертификат);

SMS – Short Message Service (услуга за кратки съобщения);

TCP – Transmission Control Protocol (протокол за контрол на предаването);

VPN – Virtual Private Network (виртуална частна мрежа);

UPS – Uninterruptible Power Supply (непрекъсваемо захранващо устройство).