УНИВЕРСИТЕТ ПО БИБЛИОТЕКОЗНАНИЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

КАТЕДРА ”НАЦИОНАЛНА СИГУРНОСТ”

СПЕЦИАЛНОСТ «ИНФОРМАЦИОННА СИГУРНОСТ»

ДИПЛОМНА РАБОТА

на тема:

СРЕДСТВА, МЕТОДИ И ДОБРИ ПРАКТИКИ ЗА ЗАЩИТА НА КОМПЮТЪРНИТЕ СИСТЕМИ И МРЕЖИ

Дипломант:
Самуил Нинов
задочно обучение
Ф.№ 158-СЗ

Научен ръководител:……
(доц. Николай Митев)

София
2018

Нинов, С. Средства, методи и добри практики за защита на компютърните системи и мрежи. Научен ръководител доц. Н. Митев. С. 2018. Катедра „Национална сигурност“. Бакалавърска програма „Информационна сигурност“. УНИБИТ. 69 с.

Брой източници – 25.

Цели на дипломната работа са описание на най-често срещаните атаки, застрашаващи съвременните компютърни системи и мрежи, дефиниране на атакуващия вектор и представяне на възможни решения за справяне с тези атаки. След разглеждане на определени методи и средства за превенция и защита срещу злонамерени действия, работата представя конкретни добри практики за намаляване вероятността от атака, както и ограничаване на щетите при извършена успешна такава.

Ключови думи: атака; достъп; защита; информация; мрежи; потребител; сигурност; системи; услуга; уязвимост.

Съдържание:

Увод

Както в реалния свят, така и във виртуалния съществуват заплахи за неговите обитатели или както е обяснено в един от експериментите, проведен от Кевин Рууз [3] на DefCon[1] – „всички знаем, че съществуват хора, които са майстори на бойните изкуства, и ако решат, няма какво да ги спре от това да ни нападнат, евентуално да ни набият и на момента няма какво да направим, за да ги спрем“. Същото важи и за всички наши електронни устройства, свързани с Интернет, били те лаптоп, смартфон, таблет или след навлизането на Internet of Things – дори домашните електроуреди. Съществуват хора, които са достатъчно вещи в манипулирането на компютърни мрежи и системи, така че решат ли да ни нападнат, няма какво да направим, за да попречим на атаката, ако изобщо разберем за нея.

Във всяка една организация или частен дом до по-голяма или по-малка степен хората се стремят да постигнат сигурност на своите данни, било то бизнес данни или снимки, които са направили през изминалото лято. Поне веднъж всеки човек индивидуално се е замислял за това какви заплахи съществуват и се експлоатират, какви уязвимости крият устройствата ни, какъв е шансът точно нашето устройство да попадне под ударите на хакерите. Рядко обаче хората използват термини като уязвимост, заплаха, риск и т.н. правилно. Затова ще ги дефинираме, така че да придобием представа какво стои зад тези наименования, започвайки от активите.

Активите [4] са всичко, което има стойност за организацията, нейните бизнес операции, включително информационните ресурси, на които се крепи мисията ѝ. Заплахата е всеки случай, независимо дали умишлен или неволен, който има потенциала да навреди на организацията или лицето чрез отказ на услугата, неоторизиран достъп, унищожаване, промяна или разкриване на информация. Уязвимостта представлява слабост на актива. Било то фабричен дефект при неговото производство или допусната грешка при внедряването на този актив в дадена система, тази слабост може да доведе до нежелано и

[1] DefCon – една от най-големите „хакерски“ конвенции, провеждаща се всяка година в Лас Вегас, САЩ.

неочаквано компрометиране на сигурността на компютърните системи, мрежи, приложения или използвани протоколи. Експлойт е софтуерен код или поредица от команди, които се възползват от конкретна уязвимост в хардуерна или софтуерна компютърна система и предизвикват неочаквано или нежелано поведение на системата. Рискът на свой ред е потенциалът на дадена заплаха да експлоатира някоя уязвимост на актив или група активи и да причини вреда на организацията или лицето, притежател на актива. Казано с други думи – активът е това, което се опитваме да предпазим, заплахата е това, от което се опитваме да се предпазим, уязвимостта е „дупката“ в нашия опит за защита, а рискът е мястото, на което се пресичат активите, заплахите и уязвимостите.

Информационната сигурност и в частност защитата на компютърните системи и мрежи е частта от информационните технологии, която се развива най-бързо и всеобхватно през последните години. Актуалността на темата е призната във всички сфери на бизнеса и нейното изследване представлява предмет на интерес на все повече съвременни научни дейности.

Актуалност и мотивировка:

В съвременния свят всяка една корпорация, както и всички правителствени организации събират, съхраняват, обработват и обменят информация по електронен път чрез дигитални средства или чрез Интернет. В чести случаи тази информация е със статут на конфиденциална или привилегирована информация, което я прави интересна за трети лица. В най-общия случай тези лица търсят постигане на лична облага, използвайки тази информация. Със зачестилото използване на информационните технологии във всички сфери на бизнеса, прозорецът за проникване от злонамерени лица нараства, съответно нараства и необходимостта от защита на периметъра, мрежите, системите и информацията в тях. Заучените положения за защита и конвенционалните методи работят, но не достатъчно добре. За да можем качествено да защитим своите активи, трябва добре да познаваме анатомията на атаката – какви са типовете, как се осъществяват и т.н.

Целта на настоящия материал е да опише най-често срещаните атаки, които застрашават съвременните компютърни мрежи и системи, да опише

атакуващия вектор, както и най-разпространените в тези системи и мрежи уязвимости. Разгледани са методи и средства, които могат да бъдат използвани за превенция и защита срещу злонамерени действия. Описани са и съвременни добри практики за намаляване вероятността за успешна атака, както и за ограничаване на щетите при успешна такава.

Задачи:

- Запознаване и анализ на кибератаките срещу компютърни системи, случили се през последните години;
- Описание на методи за превенция на различни типове атаки, комплексна защита;
- Посочване на примерни средства, които могат да бъдат внедрени и използвани, за осигуряване на конфиденциалност, интегритет и цялостност на информацията;
- Описание на начините за внедряване и приложение на вече утвърдени добри практики.

Обект на настоящата дипломна работа е изследването на някои от най-мащабните компютърни атаки, осъществени до момента, както и посочване на евентуални мерки за защита, които могат да бъдат предприети срещу подобни действия в бъдеще.

Предметът на материала е да запознае с уязвимостите и експлойтите, използвани за компрометиране на компютърните системи и мрежи, както и методите за намаляване мащаба на щетите, които атаките могат да нанесат. Без адекватно познание на видовете атаки е невъзможно изграждането на реалистична представа за евентуалните бъдещи такива и за това как да се предпазим от тях.

Методиката включва емпирични методи като наблюдение, сравнение и измерване, както и някои емпирико-теоретични методи – анализ, синтез, индукция, дедукция, верификация. Събрана е първична теоретична информация, установени са общите и различните аспекти на разглежданите заплахи, а като краен резултат е търсенето на обобщени емпирични факти. Изследването на изброените заплахи е осъществено посредством сегментиране на общите

понятия в отделни компоненти и последвало обединяване на тези компоненти с оглед установяване начина на мислене на атакуващите, както и вектора на атака. Получените данни определят актуалните проблеми, свързани с кибератаките, което помага за намирането на подходящи решения за тях. От друга страна тези решения могат да се превърнат в основа на евентуална по-усъвършенствана методология за справяне с кибератаките в бъдеще.

Глава първа: КОМПЮТЪРНИ АТАКИ И ВЕКТОР НА АТАКАТА

1.1. Основни типове компютърни атаки

Компютърната атака представлява злонамерено действие срещу компютърна система и/или мрежа с цел отказ на услуга, извличане на информация, манипулация на данни, изтриване на информация и други. В най-общия случай основна цел на компютърните атаки е, но не се ограничава до, парична облага за атакуващия. Други подбуди за атака биха могли да бъдат дестабилизация, шпионаж, хактивизъм[2] или дори форма на отмъщение.

Според мотивацията, извършителите на киберпрестъпленията биват крадци, шпиони, хактивисти и лица, раздухващи слухове (т.нар. whistleblowers).

Крадците могат да атакуват както обикновени хора или корпорации, като най-често компютърните атаки са насочени към големи групи потребители. Често подходът им може да бъде засечен и по-нататък ще разгледаме начините, които използват.

Шпионите могат да бъдат измамници, конкуриращи се компании или правителства. Тяхна цел са научно-изследователска дейност, финансови, търговски или стратегически данни. Оттам може да се ескалира към кражба на самоличност, извличане на банкови данни, кражба на лична информация, локализиране на местоположение в реално време, обири и други.

Хактивистите, от друга страна, осъществяват атаки, за да се опитат да наложат техните политически убеждения. Често тяхната цел е свързана със свобода на словото, човешки права или просто негодуване срещу монопола. Подходите и атаките, които използват обикновено, са DoS атаки или обезобразяване на сайт, като заменят съдържанието на дадения сайт с подбрано от тях такова. Пример за хактивисти са групите Anonymous или Wikileaks.

Лицата, раздухващи слухове, не осъществяват атаки, за да получат парично обезпечение. Обикновено тяхната цел е да изобличат някаква измама или неправда, която те смятат за такава. В съвременния живот това се пренася и

[2] Хактивизъм – сложна дума, създадена от думите хакер и активизъм. Представлява злонамерено използване на компютърни технологии за постигане на политически цели.

във формата на атаки над компютърни мрежи и системи. Най-известното лице, което успя да изнесе, разпространи и разобличи информация в последното десетилетие е Едуард Сноудън.

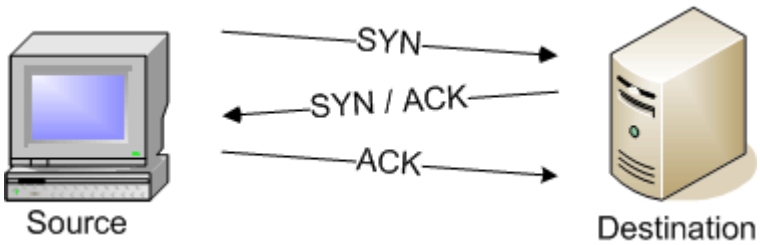
В крайна сметка, независимо от целта и мотива на нападателите, и независимо дали са срещу компютърни терминали, информационни, индустриално контролни системи, мрежата или приложния слой, атаките основно се делят на DoS атаки, man-in-the-middle (MitM), malware атаки, XSS (cross-site scripting) и социално инженерство.

1.2. Denial of Service (DoS) атаки

Атаки от типа „отказ на услугата“ (DoS), независимо от начина, по който са извършени, целят да прекъснат нормалната работа на системата, която е цел на атаката. Най-често те се осъществяват като атакуващия претрупва целта със заявки, така че сървърът поемащ заявките, да изчерпи целия си наличен ресурс. По този начин, при опит на потребител да достъпи информацията, налична на този сървър, заявката няма да бъде обработена, понеже няма да има достатъчно ресурс, за да му бъде върнат отговор. Разновидност на DoS атаката е DDoS (Distributed Denial of Service), при която „наводняването“ със заявки идва от много устройства. Обикновено това са устройства, които не принадлежат на атакуващия, а са устройства на потребители, които не подозират, че машините им изпращат заявки към сървъра или ресурса, цел на атаката. Такива заразени устройства се наричат „зомбита“, а мрежата от тези устройства – „зомби мрежа“. Съществуват много видове DDoS атаки, но основно се разделят на три категории:

- Volume Based Attacks – изпращат се голямо количество заявки, при което се достига лимита на трафика, който услугата може да понесе. Когато той е достигнат, новите заявки на потребителите няма да бъдат допускани.
- Protocol Attacks – това са заявки, които са насочени към инфраструктурните елементи (защитни стени, системи за разпределение на натоварването и т.н.). Пример за подобна атака е SYN flood атаката. При установяване на връзка между потребител и сървър чрез TCP се използва т. нар. three-way-handshake или казано иначе необходими са три стъпки. Клиентът

изпраща SYN до сървъра, в отговор сървърът изпраща SYN-ACK до клиента и накрая клиентът изпраща обратно ACK, като по този начин се потвърждава изградената връзка (фиг. 1.). При осъществяване на SYN flood атака, атакуващият изпраща SYN, сменя IP адреса си с фалшив, сървъра връща SYN-ACK на фалшивия адрес и никога не получава финалния ACK обратно. По този начин сървърът изпраща SYN-ACK заявки, които никога не биват потвърдени, и при достигане на достатъчно голям брой полуотворени връзки, ресурсите се изчерпват и новите, реални потребители не могат да осъществят връзка със сървъра.



Фиг. 1. TCP Three-Way-Handshake

➢ Application Layer Attacks – основна цел на тези атаки са приложенията и обикновено предсатвляват насочени атаки. Извършват се множество заявки към дадено приложение, при което тези заявки изглеждат като идващи от реални потребители. Целта е да се деактивира функционирането на точно определена услуга, предлагана от приложението, което от своя страна затруднява потребителите, които искат да я използват по предназначение.

Най-мащабната DDoS атака, виждана до момента, датира от септември 2016 година. Използвани са над 145 хиляди устройства, които са изпращали заявки към френската хостинг компания OVH. Според снимка, публикувана от собственика на компанията (фиг. 2.), атаките са били няколко по едно и също време, като е бил постигнат рекордния трафик от 1 Tbps (терабита в секунда). Най-сериозната атака е достигнала 799 Gbps (гигабита в секунда) и 93 Mpps (милиона пакета в секунда), като заявките са били изпратени основно от CCTV[3]

[3] CCTV – Closed Circuit Television се използва като общо наименование за всички видео камери, които осъществяват предаване на сигнал към определено място.

устройства. Освен CCTV устройствата, които са били конфигурирани с парола по подразбиране, са използвани и потребителски маршрутизатори, компютри, както и други Internet of Things устройства.

```
log /home/vac/logs/vac.log-last | egrep "pps\|.....
bps" | awk '{print $1,$2,$3,$6}' | sed "s/ /|/g" | cut -f
1,2,3,7,8,10,11 -d '|' | sed "s/.........bps/Gbps/" | sed
"s/......pps/Mpps/" | cut -f 2,3,4,5,6,7 -d ":" | sort | g
rep "gone" | sed "s/gone|//"
Sep|18|10:49:12|tcp_ack|20Mpps|232Gbps
Sep|18|10:58:32|tcp_ack|15Mpps|173Gbps
Sep|18|11:17:02|tcp_ack|19Mpps|224Gbps
Sep|18|11:44:17|tcp_ack|19Mpps|227Gbps
Sep|18|19:05:47|tcp_ack|66Mpps|735Gbps
Sep|18|20:49:27|tcp_ack|81Mpps|360Gbps
Sep|18|22:43:32|tcp_ack|11Mpps|136Gbps
Sep|18|22:44:17|tcp_ack|38Mpps|442Gbps
Sep|19|10:13:57|tcp_ack|10Mpps|117Gbps
Sep|19|11:53:57|tcp_ack|13Mpps|159Gbps
Sep|19|11:54:42|tcp_ack|52Mpps|607Gbps
Sep|19|22:51:57|tcp_ack|10Mpps|115Gbps
Sep|20|01:40:02|tcp_ack|22Mpps|191Gbps
Sep|20|01:40:47|tcp_ack|93Mpps|799Gbps
Sep|20|01:50:07|tcp_ack|14Mpps|124Gbps
Sep|20|01:50:32|tcp_ack|72Mpps|615Gbps
Sep|20|03:12:12|tcp_ack|49Mpps|419Gbps
Sep|20|11:57:07|tcp_ack|15Mpps|178Gbps
Sep|20|11:58:02|tcp_ack|60Mpps|698Gbps
Sep|20|12:31:12|tcp_ack|17Mpps|201Gbps
Sep|20|12:32:22|tcp_ack|50Mpps|587Gbps
Sep|20|12:47:02|tcp_ack|18Mpps|210Gbps
Sep|20|12:48:17|tcp_ack|49Mpps|572Gbps
Sep|21|05:09:42|tcp_ack|32Mpps|144Gbps
Sep|21|20:21:37|tcp_ack|22Mpps|122Gbps
Sep|22|00:50:57|tcp_ack|16Mpps|191Gbps
You have new mail in /var/mail/root
```

Фиг. 2. Лог файл, показващ входящия трафик към OVH

На следващо място се нарежда DDoS атаката, която успя да повали множество услуги като Twitter, Spotify, PayPal, Amazon, Reddit, GitHub и други, общо около 70 услуги. Това е атаката от 21-ви октомври 2016 година срещу американската компания Dyn, Inc. Като компания, Dyn предлагат мониторинг, e-mail, както и DNS услуги на своите клиенти. Така наречената Dyn DNS кибератака започва сутринта на 21-ви октомври и е била насочена към тяхната DNS инфраструктура в североизточните щати. В резултат, всяка DNS заявка от клиент, отправена към сървърите на Dyn, бива забавяна или неосъществена.

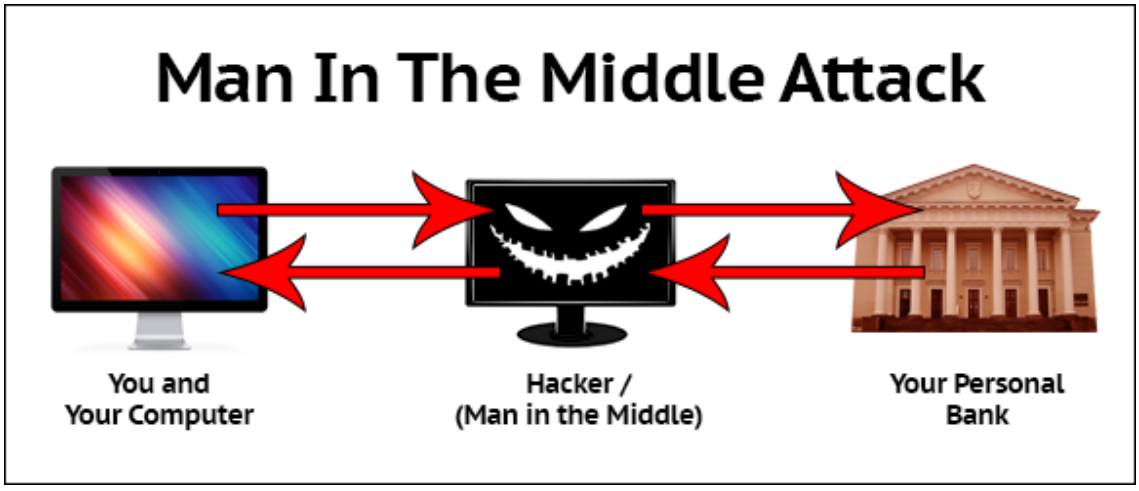
За целта на гореописаните атаки са използвани устройства заразени с Mirai, или в превод от японски – „Бъдещето“. Mirai е вид злонамерен софтуер, който има възможност да зарази мрежово свързани устройства, инсталирани с Linux и по-късно Windows операционни системи, и да ги превърне в отдалечено

контролирани ботове[4], които могат да бъдат и част от ботнет[5]. Mirai и самата ботнет мрежа се управляват от отдалечен сървър за командване и контрол (C&C – Command and Control), който има две основни функции. Едната е да продължава да сканира и компрометира Internet of Things устройства, а втората – да започне изпращането на заявки по команда от C&C сървъра. При по-детайлно разглеждане на кода на Mirai [5] е установено, че той функционира на няколко нива. Освен през приложния слой, се наблюдават SYN и ACK flood, DNS flood, UDP flood и други, което всъщност прави ботнета изключително ефективен за DDoS атака.

1.3. Man-in-the-middle (MitM) атаки

При този тип атаки извършителят на атаката, се поставя между потребителя и сървъра, който предлага дадена услуга (фиг. 3). При успешно прилагане на такава атака, извършителят изгражда две различни сесии – една с потребителя и една със сървъра. Когато потребителят се опита да достъпи този сървър, в общия случай атакуващият вижда този трафик, записва го и се представя пред потребителя като достоверния ресурс и по този начин получава цялата информация, която потребителя изпраща по време на текущата сесия. С изградената връзка към сървърната част, атакуващият може да препредава всяка заявка, която е получил от потребителя, от съображение да не алармира за присъствието си или да получи допълнителна информация. Като друг вариант той може да използва прихванатата сесия, за да представи себе си като легитимния ползвател на услугата и да получи неоторизиран достъп до чувствителна информация, която се намира на този сървър. В тези случаи се наблюдава следната последователност от действия и събития – потребителят приключва работа със сървъра, подава заявка за затваряне на сесията, при което нарушителя му връща отговор, че сесията е успешно затворена, но реално не разпада своята връзка към сървъра.

[4] Интернет робот – уеб робот, WWW робот или просто бот е софтуерна програма, която има възможност да стартира автоматизирани задачи / скриптове през Интернет.
[5] Ботнет – група от Интернет свързани устройства, на които работят един или повече ботове.



Фиг. 3. Поток на комуникацията при MitM атака

По-съвременен вариант на MitM е Man-in-the-Browser (MitB). Подходът на атака е същият – извършителят поставя злонамерен код на машината на потребителя, който код се изпълнява в браузъра. Този код е под формата на malware[6], който записва данните, изпращани между потребителя и различни сайтове, които атакуващия предварително е задал да бъдат следени. Причината MitB да става все по-популярен е, че позволява на извършителите да се целят в по-широка група от потребители и не изисква те да бъдат във физическа близост до набелязаната цел.

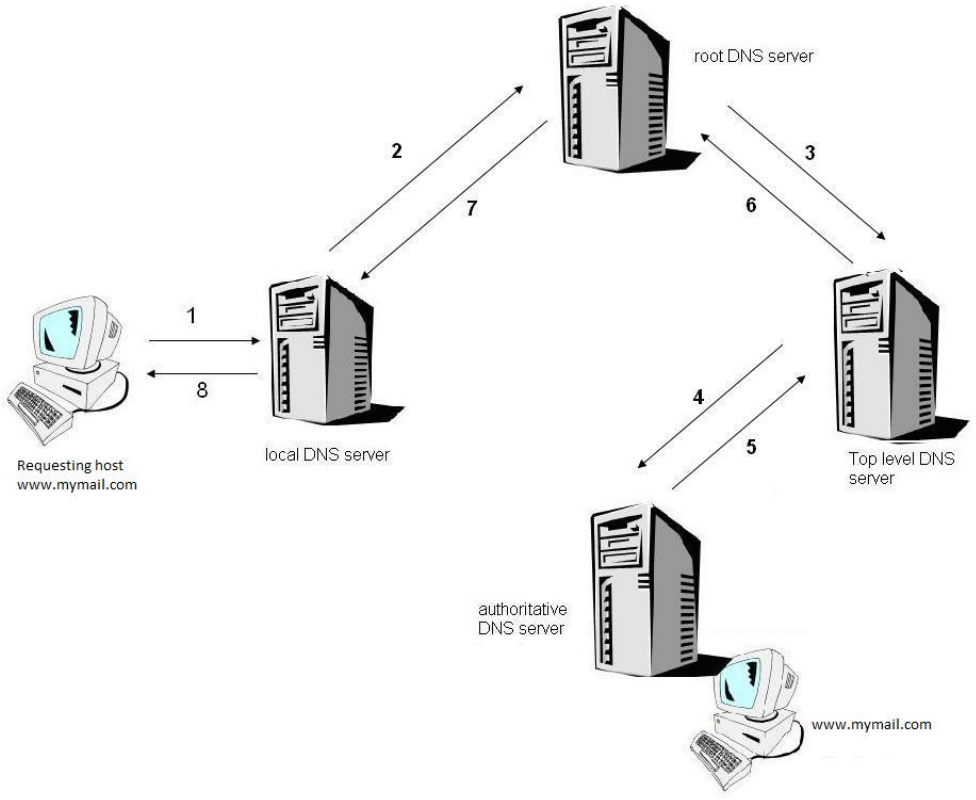
Веднъж попаднал по средата между потребителя и сървъра, атакуващият има много варианти за нанасяне на вреди:

- ARP cache poisoning – това е един от най-старите видове MitM атаки, известна още като ARP spoofing или ARP poison routing. ARP протоколът служи за преобразуването на адреси от ниво 2 и ниво 3 от OSI модела, т.е. асоциира MAC и IP адреси в даден мрежов сегмент. Поради тази причина ARP spoofing атаката е приложима само когато хостовете, които са цел на „подслушване“, са в един и същ сегмент на мрежовата инфраструктура. За да не се натоварва мрежата с постоянни ARP заявки, всеки хост създава ARP таблица с адресите на всички други хостове в своя сегмент, но една от най-сериозните слабости на протокола е липсата на автентикация при връщане на отговор от ARP заявката. Хостовете нямат механизъм, по който да проверят дали информацията, която получават, е

[6] Malware – идва от англ. Malicious Software, което означава злонамерен софтуер.

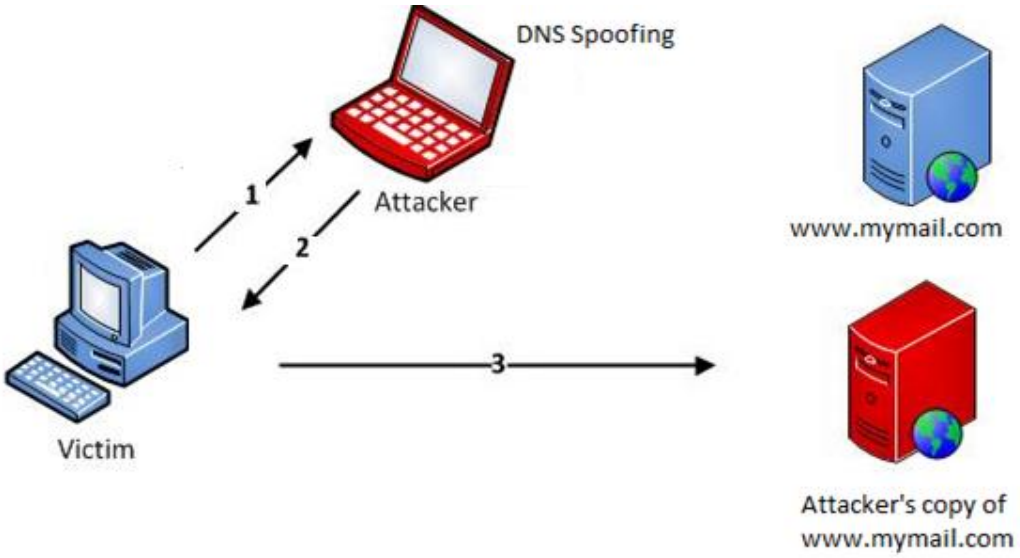
вярна или не. Използвайки тази слабост атакуващият може да „отрови“ ARP таблиците на хостовете в сегмента и да се представи за ресурс, какъвто не е, като по този начин да се яви посредник между два хоста и да получи възможност да вижда трафика, който те обменят.

➢ DNS spoofing – при подобна атака, най-общо казано, атакуващият предоставя фалшива DNS[7] информация на потребителя. Т.е. при опит на клиента да отвори пощенската си кутия на адрес www.mymail.com, атакуващият замества IP адреса на реалния сървър с IP адрес по негов избор – обикновено това е работната станция на атакуващия, на която работи фалшив сървър, където клиентът да въведе потребителското си име и паролата. По този начин извършителят вижда тези име и парола, съответно може да ги използва да достъпи пощата на потребителя на истинския www.mymail.com сайт. Нагледно на фиг. 4 е изобразен нормалния поток при достъпване на сайта www.mymail.com, а на фиг. 5 – потока, когато е намесен MitM.



Фиг. 4. Нормалният поток при DNS заявка

[7] DNS – с помощта на Domain Name System се осъществява преобразуването на имената на хостовете в IP адреси.



Фиг. 5. DNS потокът при намеса на MitM

➢ Session hijacking – след като бъде изградена сесия между клиент и сървър, атакуващият може да „открадне“ тази сесия и да се представи като легитимен клиент на сървъра. В този случай, без да е необходимо да се оторизира през сървъра, на атакуващия ще му бъдат предоставени същите права като тези на потребителя.

➢ SSL hijacking – SSL и TLS[8] са протоколи за криптиране на комуникацията между клиент и сървър. Съвместно с други протоколи те осигуряват сигурна комуникация при използването на различни услуги. SSL hijacking не е атака срещу самия протокол, а по-скоро срещу процеса при отваряне на желания ресурс. Нека разгледаме атаката, когато се използва HTTPS протокола. В чести случаи потребителят посещава сайт, следвайки линк, или знаейки, че когато в уеб браузъра напише www.example.bg, ще му се отвори търсената страницата, като разчита, че доставчикът на услугата е подсигурил комуникацията. Това действително е така. Със зачестилите кибератаки и кражби на информация през последните години всяка корпорация и доставчик на услуга засилиха използването на сигурна комуникация за своите сайтове и наложиха приемането на заявки само по HTTPS протокол. По този начин дори някой да се

[8] SSL/TLS – Secure Socket Layer и Transport Layer Security са криптографски протоколи за защита на комуникацията, предавана по компютърни мрежи.

опита да прихване трафика между клиент и сървър, то той ще бъде криптиран и няма да носи никаква информация на атакуващия. SSL hijacking атаката е насочена към потребителя и към момента, в който той отваря уеб страницата. Процесът се състои в прихващане на трафика преди той да е изпратен към уеб сайта.

Последователността на атаката е следната:

- Потребителят подава заявка за отваряне на сайт https://example.bg;
- MitM прихваща трафика, вижда заявката и му връща отговор във вид на пренасочване към http://example.bg;
- Браузърът на потребителя автоматично изпраща заявка за отваряне на незащитения http://example.bg;
- MitM отваря страницата https://example.bg от легитимния сървър и я препраща към потребителя като http;
- Потребителят изпраща заявка (примерно потребителско име и парола) по http, която атакуващият получава;
- MitM вижда и записва съдържанието на заявката и го препраща към легитимния сървър по защитения https протокол;
- Сървърът връща отговор, който атакуващия отново препраща към потребителя по http и т.н.;

Този процес продължава, докато има отворена сесия към съответния сайт. По този начин за сървъра е спазено изискването за използване на HTTPS, а клиентът получава информацията, от която има нужда, без да знае, че някой вижда трафика му.

1.4. SQL Injection (SQLi) и Cross-site Scripting (XSS)

SQL[9] атаките се състоят във внедряване или т. нар. „инжектиране“ на SQL заявка в посока от клиента към приложението. Успешните SQL injection атаки могат да доведат до извличане на чувствителна информация, промяна съдържанието в базата данни, изпълнение на администраторски операции в нея

[9] SQL – Structured Query Language, или език за структурирани запитвания, е език за програмиране, предназначен за създаване, промяна, обработка и извличане на данни от релационни бази данни.

или достъп до операционната система, върху която е инсталирана. Това са едни от най-честите типове атаки, поради няколко причини – не изисква физическа близост до целта; в съвременния свят всяка организация има свой уебсайт, зад който стои SQL база данни; в повечето случаи сайтовете са самоделно направени и нямат заложени механизми за сигурност. Съществуват няколко разновидности на SQL injection атаката:

- Error-based Injection – както става ясно от името, атакуващият изпраща SQL заявка от приложението към сървъра и очаква да му върне грешка. Целта на този тип SQLi е чрез грешките да се направи извод за архитектурата на базата данни. Веднъж познавайки архитектурата на базата, нападателят ще знае каква заявка да състави и изпрати към сървъра, така че да получи достъп до нея или да разкрие информация за съдържанието ѝ.
- Union-based Injection – това е техника, която се възползва от оператора UNION в SQL, който комбинира и извежда резултатите от два или повече отговора от базата данни.
- Blind SQL Injection – още известно като дедуктивно SQL „инжектиране“. Това е от типа атаки, при които е неизвестно дали приложението и базата са уязвими. Основната идея е да се наблюдава поведението на базата данни без да се очаква конкретна информация от приложението, т.е. прави се проверка дали приложението ще върне празна уеб страница или няма да обработи заявката. В резултат на наблюдаваното поведение е възможно да се направят изводи за това дали базата данни може да бъде манипулирана с SQL injection.

Един от примерите за потенциални щети, които може да нанесе SQLi, е атака от 4-ти март 2018 година, когато френски изследовател по сигурността успешно е изпълнил SQL заявка, която извлича лични данни на над 47 хиляди служителя, работещи и пенсионирани в телекомуникационна компания в Индия. Изследователят твърди, че това не е първият път, когато тази уязвимост е използвана. За пръв път негов колега, студент III-ти курс в Индия, открива уязвимостта през 2016 година и е направил многократни опити да предупреди ръководството на компанията, но не е получил отговор. Уязвимостта е открита в

страницата за въвеждане на потребителско име и парола, използвайки Blind SQLi.

SQL инжектирането може да бъде комбинирано и с Cross-site scripting (XSS). XSS е атака, която използва уязвимост на уеб приложение и „вмъква“ нежелан код, който се изпълнява в браузъра на крайния потребител. Най-общо казано атаката цели да намери уязвимо място в приложението, чрез което да вмъкне злонамерен код в базата данни. Когато легитимен клиент на сайта направи заявка за някаква информация и попадне на компрометирания компонент, уеб приложението ще върне търсения отговор заедно със злонамерения код. Целите на атаката може да са много – придобиване на достъп до защитена зона на сайта (чрез постигане на кражба на сесията), подвеждане на потребителя да въведе информация към трети източник, инсталиране на нежелани програми на компютъра на потребителя (Spyware, Trojan и т.н.). Обикновено крайният потребител не може да намери визуален белег, по който да разкрие атаката.

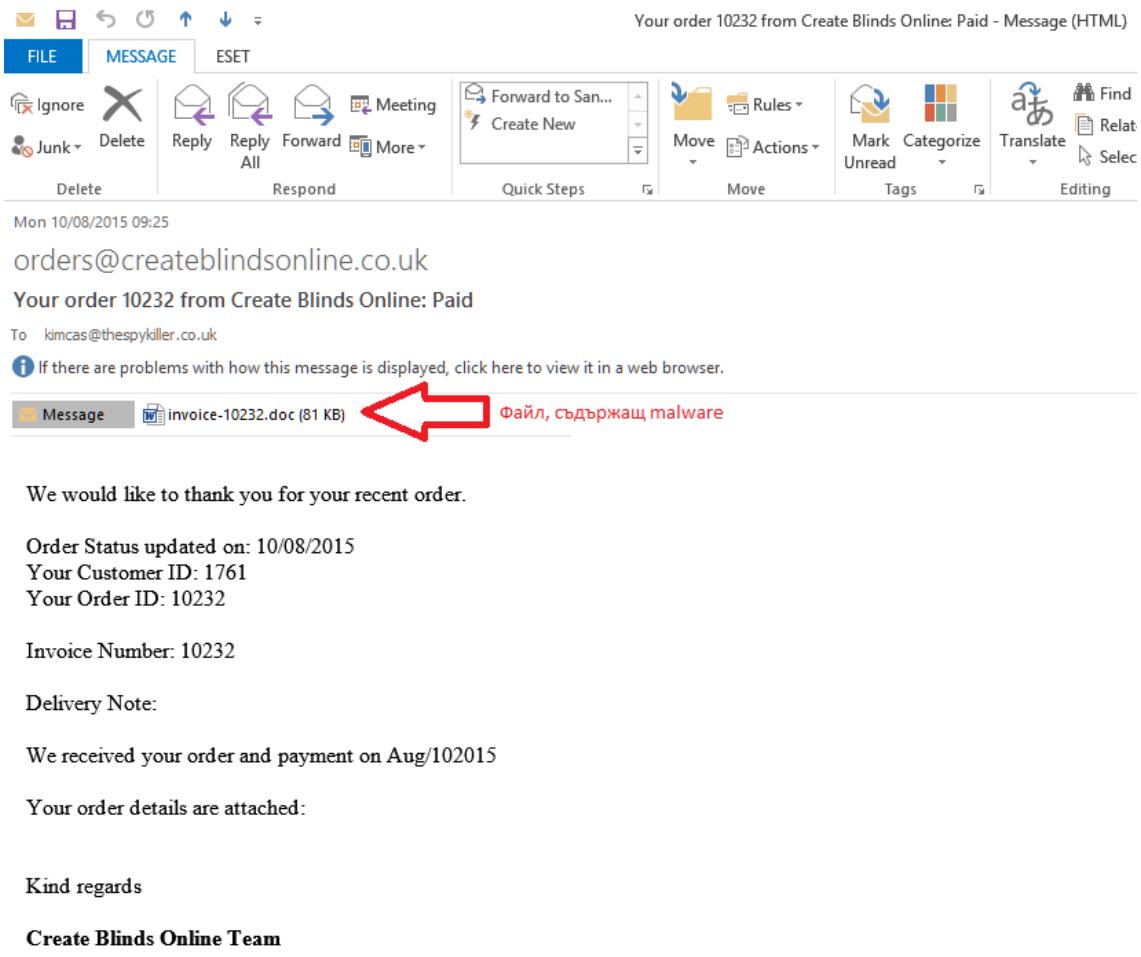
XSS атаките, които произхождат в посока от сървъра към клиента, са два вида:

- Динамични – атакуващият предоставя връзка или друг вид „маскиран“ код към клиента. Когато клиентът последва такава връзка, той попада на дадена услуга в оригиналния уебсайт, но вече с модифициран от атакуващия код. Директните атаки се реализират най-често чрез изпращане на писма по електронната поща към жертвата или чрез съобщения в различни чат приложения.
- Статични – атакуващият успява да вмъкне нежелания код в базата данни на приложението и изчаква клиентът сам да отвори уязвимата страница. Това са най-честите атаки при социалните мрежи – форуми, блогове, дискусионни групи, и т.н.

1.5. Атаки, използващи вреден софтуер (malware)

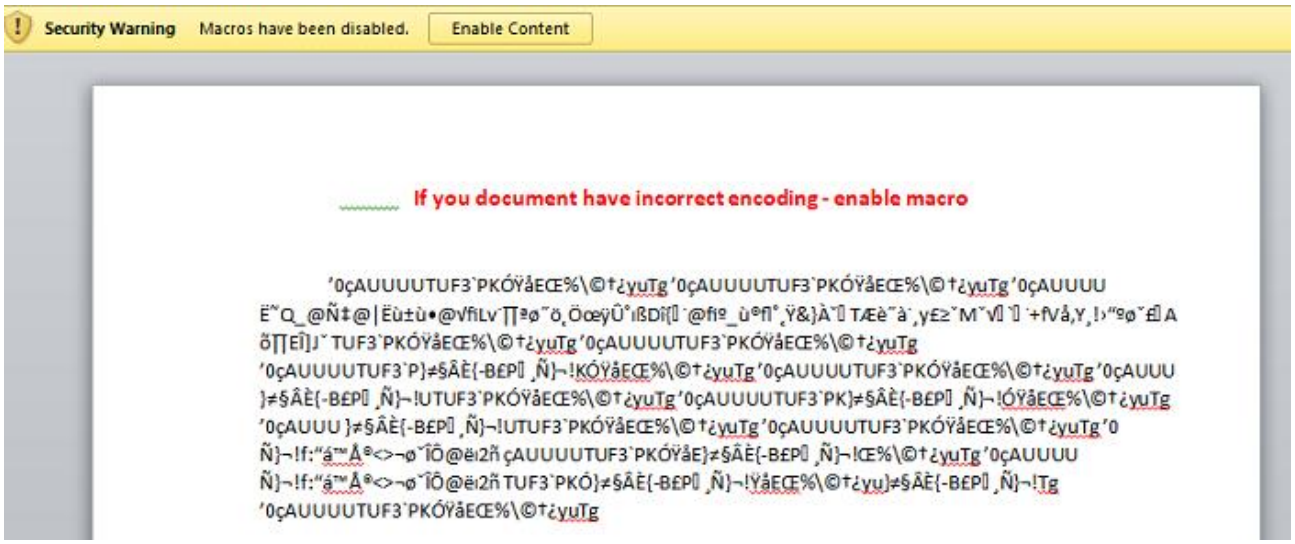
Използването на malware е метод, често използван от атакуващите, за да навредят на потребителите по един или друг начин като в най-общия случай

крайната цел е парична облага. Съществуват много видове malware и много техники за разпространение на такъв. В последните няколко години драстично зачестяват случаите, при които malware бива разпространяван чрез spam[10] съобщения. Пример за spam съобщение, изпратено по електронна поща, може да се види на фиг. 6. В дадения пример, подателят е приложил текстов документ invoice-10232.doc, като при неговото изпълнение текстът вътре е нечетим. Единственото четимо в съобщението (фиг. 7) е онази част, която ни уведомява, че при наличие на проблем с визуализирането на документа, следва да се разрешат макрос функциите на програмата. Макрос функциите позволяват запис и изпълнение на няколко последователни стъпки в приложението. В конкретния случай, ако потребителят разреши използването на макроси, се стартира скрипт, който има за цел да зарази компютъра с някакъв тип вреден софтуер.



Фиг. 6. Spam съобщение, съдържащо файл с malware

[10] Spam – представлява масовото изпращане на електронни съобщения, обикновено с нежелан характер.



Фиг. 7. Съдържанието на прикачения файл

Други варианти за заразяване със злонамерен софтуер са инсталиране на програма, която в себе си съдържа вреден код, криещ се в стандартния ѝ код, или просто посещение на компрометиран уеб сайт, който открива уязвимост в браузъра на потребителя и се възползва от нея. Когато malware-ите се използват целенасочено, обикновено тази цел е да се стигне до контрол върху потребителския компютър, откъдето атакуващият може да започне сканиране на мрежата за допълнителни компютри, които съдържат чувствителна информация. Както описахме по-рано типовете malware са много, но ние ще се спрем на онези от тях, които могат да бъдат използвани за целенасочена атака:

- Trojan („Троянец“) – наподобява програма, която потребителят би искал да инсталира. В зависимост от желания резултат, атакуващия може да използва троянеца, за да инсталира backdoor[11] на компютъра, да изтрие съдържание от твърдия диск, да открадне такова или да започне да разпространява друг тип malware.

- Ransomware („криптовирус“) – това е тип malware, който при стартиране криптира файловете на потребителя. Обикновено се използва за парична облага, като заразява файловете на отделни потребители и изисква

[11] Backdoor – е метод, използван да се придобие неоторизиран достъп до компютърна система.

заплащане за отключването им. В чести случаи се използва и за целенасочени атаки с цел блокиране на достъпа до ресурсите на цяло предприятие.

- Spyware – както е посочено в името му, този вид malware шпионира потребителя, на чийто компютър е инсталиран. Целта е да се съберат персонална информация, потребителски имена, пароли и като цяло всичко, което потребителят прави на компютъра си.

Най-забележителната ransomware атака, която успя да порази над 300 хиляди компютъра по цял свят, е следствие от пробив в сигурността на SMB[12] протокола (CVE-2017-0144). Според Forbes [6], разработената от NSA (National Security Agency или Агенция за национална сигурност) уязвимост в SMB протокола, успя да се разпространи в над 150 държави. Microsoft операционните системи използват SMB протокола при споделяне на файлове, принтери, серийни портове или друга комуникация между хостове. Т.е. всички Windows-базирани операционни системи го използват, следователно това е причината от тази уязвимост да са засегнати най-вече работните станции и сървъри, използващи Microsoft Windows. През месец март 2017 година, Microsoft издават обновления за операционните си системи, които поправят уязвимостта, но много компании и потребители не инсталират обновленията навреме. Месец по-късно хакерска групировка наречена Shadow Brokers, вади наяве информация за тази уязвимост, а експлойтът е наречен EternalBlue. Това дава началото на разработки, възползващи се от уязвимостта. Най-забележителната разработка е криптовируса наречен WannaCry (още известен като WCry или WanaCrypt0r). На 12 май 2017 година първите поразени от мащабната WannaCry атака са една от четирите здравноосигурителни служби във Великобритания (NHS) и Telefónica, най-големият телеком в Испания, а по-късно същия ден и гигантът в доставките FedEx.

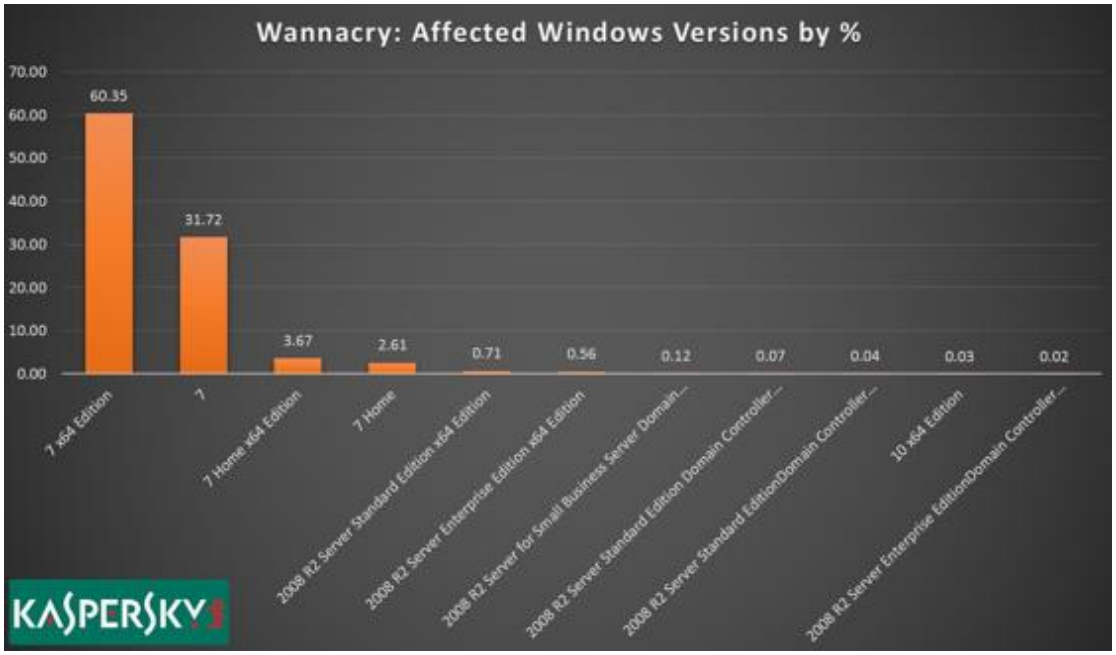
Самата уязвимост позволява манипулирането на Windows SMB v1 протокола, като дава възможност за изпълнението на произволен код. WannaCry използва тази уязвимост като метод за разпространение между всички операционни системи, които използват протокола и нямат необходимите

[12] SMB - Server Message Block е протокол за споделяне на файлове и друга комуникация между хостове.

инсталирани обновления (обновлението от бюлетина за сигурност на Microsoft MS17-010).

При направен технически анализ [7], става ясно, че когато WannaCry попадне в дадена компютърна система, се стартира активиращ компонент (dropper), който първоначално се опитва да направи връзка към несъществуващ домейн, съставен от произволни символи - **iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com**. Понеже към 12 май 2017 подобен домейн не е съществувал, WannaCry изпълнява последващите компоненти, които са заложени в кода му, а именно криптиране на файловете. Ако връзката към посочения домейн се осъществи, програмата се счита за изпълнена и не продължава с изпълнението на останалите компоненти. И до днес експертите по сигурност не разбират защо WannaCry е написан по този начин. Това намалява щетите от атаката, а след като изследовател в сферата на ИТ сигурността регистрира домейна по-късно в деня на атаката, много компютърни системи успешно се свързват към него и прекратяват последващите действия на вируса.

На фиг. 8 може да се види статистика, предоставена от руския антивирусен производител Kaspersky [8], където ясно се вижда, че 98% от засегнатите от WannaCry устройства използват Microsoft Windows 7.



Фиг. 8. Засегнати от WannaCry Windows-базирани устройства

1.6. Социално инженерство

Както е всеизвестно, човекът е най-слабото звено в сигурността и затова социалното инженерство е ключов компонент при атаката срещу коя да е система. Социалното инженерство е „изкуството“ да манипулираш човек или група от хора с цел да бъдат използвани като входна точка за атака. Подобен тип атаки съществуват от десетки години като само се използва различен вектор на атака, т.е. те могат да бъдат под формата на текстово съобщение, електронна поща, телефонно обаждане, интеракция с хора и околна среда и т.н. Обикновено тези атаки целят да се възползват от емоциите на човека, карайки го без да се замисля да направи нещо, което ще доведе до евентуално разкриване на чувствителна информация или допускане на атакуващия в определена компютърна система. Основните методи за атака чрез социално инженерство включват:

- Phishing – „фишинг“ или „зарибяване“ е може би най-често използваният метод за атака. При него атакуващите разпращат електронни съобщения или поща, която претендира, че идва от достоверен източник и се опитва да убеди получателя да предприеме някакво действие – да даде лична или финансова информация, да отвори сайт, да отвори прикачен файл и т.н. Фишинг атаките обикновено се изпращат масово към всякакъв тип потребители. По-целенасоченият метод за атака чрез фишинг се нарича „Spear Phishing”, при който целта на атакуващия е определен човек или предприятие. Зад тази атака стои предварително събрана информация за потребителя и организацията като тип на бизнеса, партньори, с които организацията работи, или дори лични детайли за служителите. Друга разновидност на фишинг е атаката срещу членове от изпълнителното ръководство, която се нарича “Whaling” и също включва значителна подготовка преди осъществяване.
- Baiting – „примамването“ е друг метод, при който атакуващият се възползва от човешкото любопитство. Най-честия подход е поставяне на USB флаш памети или класическото – CD с надпис „Най-великите хитове на 80-те“, на места, където ще бъдат намерени от минувачи. На тези устройства обикновено

има malware, който се активира или при поставяне на устройството в компютър, или при стартиране на програма от него. Методът не се изчерпва само с физически устройства. Рекламните банери по сайтовете могат да отведат потребителя до друг сайт, чието съдържание е злонамерено. В наши дни е много лесно да се открият интересите на даден човек. При целенасочена атака след откриването на нещо, което е хоби или просто е интересно за потребителя, атакуващият може да използва тази информация, за да го примами и накара да предприеме действие, което да доведе до застрашаването на компютърна му система.

- Tailgating – този метод има изцяло физическо естество. Обикновено се отнася за атаки, осъществявани към корпорации. Въпреки физическата природа на този способ, той може да доведе до много сериозна компютърна атака. Начинът на прилагане е когато неоторизирано лице последва служител на предприятието през служебен вход и в зона само за служители. Веднъж влязъл в сградата, атакуващият може да се сдобие с достъп до компютрите, на които може да инсталира malware или по някакъв друг начин да компрометира компютърните системи. Друг вариант на подобна атака е когато атакуващият се представи като служител на фирма за поддръжка на някаква услуга, да речем подизпълнител на интернет компания, който е дошъл да диагностицира проблем със свързаността. Когато бъде оставен без надзор, атакуващият може да предприеме стъпки за инсталиране на backdoor или да направи друг тип злонамерено действие.

Изводи към първа глава:

1. За някои атаки е нужен добре изработен софтуер, но истината е, че повечето от тях разчитат на човешкия фактор. В днешната ера на технологичен напредък все повече хора имат досег с информационни технологии и компютърни мрежи под една или друга форма. Това увеличава вероятността за човешка грешка, независимо дали става дума за невнимание при отваряне на spam, случайно издаване на информация посредством социално инженерство или недостатъчно знание за това как да защитим използваната от нас технология.

2. Наблюдаваното разнообразие от атаки и сравнително лесното им изпълнение дава основа на някои по-предприемчиви търговци да развият бизнес чрез предоставяне на услуги за платени контролирани кибератаки. Това още повече налага важността от адекватна система от мерки за защита.

3. С навлизането на Internet of Things броят на свързаните към глобалната Интернет мрежа устройства започна да нараства експоненциално. По този начин многократно се увеличава повърхността, която атакуващият може да нападне. С други думи, за разлика от атаките преди време, когато компрометираният елемент можеше да бъде единствено информацията, сега заплахите започват да придобиват физически осезаеми измерения – евентуалният достъп до IoT битови електроуреди би представлявал грубо навлизане и нарушаване на личната физическа неприкосновеност на човека.

4. Атаките срещу компютърните системи еволюират. Стават по-изискани, по-мащабни и се превръщат в глобален проблем за сигурността, т.е. бавно, но сигурно те се превръщат в аналог на оръжие за масово поразяване на киберниво.

Глава втора: МЕТОДИ И СРЕДСТВА ЗА ЗАЩИТА НА КОМПЮТЪРНИТЕ СИСТЕМИ И МРЕЖИ

2.1. Основни методи и средства за защита

В наши дни не съществува предприятие, което да не зависи от информационните технологии, както рядко съществува и дом без компютър или мрежова свързаност. С нарастващата необходимост от информационните технологии и нарастващия брой ИТ услуги, които се появяват, нараства и актуалността въпроса – как да се защитим от тези, чиято цел е да ни ограбят, измамят, манипулират и т.н. Проблемът със сигурността на информационните системи се задълбочава с всеки изминал ден. Организациите инвестират все повече време и ресурс, за да подобрят сигурността си. Измислят се нови протоколи за сигурност, нови подходи, политики, услуги и решения. Истината е, че не съществува универсално решение за сигурност и няма информационна, компютърна или мрежова система, която да е абсолютно и напълно защитена от нападение. Ще разгледаме различни подходи и инструменти за защита на описаните в настоящата работа атаки, но в крайна сметка една система е толкова сигурна, колкото най-слабия ѝ елемент. Независимо дали можем да си го признаем или не, този елемент е потребителят, т.е. самите ние.

Редно е да се спомене, че сигурност и защита са близки по значение, но въпреки това различни термини. Докато защитата е по-скоро механизъм, сигурността се идентифицира като политика.

Даден продукт, система или услуга се счита, че покрива базово ниво на защитеност, когато са спазени трите основни принципа на информационната сигурност, а именно:

- Конфиденциалност – само оторизирани лица имат достъп до информацията. Конфиденциалността на информацията в информационните системи е функция, регулираща обществените отношения, с която се управлява достъпа до информацията (нейната достъпност) и не се допуска нейното разкриване от неоторизиран потребител.

➢ Интегритет – информацията е непроменена спрямо момента, в който е създадена. Има интегритет, когато налице е невъзможност за промяна на информацията без разрешение. Интегритетът е нарушен, когато служител несъзнателно или съзнателно изтрие или унищожи важна информация, когато вреден софтуер зарази компютър, когато служител или външно лице има възможността неоторизирано да промени чувствителна информация.

➢ Достъпност – осигуряването на достъп до информация за хора, които имат право да я ползват. Достъпността представлява възможност на информацията да бъде достъпна, когато е необходима. За да се постигне достъпност, компютърните системи, които обработват и съхраняват информацията, техническите мерки за защита и комуникационните канали, използвани за предаването, следва да работят коректно.

В допълнение към трите принципа могат да бъдат включени и направленията автентичност, отчетност, гарантираност и надеждност.

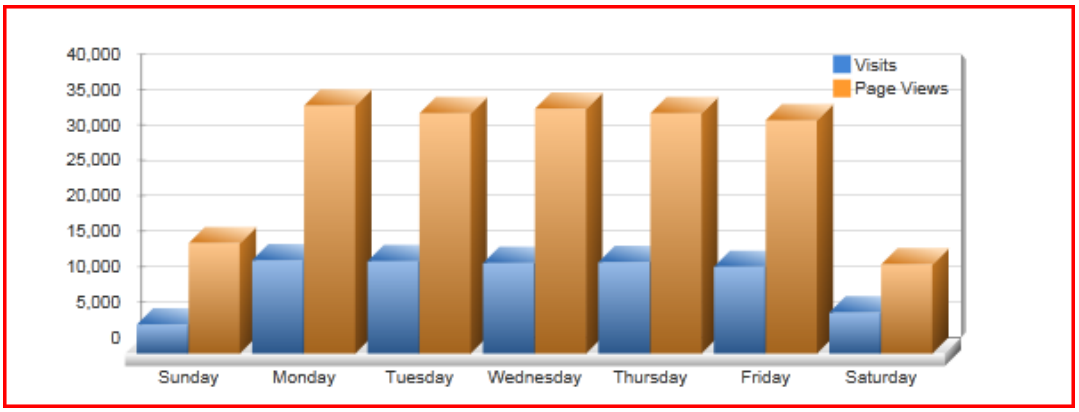
Сигурността е комбинация между технически средства и установени политики, процедури и процеси. Сигурността, която може да се постигне само с един от тези компоненти, е ограничена. В тази глава ще обърнем внимание основно на техническите средства за защита, ще споменем някои управленски такива и ще опишем един от най-важните елементи за защита, а именно потребителска бдителност.

2.2. Защита от DoS и DDoS атаки

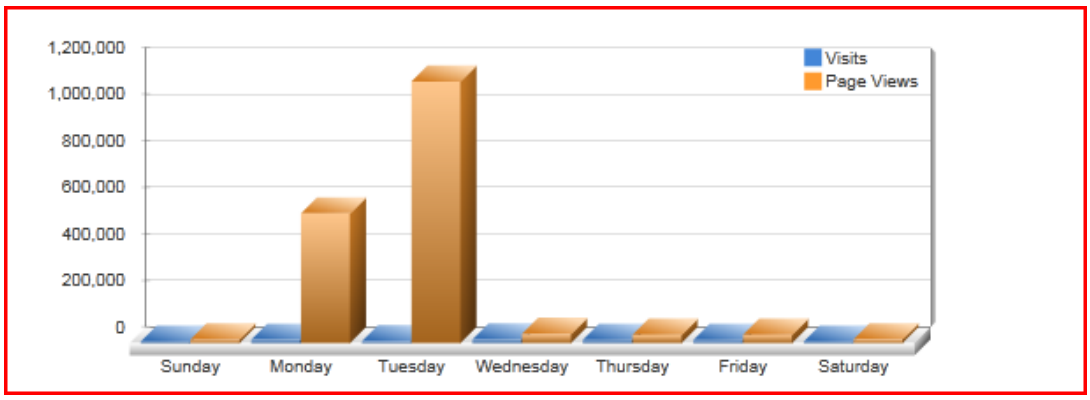
Най-общо казано, за да се защитим от DoS и DDoS атаки, трябва да се засече и блокира вредния трафик. Най-лесният метод е чрез използването на защитна стена. При стандартна DoS атака могат да се видят IP адресите и портовете, от които идва трафикът, и с правила в защитната стена той да бъде блокиран. Този метод, обаче, не работи при по-сложните атаки. За тях е желателно да има план за противодействие и смекчаване на ефекта им. Такъв план за противодействие на DoS и DDoS атаки включва:

➢ Разпознаване на атаката – първото и най-добро противодействие е да бъде разпозната атаката като такава. Не всички прекъсвания на услугата са

следствие от DDoS атаки. Възможно е да има технически проблеми с доставчика на интернет или може да има временно прекъсване на даден уеб сайт, поради профилактика. Желателно е да бъде направена статистика на активните посетители на сайта, когато той е наш. При направена такава статистика, всяко изменение от нея би могла да е DoS атака. На фиг. 9 могат да се видят нормалните посещения и разгледани страници на уеб сайт. При нормална посещаемост на сайта се вижда, че са разгледани максимум 35 хиляди страници на ден. На фиг. 10 е същият сайт, но след DoS атака, където се вижда, че разгледаните страници са стигнали над 1 милион със значително по-малък брой посещения. Подобна статистика би могла да послужи за идентифициране на DoS и DDoS атаки.



Фиг. 9. Статистика на посещения и брой заявки към уеб сайт



Фиг. 10. Статистика на посещения и брой заявки при DoS атака

➢ Презапасяване – в зависимост от необходимостта услугата ни да е постоянно активна е желателно веднъж след като сме измерили нормалния трафик, да подготвим запас от десет пъти повече този трафик.

➢ Правилна конфигурация на устройствата – маршрутизаторите, защитните стени, както и NGFW[13] (защитни стени от следващо поколение) могат да бъдат конфигурирани да спират определен тип трафик. Пример за подобна конфигурация би бил спирането на ICMP[14] заявките. IDS устройствата (Intrusion Detection System) имат възможност да разпознават трафика и да блокират този, който сметнат за вреден. IDS устройствата трябва да бъдат конфигурирани правилно, за да се избегне ефекта на грешките (false positives), които биха могли да бъдат допуснати при блокиране на трафик. Поставянето на load balancer[15] за разпределение на трафика и балансиране на натоварването между няколко сървъра също би смекчил атаката. Тези устройства, независимо дали са физически или виртуални, служат като разпределител на трафика, т.е. те наблюдават натоварването на сървърите, обслужващи услугата, и изпращат входящите заявки към по-малко натоварените сървъри.

➢ Познаване на клиентите – в зависимост от предлаганата услуга, някои компании могат да ограничат от къде може да се достъпи техния сайт, сървър или услуга, които предоставят. Например ограничаване на достъпа до сайта ни или до пощенския ни сървър от определена държава, да речем Китай или САЩ, може да помогне за смекчаване на евентуална DoS атака. САЩ и Китай са две от страните, които са начело на класацията [20] за DDoS атаки в края на 2017 година. Друг вариант е случаят, когато предлагаме нашата услуга на локално ниво на територията на Република България. Тогава можем да позволим посещения до уеб услугата само от IP адреси, които се намират в страната. С напредналите облачни услуги това е почти невъзможно, понеже големите доставчици на такива услуги се намират извън територията на страната и трафикът преминава през чуждестранни IP адреси. Двата примера за ограничаване на входящите заявки са неприложими, когато услугата е интернационална.

[13] NGFW – Next Generation Firewall – трето поколение защитна стена с допълнителни функционалности.
[14] ICMP – Internet Control Message Protocol е протокол, най-често използван за диагностика на мрежови устройства.
[15] Load Balancer – устройство или софтуерен продукт, който разпределя мрежовия или приложния трафик между няколко устройства.

2.3. Защита срещу MitM атаки

Най-ефикасният метод за защита срещу MitM атаки е потребителската бдителност. Зачестилите измами през изминалите години научиха не само разработчиците на сайтове и услуги, но и потребителите да внимават, когато става въпрос за онлайн ресурси. Въпреки това доста потребители не обръщат внимание на предупрежденията, които могат да помогнат за предотвратяването на Man-in-the-Middle атаки. За да се гарантира сигурна комуникация, собствениците на сайтове и услуги следва да внедрят необходимите мерки, понеже в по-голямата си част условията за комуникация се определят от сървъра, на който се намира услугата. Пример за подобна по-сигурна комуникация е, когато даден уебсайт предлага криптиране на връзката между себе си и клиента чрез SSL или TLS протокола. Внедряването на SSL/TLS в комуникацията изисква и валиден сертификат, който да доказва, че посетеният сайт наистина е този, който търсим. В генералния случай за доказване на истинността на сертификата той трябва да бъде издаден от сертифициращ орган, на който потребителските машини да „вярват“. В зависимост от това дали уебсайтът ще бъде достъпен за клиенти извън организацията или само за потребители в организацията съществуват няколко варианта за издаване на сертификат:

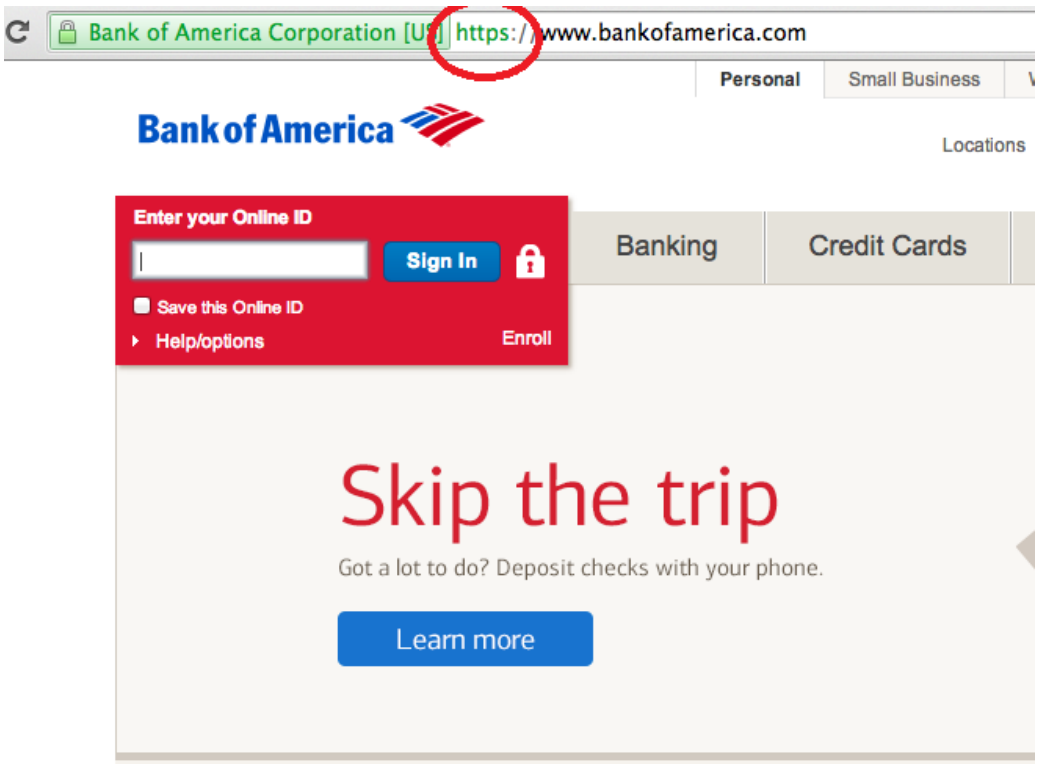
- Самоподписан сертификат (Self-signed certificate) – тези сертификати се издават от самия сървър, на който се намира и работи услугата. Целта е да се премине към използването на комуникация по защитен порт, но без да се предоставя истинност на самия сертификат. Най-често такива сертификати намират приложение за тестови цели преди сайта да влезе в експлоатация и да стане достъпен за други потребители.
- Частен сертификат (Private certificate) – когато няма необходимост услугата да е налична в Интернет, а ще се използва само от потребители на организацията, се използват т.нар. частни сертификати. За издаването им е необходимо изграждане на инфраструктура на публичния ключ или PKI в рамките на организацията. На върха на изградената инфраструктура стои

основният сертифициращ орган (Root Certificate Authority), до който се допитват всички сървъри и потребителски станции, част от организацията.

➢ Публичен сертификат (Public certificate) – тези сертификати се издават от световно известни сертифициращи органи, които през годините са се доказали като надеждни и сигурни. В резултат на това производителите и разработчиците на операционните системи и браузъри им „вярват“.

От страна на клиента основните методи за защита от MitM атаки са:

➢ Винаги трябва да се обръща внимание дали комуникацията към даден сайт е криптирана. Най-лесно това може да стане чрез поглеждане на адресната лента, където ако имаме криптирана комуникация, можем да я разпознаем по HTTPS (Hypertext Transfer Protocol Secure) протокола (фиг. 11).



Фиг. 11. Страница, отворена през HTTPS

При изпълнение на SSL hijacking атаката в адресната лента на браузъра потребителят ще вижда, че връзката към уебсайта се осъществява по HTTP и по този начин ще знае, че има нередност в комуникацията между работната му станция и сървъра.

➢ Не трябва да се пренебрегват съобщенията за грешен сертификат на сайта (фиг. 12). Тези предупреждения могат да означават, че този сертификат не отговаря на сайта, който сте посетили.

Фиг. 12. Предупреждение за проблем със сертификат

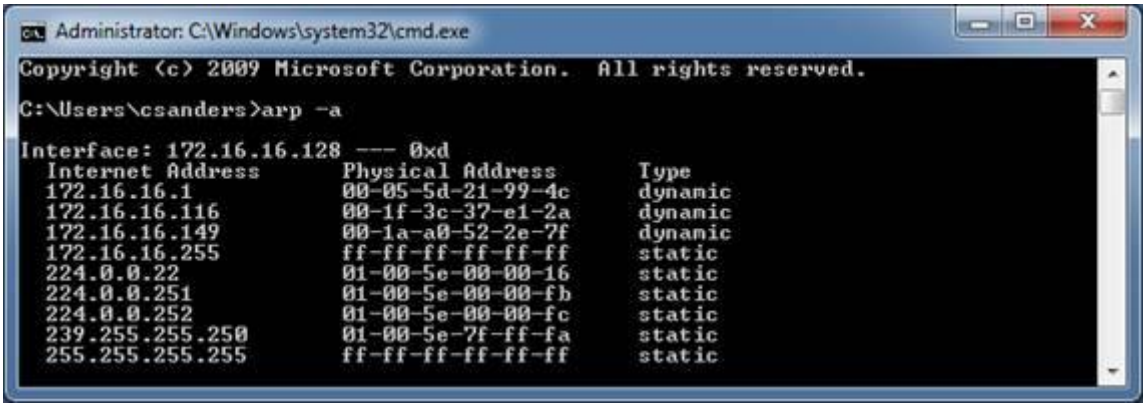
В зората на масовото внедряване на SSL/TLS и сигурната комуникация на уебсайтовете са познати случаи, в които пропуски в конфигурацията на сайта може да доведе до грешка със сертификата. Съответно повечето потребители са привикнали със съобщението и не обръщат внимание, продължавайки към сайта, въпреки предупреждението. В случаите когато няма конфигурационна грешка, при продължаване към сайта и въвеждане на потребителско име, парола, ЕГН, номер на личен документ или друг тип информация евентуалният „човек по средата“ ще види въведените данни и може да ги използва, за да придобие достъп до защитена за потребителя информация или да се представи за него, използвайки личните му данни.

➢ Често наблюдавано е свързването към безжични мрежи без парола с цел използване на интернет свързаност. Това също може да доведе до MitM атака. Когато свързването към такава мрежа е неотложно, трябва да се избягва отварянето на ресурси, които съдържат чувствителна информация като онлайн

банкиране и т.н. С помощта на съвременните мобилни устройства всеки може да създаде своя безжична мрежа и да я остави със свободен достъп (без парола), очаквайки някой да се свърже към нея, след което да използва необходимите инструменти, за да осъществи MitM атака.

Почти всички видове Man-in-the-Middle атаки се осъществяват от вътрешната мрежа на потребителя или компанията. До тук разгледахме как потребителят може да се защити от „човека по средата“, но има и случаи, в които средностатистическият потребител няма как да разбере или да разпознае подобна атака. Когато се изгражда концепцията за ИТ сигурност, основния фокус пада върху подсигуряване на периметъра и предпазване от външни заплахи. Рядко администраторите и специалистите по сигурността очакват източникът на атаката да бъде вътрешен човек или някой с физически достъп до устройствата във вътрешната мрежа, но това не означава, че е невъзможно. От страна на вътрешната инфраструктура също могат да бъдат предприети мерки за защита от Man-in-the-Middle:

- Защитата на корпоративната мрежа от ARP cache poisoning е сложен процес, тъй като потребителят може да не разбере за атаката, а дори и да разбере тя вече ще бъде осъществена. Когато говорим за превенция от отравяне на ARP таблиците, трябва да знаем, че ARP протоколът работи само и единствено в локалната мрежа, т.е. ако имаме различни устройства в различни мрежови сегменти, ARP атаката не следва да ни тревожи. Ръчното добавяне на стойности в ARP таблица за всеки от хостовете ще избегне динамичността на процеса. По този начин, когато потърсим някакъв ресурс в същата мрежа, компютърът ни няма да излъчи broadcast заявка, търсейки ресурса, а ще го открие в таблицата. Пример за ARP таблица в Microsoft Windows операционна система може да се види на фиг. 13, където е показано как могат да се проверят текущите записи в таблицата. Статичните записи в таблицата на същата операционна система могат да бъдат направени чрез командата “arp –s <IP address> <MAC address>”. В по-големи мрежи и в среда, в която мрежовата конфигурация често се променя, този метод е неприложим.



Фиг. 13. ARP таблица в Microsoft Windows OS

➢ Подобно на ARP, DNS spoofing атаката също е трудна за разпознаване, поради пасивния ѝ характер. Тук работи същият механизъм както при ARP cache poisoning превенцията, т.е. ръчно нанасяне на асоциацията между DNS имената и IP адресите във файла, който операционната система проверява преди да направи запитване към DNS сървър. В Microsoft Windows тези записи се намират във файл C:\Windows\System32\drivers\etc\hosts, а в UNIX базираните операционни системи в – /etc/hosts. Този метод отнема време и усилия, понеже записите във файла следва да бъдат направени на всеки един хост и при евентуални промени в DNS конфигурацията да бъдат допълнени новите записи или премахнати стари, които вече не се използват.

DNS spoofing е от типа атаки, които няма да изчезнат докато DNS протоколът съществува. Те са сравнително лесни за изпълнение и са трудни за засичане. Поради тази причина е разработен механизъм за автентикация на DNS заявките наречен DNSSEC (DNS Security Extensions). Както беше показано на фиг. 4, когато потребителят направи заявка за отваряне на даден ресурс, тя стига чак до достоверния DNS сървър, отговарящ за този сайт. DNSSEC използва асиметрична криптография и двойка ключове, за да удостовери истинността на върнатия отговор.

Приложението на съвременни методи за защита на вътрешната мрежа е нещо, което всяка компания следва да внедри, за да има централизиран поглед върху инфраструктурата си и да има възможност за идентифициране и, при необходимост, контрол на неоторизирана техника. През 2004 година за пръв път

се използва термина BYOD (Bring Your Own Device) или още наречено „донеси свое собствено устройство“. През 2009 година този термин отново изплува и година по-късно започва да се превръща в концепция, която бизнес компаниите започват да приемат с цел техните служители да станат по-продуктивни. Няколко години по-късно BYOD вече се превръща в политика, в която компаниите позволяват служителите им да работят от своите устройства, когато им е по-удобно. Това разбира се крие и своите рискове. Реално нищо не би могло да попречи на някого да донесе собствено си устройство, да се свърже към корпоративната мрежа и да започне да „слуша“ трафика. Един от доказалите се подходи за защита срещу подобен тип заплахи е внедряването на технологично решение за Network Access Control.

Network Access Control (NAC) представлява подход за контрол на достъпа до корпоративните мрежи. Той дава възможност за по-задълбочен поглед върху крайните устройства и позволява свързване към мрежата само на тези, които отговарят на предварително зададени критерии и политики. По този начин администраторите могат да дефинират изисквания към преносимите компютри, телефоните, таблетите преди да им позволят да се свържат към корпоративната мрежа. Изискванията могат да включват:

- Изискване за типа на устройството, когато знаем какъв тип устройства използват нашите потребители. Налагане на ограничения по марка, модел, процесор на машината и т.н.;
- Изискване за наличие на инсталирано минимално или конкретно обновление за сигурност на операционната система;
- Изискване за наличие на обновена антивирусна програма със сигнатури, не по-стари от 3 дни;
- Изискване за конкретна версия на операционната система. По този начин потребител, който се свърже с компютър с инсталирана операционна система Windows XP, няма да може да се свърже към мрежата.

Внедряването на NAC може да спомогне за ограничаване на възможността за свързване на устройства, които могат да компрометират

сигурността отвътре или да послужат като работна станция на „човека по средата“.

2.4. Защита срещу SQL Injection и Cross-site Scripting

Имайки предвид, че най-често векторът на атака при SQL инжектирането и XSS е от клиентска страна, като основно правило и метод за превенция е филтриране и валидиране на потребителските заявки. Това, разбира се, не е единственият метод на защита, който трябва да се разглежда, когато се проектира дадено уеб приложение:

- Готови отговори с използване на параметрични заявки – този тип защита се дефинира в приложението и има за цел да гарантира, че приложението няма да интерпретира и да предаде заявката погрешно към базата данни. По този начин структурата на заявката е отделена от подаваните параметри, т.е. приложението винаги има предварително подготвена процедура, а единственото, което иска от базата данни е стойността на параметъра. Съответно при опит за SQLi няма да бъде отворена възможност за промяна на заявката към базата данни, като вместо това приложението ще предаде злонамерената заявка като параметър.
- Съхранени процедури – използването на съхранени процедури е един от начините за превенция на SQL инжектиране, понеже клиентът няма възможност за изработване на случайни SQL заявки. Кодът за тези процедури е дефиниран и се съхранява в базата данни, а не в приложението и то го извиква от базата, само когато е необходимо. По този начин, когато клиентът се опита да напише злонамерена SQL заявка в уеб приложението, то няма да я разпознае и няма да направи обръщение към базата данни.
- Валидиране на входа – това е метод, който се прилага с цел избягване на символи, използвани при SQL injection атаките. Има два основни подхода при валидирането:
  - Забраняване на символи – забранява се въвеждането на определени символи или се насилва тяхната промяна при изпращането им от приложението към базата данни. Замяната най-често се прилага за

специалните символи (!, @, #, %, * и т.н.) и се прави с цел базата данни да не интерпретира тези символи като част от SQL заявка. Пример за такава подмяна би било поставянето на наклонена черта (\ ) пред символи като „ ‘ “, „ “ “ и други, използвани за манипулация на базата. Негатив при този подход е, че разработчикът на приложението и базата данни трябва да предположи всяка възможна комбинация от символи, която би могла да бъде използвана за SQLi уязвимости;

• Позволяване на символи – разрешава се въвеждането само на определени символи. По този начин, ако дадено поле в приложението трябва да се състои от определен тип символи, то за него следва да се наложат ограничения и позволение за въвеждане само на разрешените такива. Така при въвеждане на неоторизирани символи приложението няма да обработи заявката или изобщо няма да позволи потребителят да въвежда в това поле. Най-често срещаният метод за реализация на описаното е чрез използването на регулярни изрази (regex или regular expression). Пример за позволени символи в поле за потребителско име, използвайки regex в ASP.NET е „ **^[a-zA-Z-\s]{1,40}$** “. Този израз ще позволи използването на английската азбука, главни букви, малки букви и тире. Допълнително е наложено и ограничение за максимален брой символи в потребителското име (от 1 до 40).

➢ Ограничаване на привилегиите – представлява метод за намаляване на щетите при пробив с SQLi. Приложенията използват предварително дефинирани акаунти за свързване към базата данни, т.е. когато клиентът въвежда данни в приложението, то изпълнява заявката към базата, използвайки този акаунт. При разработка на приложение с база данни се препоръчва спазването на принципа „най-малко привилегии“. Така при евентуална SQLi атака, ако акаунтът не е администратор на базата данни и няма права за изтриване и промяна на съдържанието в таблиците, злонамереното лице няма да има възможност да осъществява промени или да изтрива информация.

➢ Съобщения за грешка с общо значение – когато говорим за SQLi атаки, базирани на върнати грешки от приложението или базата данни, методът

за превенция е чрез използването на съобщения, които не дават конкретна информация за грешката. Така атакуващият ще бъде затруднен в опита си да разбере каква е архитектурата на базата данни.

Сам по себе си всеки от изброените подходи е недостатъчен, когато говорим за защита от SQL инжектиране и XSS, но ако се комбинират, тези подходи могат да са силен инструмент при борбата с този тип атаки. Разбира се сигурността на приложението и неговата възможност да изпълнява своите функции трябва да се балансират. В крайна сметка, ако потребителят среща затруднения, породени от мерките за сигурност, то той няма да намира полза в употребата на това приложение.

Друг способ за превенция на SQLi и XSS е чрез използването на защитна стена за уеб приложението (Web Application Firewall - WAF). Този тип защитни стени работят на приложния слой от OSI модела и служат като посредник между клиента и уеб приложението. За разлика от мрежовите защитни стени от ниво 3 и 4, WAF има възможност да вижда HTTP/S заявките между клиента и сървъра и да ги филтрира, базирано на предварително зададени правила.

2.5. Защита срещу malware

Основният метод, който се използва за разпространение на malware са spam електронните съобщения, които ще разгледаме в следващата стъпка от защитата срещу атаките. Това отново призовава за допълнително развитие на потребителската бдителност, която е на първо място що се отнася до защита от malware. Когато по невнимание потребителят все пак отвори или направи опит да инсталира злонамерена програма, основните подходи, които се ползват за защита са:

- Антивирусна програма – представлява софтуер, който използва различни алгоритми да засича и премахва malware. Основният метод, който използва е търсене на т. нар. сигнатури (definitions или signatures), които представляват образци на кода, съдържащ се в даден malware. Друг метод е евристичният анализ, който засича нови заплахи с подобен код на вече познатите

за антивируса malware-и. По този начин, дори да не са качени последните сигнатури на антивирусния софтуер, заплахите също могат да бъдат засечени. Последният метод, на който ще се спрем е sandbox детекцията. При него антивирусният софтуер стартира програми със съмнителен код в тях в изолирана среда. По този начин, ако програмата наистина е вирус, тя не заразява реалната среда.

- Регулярно обновяване на операционната система – повечето заплахи се възползват от уязвимости в кода на самата операционна система или от протоколи, които операционната система използва. Регулярното инсталиране на обновления, издадени от разработчиците, могат да минимизират ефекта на евентуално заразяване с malware.

- Регулярно обновяване на приложенията – редом с операционната система е препоръчително да се инсталират такива обновления и за приложенията, които потребителят използва. Желателно е винаги да се обновява и използва последната възможна версия на браузъра. По този начин потребителят винаги има последните технологии, които браузърите използват за идентифициране на сайтове, разпространяващи злонамерен софтуер.

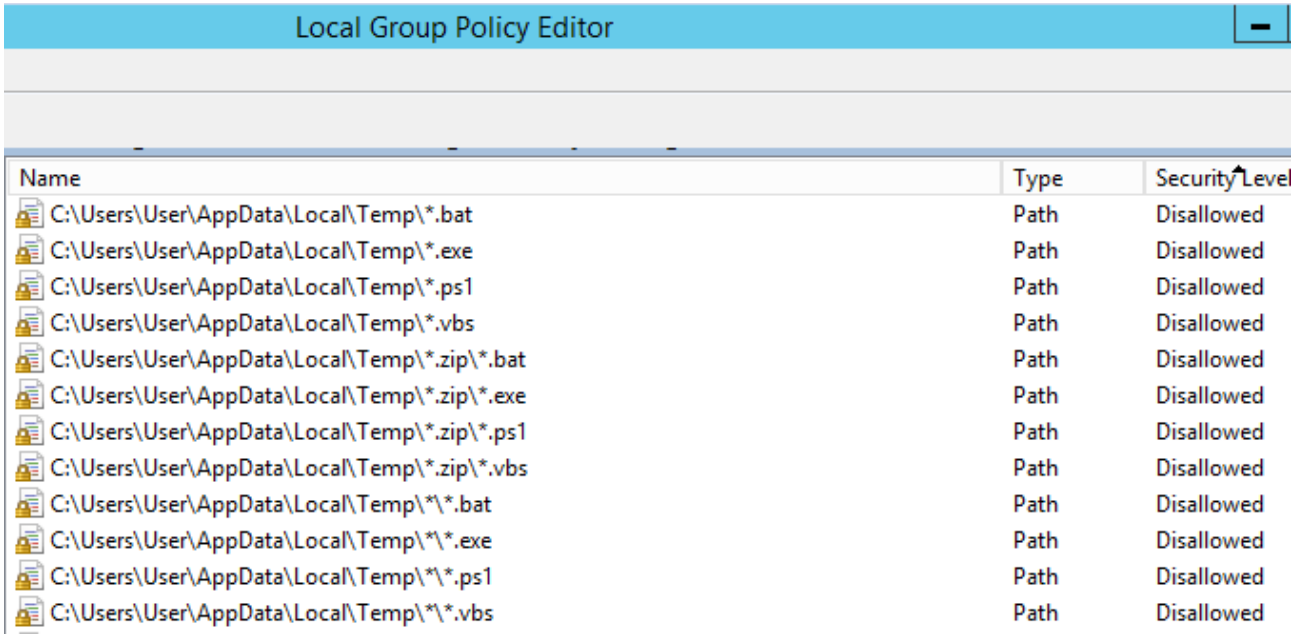
- Резервни копия – един от най-добрите подходи, за да не изгубим данните си, са резервните копия (backup). В случая на ransomware, при поразяване на някоя потребителска станция, всички файлове биват криптирани (фиг. 14). Обикновено извършителите изискват заплащане срещу отключване на файловете, но това не винаги е гаранция, че ще бъде изпратен ключ на потребителя, с който той да ги отключи. Най-добрият подход срещу подобен тип заплахи е наличието на направени резервни копия, от които може да се възстанови поразената информация.

Фиг. 14. CryptoLocker, един от първите ransomware-и

Един от най-ефективните методи за създаване на резервни копия е т.нар. стратегия 3-2-1, която ще разгледаме в следващата глава.

➢ Създаване на групови политики и Software Restriction Policy – груповите политики са инструмент за редица допълнителни настройки по операционната система. В корпоративна среда груповите политики се налагат централизирано на ниво домейн (активна директория), но могат да бъдат наложени и за всяка организационна единица поотделно. Тези конфигурационни политики могат да изиграят безценна роля, когато става въпрос за предпазване от malware чрез използване на Software Restriction Policies. Чрез тях може да бъде оказано в операционната система кои файлове са позволени за изпълнение, кои не са и от кои директории не могат да бъдат стартирани. Този метод на защита е лесен за изпълнение в големи и малки среди и е ефикасен, когато говорим за масови и нецеленасочени атаки. На фиг. 15 е показана конфигурация при Windows операционна система, при която е забранено изпълнението на .exe, .bat и други типове файлове от директорията %Temp%. При опит за изпълнение на файлове, идващи от Интернет, това е директорията, в която те временно се

записват. Чрез дефиниране на тези правила намалява вероятността да бъде изпълнен файл без реално потребителят да желае това.



Фиг. 15. Local Group Policy Editor

Когато говорим за групови политики в организацията има два подхода, които се използват при дефинирането на им:

- Blacklist (черен списък) – при този подход се забраняват само приложенията, типовете файлове и директориите, за които е ясно, че могат да доведат до евентуално изпълнение и заразяване със злонамерена програма;
- Whitelist (бял списък) – за разлика от черния списък, при този подход се разрешават единствено приложенията, които потребителя използва, т.е. всичко различно от позволените приложения и файлове няма да бъде изпълнено. По този начин вероятността компютърът да бъде заразен с malware е нищожен. Основното приложение на белия списък е в корпоративна среда. Някои организации използват този подход и за контрол на приложенията, които служителят може да изпълнява и по този начин всяко звено използва само необходимите за него софтуерни продукти.

2.6. Защита срещу атаки от тип социално инженерство

Както споменахме по-рано, човекът е най-слабото звено в сигурността на компютърните системи. Точно поради тази причина в последните години се обръща огромно внимание на обучението на персонала, така че потребителите да могат да разпознават, когато някое електронно писмо, съобщение или друга комуникация са измамни или приложението, което се опитват да инсталират, би могло да бъде злонамерено. Основните методи, с които човек може да се предпази от такива атаки или да смекчи ефекта им са:

- Ако не го очакваш, не го отваряй – това е често използвана фраза, която има за цел да предупреди потребителите, че не всяко писмо, което получават, е предназначено за тях и не всяко съобщение има невинен характер. В най-честия случай, подобни писма имат и прикачен файл, който при отваряне изисква допълнително действие от потребителя. Има начини, по които може да се разпознае подобно съобщение, но това изисква определено ниво на зрялост, когато става въпрос за ИТ и телекомуникации. Пример за това е когато при поздрав в началото на писмото не се използва името на човека, а потребителското му име (нарп. – „Здравейте, S.Ninov!“, вместо „Здравейте, г-н Нинов“ или подобен общоприет поздрав). При целенасочени атаки, разбира се, това е много по-трудно да се различи, понеже атакуващият знае точно на кого изпраща кореспонденция, как се казва даденият човек, с какво се занимава и т.н. Това е причината да се използва израза „Ако не го очакваш, не го отваряй!“.
- Когато бъде открита „изгубена“ флаш памет, CD или друга медия, не трябва да се прибързва и отваря на компютъра. В този случай е желателно да се използва виртуална среда (sandbox), на която да бъде отворено устройството, за да бъде избегнато заразяване на реалната среда. Друг подход, който може да се използва и наподобява sandbox, е откритата медия да бъде възпроизведена в изолирана виртуална мрежа. Подобно сегментиране на мрежи може да бъде постигнато със създаването на частни VLAN[16]-и и предотвратяване на

[16] VLAN – виртуална локална мрежа представлява логическа подмрежа, която може да бъде използвана за логическо групиране или изолиране на устройства, използвайки втория „Канален слой“ от OSI модела.

комуникация от и към тях чрез правила за достъп (ACL), дефинирани в маршрутизаторите, комутаторите или защитните стени.

➢ Двуфакторна автентикация – в случай че някой все пак успее да ни измами и да му предоставим по един или друг начин парола за достъп до даден ресурс, двуфакторната автентикация (2FA) може да се яви като пречка за атакуващия. 2FA се явява като допълнително ниво на защита за достъп до определена система. Работи по следния начин – след въвеждане на потребителско име и парола следва да се въведе и допълнителен автентикационен код, който се изпраща на посочена от потребителя електронна поща, мобилен телефон или на създадено за целта устройство, наречено токен (от англ. token). По този начин, за да достъпи даден ресурс, атакуващият трябва да притежава паролата на клиента, както и да има достъп до пощата, телефона му или до токена, за да може да узнае допълнителния код.

➢ Потребителската парола е за собствено ползване – предоставената парола за достъп до даден ресурс е само и единствено за ползване от потребителя, на когото е предоставена. В никакъв случай не трябва да се предоставяна на никого, дори някой да се представя за ИТ персонал, който се опитва да помогне с някакъв казус.

➢ Познавай колегите си – що се отнася до физическото естество на социалното инженерство, важно е всеки служител, посетител или обслужващ персонал да носи ID карта. Когато става въпрос за сграда, в която се контролира достъпа, е важно всеки един служител да се маркира на всяка врата, през която преминава. По този начин, когато атакуващият се опита да влезе, след легитимен служител и без да се маркира, веднага ще изпъкне като нарушител.

Изводи към втора глава:

1. Когато искаме да обърнем сериозно внимание на защитата на компютърните системи, основен „инструмент“ са потребителите. Постоянното обучение, следенето на тенденции, информираността като цяло повишават сигурността на човешкия фактор и по този начин подпомагат изграждането на една по-сигурна информационна среда.

2. Стремежът към разработване на по-сигурни приложения драстично намалява вероятността за пробив. При разработването на приложения бизнесът и сигурността трябва да се срещнат по средата и да се предприемат необходимите мерки за осигуряване на баланс между функционалност и сигурност.

3. Защитата от нерегламентиран достъп е процес, който не трябва да се приема като приключен след закупуването на съответния продукт или внедряването на конкретната методика. Той следва да е постоянен, цикличен и да се стреми към непрестанно подобрение.

4. Кибератаките не са проблем, който се наблюдава на персонално ниво, организация или държава, а са глобална заплаха. Необходимо е осъзнаване, че сами няма да успеем да спрем тази заплаха. Ако всеки индивидуално, ако всяка организация, независимо дали частна или правителствена, се погрижат да осигурят необходимото и адекватно ниво на защита, то кибер престъпниците ще имат много ограничена повърхност, която да експлоатират.

Глава трета: ПРИЛАГАНЕ НА ДОБРИ ПРАКТИКИ ЗА ЗАЩИТА НА КОМПЮТЪРНИ СИСТЕМИ И МРЕЖИ

3.1. Добри практики при изграждане защита на периметъра

В предната глава стана ясно, че универсално решение за сигурност няма, затова организациите залагат на многопластова защита. Тя е съставена от няколко нива на сигурност, които максимално да затруднят евентуалния опит за проникване в системите им.

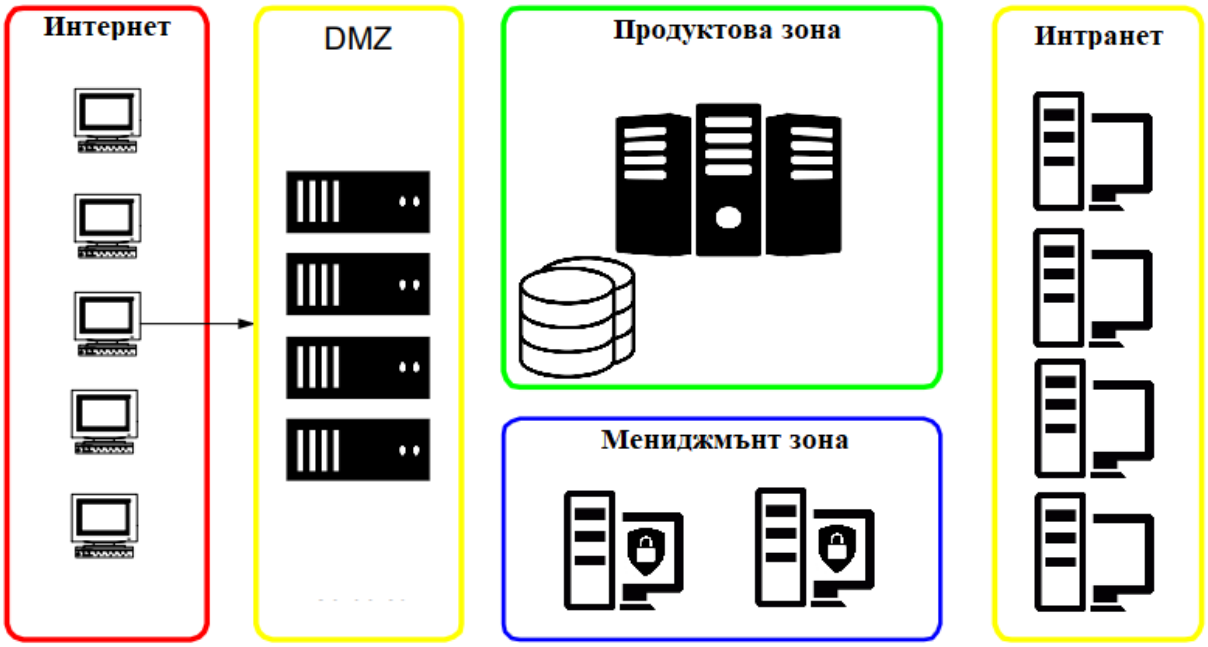
Традиционният подход за защита се състои в подсигуряване на периметъра, откъдето може да дойде евентуалната атака, и приемайки, че вътрешните потребители и системи са защитени, понеже злонамерените лица се намират извън тази граница. Този подход бързо започна да бъде отхвърлян с навлизането на BYOD и IoT. Оказа се, че подсигуряване на периметъра като единствено средство за защита, не е достатъчно, за да бъде изградена сигурна среда за потребителите и ИТ системите. Когато става въпрос за защита на периметъра, познаването и следването на добрите практики и съвременните тенденции може да донесе много позитиви.

3.1.1. Създаване на сегментирани зони за сигурност

Сегментирането по зони и филтрирането на трафика между тези зони е принцип, който се прилага от много време и е доказал своята ефективност, а главният инструмент за сигурност на информационните системи е управлението на защитни стени. Този подход може да доведе до сложни ситуации, ако няма добре дефинирана и приложима глобална схема. Тя трябва да даде общ изглед върху глобалния дизайн на ИТ инфраструктурата, да избегне създаването на излишни зони, да подпомогне оторизирания достъп до приложенията и да подобри управлението на мрежовото филтриране. Всичко това води до по-добър контрол върху мрежовата сигурност на по-ниска цена, като освен това поставя и контрола върху самата сигурност на правилното място, където всъщност ресурсите и активите ще бъдат защитени. Липсата на такава глобална схема би довело до появата на една много усложнена система с едновременното

съществуване на определен брой зони без ясна цел. В такава ситуация управлението на мрежовия поток може да се окаже доста трудно, особено с наличието на защитни стени, пълни с недокументирани правила, които никой не разбира напълно. Зоните, като минимум, трябва да бъдат дефинирани както следва (фиг. 16):

- Интернет – това е зона, която е извън контрола на коя да е организация или човек. От нея идват заявки от външни за компанията потребители към вътрешните ресурси, които предоставят някаква услуга.
- Демилитаризирана зона (DMZ) – зона, в която се намират компоненти на услуги или приложения, които трябва да бъдат публикувани в Интернет. Това обикновено включва уеб сървъри, пощенски сървъри, VPN услуги, DNS сървъри и други. За управление на демилитаризираната зона се препоръчва използването на две защитни стени – едната за управление на услугите, публикувани в Интернет, а другата – за контролиране на комуникацията с останалите зони.
- Продуктова зона – в нея следва да бъдат включени всички сървъри и устройства, както и техните бази данни, приложения и услуги, обслужващи нуждите на бизнеса. Тази зона трябва да има силно рестриктивен характер и правилата да са така дефинирани, че да допускат само оторизирани потребители.
- Мениджмънт зона – от тази зона следва да се извършват всички операции, свързани с администрирането на сървърите, приложенията и услугите. Тя също следва да бъде с рестриктивен характер и да допуска само оторизираните служители, отговорни за поддръжката и администрацията на сървърите и съпътстващите услуги.
- Интранет – частна широкообхватна зона, в която се намират работните станции на вътрешните потребители. Самата интранет зона също подлежи на сегментиране, което ще разгледаме като следваща точка.



Фиг. 16. Дефинирани зони за сигурност на инфраструктурно ниво

В зависимост от необходимостта за дефиниране на допълнителни нива за сигурност, също могат да бъдат създадени:

➢ Инфраструктурна зона – някои от функциите на мениджмънт зоната могат да бъдат допълнително сегментирани в инфраструктурната. В нея следва да се поставят компоненти, подпомагащи другите зони. Такива са терминални сървъри, инструменти за създаване на резервни копия и възстановяване на такива, мониторинг и т.н.

➢ Класифицирана продуктова зона – подобно на продуктовата зона, тази също съдържа услуги, които бизнеса използва. Целта на тази зона е да съдържа бази данни и приложения, за които е нужно допълнително ниво на изолация от всички други системи, тъй като пробив в подобен тип системи би имал катастрофално въздействие. Пример за такива системи са системите за финансово счетоводство, системите за управление на човешките ресурси или системи, в които се съдържа лична информация за клиентите на бизнеса.

➢ Индустриално контролни системи (ИКС[17]) – ИКС е система, най-често състояща се от софтуер (SCADA), програмируеми контролери (PLC),

[17]Индустриално контролна система – система създадена за наблюдение и контрол на даден индустриален процес.

сензори и задвижващи устройства (actuator). При наличие на такава система и необходимост от създаване на нова мрежова зона, то тя трябва да бъде отделена от всички останали. Обикновено ИКС е моделирана от три слоя – горен, който съдържа SCADA системите, среден, който съдържа PLC и долен, където се намират сензорите и задвижващите устройства. Базирано на това моделиране самата ИКС зона също подлежи на мрежово сегментиране като в чести случаи се използва същия модел, който е показан на фиг. 14. Единствената разлика е, че в интернет зоната реално се явяват бизнес потребителите, а в интранет зоната са хората и машините, осъществяващи мониторинг, контрол и техническо обслужване на системата (администратори, инженери и т.н.).

3.1.2. Сегментиране на вътрешната мрежа

Въпреки че вътрешната мрежа, било то интранет зоната или продуктовата зона, се счита за защитена и контролирана среда, тя също е препоръчително да бъде разделена на сегменти. Това се прави с цел ограничаване повърхността на атаката и намаляване на щетите от евентуална такава. Сегментирането може да бъде осъществено по два начина – виртуално или физически. Физическото е по-сигурно, но е по-трудно и по-скъпо за осъществяване, понеже всяка отделна мрежа използва различни устройства за свързаност и защита. Виртуалното разделяне на мрежи е по-популярният и по-използваният вариант, тъй като се използва по-малък брой устройства и една защитна стена, в която са терминирани правилата за достъп. То се осъществява чрез използването на частни виртуални локални мрежи (Private VLAN). На какъв принцип да бъдат разделени мрежите е процес, който изисква задълбочен преглед на инфраструктурата, но като практика се използват следните подходи:

- Според необходимостта за ползване на ресурс – различните мрежови сегменти могат да бъдат дефинирани според необходимостта за използване на даден ресурс. По този начин лесно може да се позволи достъп само до ресурсите, които са необходими за изпълнение на дадена задача. Всеки сегмент е изолиран от останалите, като по този начин при евентуално компрометиране на една

потребителска станция няма да бъдат подложени на риск и останалите станции и информационните системи.

- По организационна структура – в корпоративна среда често се наблюдава и необходимост от споделяне на ресурси между хора, намиращи се в едно и също звено. Поради тази причина един от подходите е разделяне на всяко звено със собствена подмрежа. Този похват се използва също и от администраторите за по-лесно инвентаризиране и мониторинг на активите, т.е. има ясно определени граници кое звено в кой мрежов сегмент се намира и докъде има достъп.

Сегментирането на мрежовата инфраструктура има и приложение, когато се внедри заедно с решение за Network Access Control. Всеки хост, който не покрива NAC политиките, бива поставен в изолирана мрежа, която няма достъп до каквито и да е вътрешни ресурси, докато не изпълни минималното изискване за включване във вътрешната мрежа. Същото важи и при включване на преносими устройства, които не са част от корпоративните. При включване на устройство, което не е дефинирано като сигурно, те се отделят в т.нар. „мрежа за гости“, която представлява отделен мрежов сегмент с ограничена свързаност и няма достъп до вътрешните ресурси, а само до Интернет.

Контролът на трафика между различните мрежови сегменти се осъществява с използването на защитни стени между тях. Добра практика е чрез използването на защитните стени във вътрешната мрежа да бъдат забранени всички портове, които не се използват, както и тези, за които се знае, че на тях работи приложение или услуга, съдържащи уязвимост. По този начин в мрежата ще се вижда трафик само от приложенията, които са предварително одобрени за работа, и всяко отклонение може да бъде възприемано като предупреждение за евентуален пробив.

3.2. Добри практики при създаване на резервни копия

Когато говорим за създаване на резервни копия, не винаги е достатъчно да копираме нашите данни повторно или да създадем резервно копие на друг логически дял. Резервните копия са един от сигурните начини за намаляване

ефекта от кибератаки, целящи унищожение на данни, както и от всякакъв тип бедствия, кражба или хардуерна повреда. Една от най-добрите практики за създаване на резервни копия е чрез следване на правилото „3-2-1“. Това правило гласи да се пазят поне три копия на данните, две от които да са на различни носители, и едно да бъде съхранявано в отдалечена локация.

- Поне 3 копия на данните – под три копия се има предвид оригиналните данни и две резервни копия.
- 2 от тях на различни носители – когато резервните копия се намират на един и същ тип носител (като пример – твърд диск), вероятността един криптовирус да порази данните и резервното копие е огромна. За намаляване вероятността от загуба на информация се препоръчва едното резервно копие да се съдържа на друг носител като външен твърд диск, CD/DVD, лентова библиотека и т.н.
- 1 да бъде съхранявано в отдалечена локация – тази стъпка важи основно, когато има опасност от някакво бедствие на локално ниво. По този начин, в случай че това бедствие се осъществи, то едно от резервните копия ще е защитено.

3.3. Провеждане на тестове за проникване и етично хакерство

Най-добрата защита е доброто нападение. Двата термина „тест за проникване“ и „етично хакерство“ са близки по значение и понякога се използват като взаимнозаменяеми, но всъщност не означават едно и също нещо. Докато целта и на двете е да се извърши проверка на сигурността и да се идентифицират потенциални уязвимости и слаби места в мрежовата, сървърната инфраструктура, уеб приложенията или в информационните системи, реално тестовете за проникване са част от процеса, наречен етично хакерство. Етичното хакерство включва всички техники, които могат да бъдат използвани за компрометиране на сигурността в дадена организация, докато тестовете за проникване са по-фокусирани върху откриване на определена уязвимост. При по-подробно разглеждане на разликите между двете, етичното хакерство има за цел да тества сигурността, използвайки всевъзможен вектор на атаката, всякакви

средства и подходи от социално инженерство до разработване на конкретен 0-Day malware. Тестовете за проникване, от друга страна, се правят в по-малък обхват, т.е. правят се тестове за пробив или намиране на уязвимост в уеб приложение, ИТ инфраструктура, безжична мрежа или в дадена информационна система.

Един от най-ефективните подходи за повишаване сигурността в конкретна точка на ИТ инфраструктурата е регулярното провеждане на тестове за проникване. Процесът по проникване основно се разделя на 5 фази:

- Разузнаване – тази фаза включва събиране на предварителна информация за целта, която е обект на тест, и планиране на следващи стъпки, базирани на събраната информация. Двата метода за разузнаване и събиране на информация са активен и пасивен. Активният метод включва директен контакт със системите, които са цел на теста, с помощта на различни инструменти. Те могат да ни помогнат да установим IP адресни пространства на предлаганите услуги, DNS записи, домейн имена, какъв пощенски сървър се използва и т.н. Пасивното разузнаване се състои в използването на т.нар. посредник. Под посредник в случая се има предвид интернет търсачките (Google, Bing), публично достъпна информация за целта, бази данни с информация за публични IP адреси и собственици на домейни. На фиг. 17 е изведен резултат за домейн unibit.bg, използвайки публично достъпна информация от регистъра за област „**.bg**“. Използвайки информацията от регистъра, към момента имаме представа кой е контактното лице за този домейн, как се образуват потребителските имена на служителите в УниБИТ и къде е физическата локация на организацията. Целта на разузнавателната фаза е да се ориентираме в организацията, да се сдобием с имена, позиции и пощенски адреси на ключови хора, да опознаем бизнеса на компанията и т.н. В тази фаза е възможно да се приложи и метода на социалното инженерство във вид на обаждания по телефона и събиране на информация за служители, изпълнително ръководство, договори и други.

Фиг. 17. Публично достъпна информация за домейн ***unibit.bg***

➢ Сканиране – фазата включва прилагане на технически средства за събиране на допълнителна информация. Разликата между първата и тази фаза е, че в текущата се търси информация, която е свързана с информационните системи или ИТ инфраструктурата на компанията. Използват се инструменти за сканиране на отворени портове и техните услуги, уязвимости в приложения, версии на операционни системи, уязвимости в операционните системи, проверка на възможностите за SQL инжектиране и други. Популярен подход при откриване на уязвимости е чрез използването на решения (софтуери или платформи) за управление на уязвимостите.

➢ Получаване на достъп – това е целта при осъществяване на всяка една атака. Чрез използване на получената от предходните фази информация се прилага подходящ метод за придобиване на достъп до мрежата или до някое крайно устройство. Използването на някои от методите за атака, описани в първата глава, също могат да доведат до тази фаза. Веднъж след като е получен достъп до мрежата, отново може да се приложи сканиране, за да се очертае структурата на вътрешната мрежа и да се направи подготовка за следващата фаза. Тестовете за проникване на периметъра спират до тази стъпка, тъй като се счита, че уязвимостта е открита и нейното затваряне ще доведе до елиминиране на заплахата.

➢ Поддържане на достъп - при правилно сегментирана и добре защитена вътрешна мрежа, добиването на достъп по време на предходната фаза не е достатъчно за атакуващия, за да се сдобие с полезна информация. Затова следва да се потърси начин този достъп да остане постоянен, докато не се открие нужната информация или не се извлече необходимото количество от нея. Освен търсене на допълнителна уязвимост, целта по време на тази фаза е да бъдат изпитани вътрешните средства за мониторинг. Хората, които провеждат тестовете, трябва да са способни да си създават нови пътища (backdoors), по които да достъпват мрежата, да се опитат да увеличат правата си върху мрежата и системите и т.н., без да бъдат засечени от администраторите или от вътрешните средства за мониторинг.

➢ Покриване на следите – това е последната техническа фаза от процеса. След постигане на необходимата цел следва да се прикрият всякакви следи, които може да са оставени по време на теста, т.е. да се премахнат евентуално направените промени по конфигурациите на устройствата, новосъздадените акаунти, административни права, промяна на съдържанието на дневниците (лог файловете) и всички останали модификации, които са били направени по време на теста. По този начин може да се провери и компетентността на служителите, които отговарят за сигурността.

➢ Документиране – това е допълнителна фаза, която съпровожда всяка от разгледаните до сега. Документирането на всяка една стъпка от процеса е критично за постигане на позитивен резултат от тестовете и може да послужи като доказателство и успокоение за организацията, че няма извлечена, променена или изтрита информация по време на теста. Допълнително тази документация трябва да бъде част от доклад, който се издава в края на тестовете и има за цел да съдържа констатации и заключение за нивото на сигурност, както и за необходимите мерки, които трябва да се предприемат за подсигуряване на средата.

Когато говорим за тестове за проникване и етично хакерство, има три подхода, които могат да се приложат:

➢ Подход тип „черна кутия“ (Black Box) – при този подход теста за проникване се прави без да се предоставя предварителна информация за нивото на сигурност в организацията, т.е. имитира модел на проникване, какъвто би бил при опит за истинска атака. Уведомява се само управленското ръководство на организацията и част от ИТ персонала.

➢ Подход тип „бяла кутия“ (White Box) – за разлика от подхода тип „черна кутия“, при този се предоставя доста по-голямо количество информация за организацията, приложенията и системите. Целта на този подход е да бъде организиран и по-целенасочен. Имитира вида на атаката, каквато би била, ако вътрешен човек се опита да я изпълни. Предполага се, че недоволен бивш служител на компанията би имал необходимите знания за организацията и системите, които тя използва.

➢ Подход тип „сива кутия“ (Gray Box) – представлява хибрид между предходните два подхода. Състои се от екип, който се опитва да проникне отвън, и друг екип, който има достъп до вътрешната мрежа. Екипите споделят информация помежду си, за да се опитат да осъществят успешна атака върху системите. Идеята е да се възпроизведе евентуалния сценарий вътрешен човек да работи със злонамерено лице извън организацията.

3.4. Управление и оценка на уязвимости

Управлението на уязвимости е процес по идентифициране, приоритизиране, поправяне и докладване на уязвимости в ИТ инфраструктурата, операционните системи, базите данни и приложенията. Сканирането за уязвимости е част от тестовете за проникване, но много организации усвояват този подход като отделна мярка за допълнителна сигурност на системите. За разлика от етичното хакерство и тестовете за проникване, управлението на уязвимости е пасивно и при него човешката намеса е ограничена. Самият процес по оценка на уязвимостите включва инвентаризация на всички ИТ активи в организацията, класифицирането им на база бизнес роля и критичност за бизнеса, след което се извършва сканиране и идентифициране на познати уязвимости на всеки един от откритите активи. След констатация на уязвимостите те се

приоритизират спрямо определени критерии и се сортират по ниво на заплаха. Това ниво зависи от вида на откритите уязвимости и дали те могат да бъдат експлоатирани или не. Разбира се системите за управление на уязвимости нямат информация за всички съществуващи експлойти и е трудно да се прецени дали дадена уязвимост ще доведе до заплаха. Това би могло да бъде установено след идентифициране на текущите слабости и чрез провеждането на тест за проникване.

➢ Самите системи за управление на уязвимости могат да са какво физически, така и виртуални. Неизбежно един от основните компоненти на такава система е скенерът за уязвимости, който съдържа информация за всички познати до момента уязвимости и за това как те да бъдат открити. При внедряване на такава система първоначалното сканиране ще провери всеки актив и неговото състояние, изпращайки ICMP пакет към него. Допълнително ще сканира отворените портове и ще покаже услугите, които работят на всяка от машините. Някои системи имат възможност за въвеждане на потребителски акаунт, с който да се свържат към дадена система и да съберат допълнителна информация. Идентифицираните системи се изследват за дистрибуция и версия на операционната система, отворени портове, услуги, инсталиран софтуер, потребителски акаунти, които имат достъп до тях, файлови системи и т.н. Със събраната информация се прави корелация с база данни на познатите уязвимости и се пристъпва към следващия етап.

➢ След като уязвимостите са идентифицирани те се сортират и приоритизират спрямо риска, който носят за организацията. Различните решения за управление на уязвимостите имат дефинирани свои критерии, по които определят нивото на заплаха, но обикновено се водят по стандарта CVSS (Common Vulnerability Scoring System). CVSS представлява рамка за оценка на опасността, която дадена уязвимост представлява. В общия случай оценките варират от 0 до 10, където уязвимост с рейтинг 0 носи най-ниска опасност, а респективно 10 – най-висока. Метриката се изчислява, базирано на няколко компонента, които включват:

- вектор на атаката за конкретната уязвимост;

- колко и кои принципи на информационната сигурност могат да бъдат нарушени;
- необходими ли са администраторски права за изпълнение на атака;
- изисква ли се допълнително действие от потребител за осъществяване на атака;
- какво е нивото на трудност за изпълнение на атака;
- уязвимостта може ли да се експлоатира от Интернет;
- има ли разработен експлойт за конкретната уязвимост и т.н.

➢ След приоритизирането на уязвимостите следваща стъпка в процеса е те да бъдат третирани според нивото на заплаха, което носят. Има два основни подхода за справяне с уязвимостите:

- Поправяне – пълно елиминиране на съществуващата уязвимост. Това е постижимо само при наличие на актуализация или обновление, което поправя уязвимостта;
- Смекчаване – когато няма налична актуализация, адресираща уязвимостта, могат да се предприемат други стъпки за намаляване вероятността тази уязвимост да бъде използвана. Такива стъпки са спиране на портове и услуги, промяна конфигурацията на мрежовите устройства, поставянето на уязвимия хост в изолирана мрежа и други.

➢ Накрая на процеса е докладването на уязвимости. То може да бъде на оперативно и управленско ниво. Обикновено продуктите и платформите за управление на уязвимостите се достъпват през уеб интерфейс. Както е показано на фиг. 18, през него могат да се визуализират текущите резултати от сканиранията, така че администраторът по сигурността да може лесно и бързо да проследи какво е текущото състояние.

Фиг. 18. Доклад с нивата и типовете на откритите уязвимости

3.5. Подобряване сигурността на сървъри и работни станции

В резултат на разгледаните до тук типове и вектори на атаките, целящи неоторизиран достъп до информация, може да се заключи, че освен експлоатиране на уязвимост, другият вариант е компрометиране на потребителските акаунти и станции. За подобряване на сигурността в това направление могат да се приложат следните добри практики:

➢ Администраторски права – една от най-ефикасните практики за защита на ниво локална машина е ограничаването на администраторските права върху работните станции на потребителите. Налагайки подобни ограничения,

евентуалният нарушител, получил неоторизиран достъп до компютърната станция или потребителска парола, няма да има възможност за изпълнение на скриптове и инсталация на програми върху средата. Права следва да се предоставят само на служителите, които отговарят за поддръжката на тези станции.

➢ Използване на различни акаунти за администриране – в зависимост от системата, която следва да се достъпи, системните и мрежовите администратори, както и администраторите по сигурността трябва да имат различни потребителски акаунти:

- Стандартен акаунт – потребителски акаунт, който се използва от администратора за логване в работния си терминал и изпълнение на всекидневни задължения;
- Акаунт за работни станции – този акаунт служи за административни дейности, свързани с работните станции на потребителите;
- Акаунт за сървърни станции – акаунт, който се използва за администриране на сървъри;
- Домейн администратор – това е акаунт, който служи само за дейности, свързани с администриране на домейн сървърите или услугите.

Като правило, домейн администратор акаунтът никога не трябва да се логва на потребителски станции или сървъри, които не обслужват домейн услуги. Съответно акаунтите за сървърно администриране не трябва да се логват на работните станции, а тези за администриране на компютрите не трябва да имат права върху сървърите. Използването на тази практика намалява вероятността атакуващият да използва потребителското име и парола или компютъра на съответния служител, за да ескалира правата си и да получи достъп до по-защитена система.

3.6. Централизиран мониторинг чрез използване на SIEM

Когато говорим за добри практики в централизираното управление на ИТ инфраструктурата, правилно изградения мониторинг е неотлъчна част и един

от компонентите, които имат най-голяма стойност. Стандартният подход за наблюдение и анализ на събития е чрез използването на IDS (Intrusion Detection System) системи за откриване на нарушения, но когато говорим за холистичен поглед, внедряването и правилната конфигурация на SIEM система за наблюдение на трафика от устройствата е ключовият елемент за контрол и превенция. SIEM (Security Information and Event Management) системите са софтуерни решения, които се използват за централизирано наблюдение на всички събития в ИТ инфраструктурата. Такива системи обикновено се внедряват в организации, където се търси съответствие с даден стандарт, но освен това SIEM системите предлагат допълнително ниво на сигурност чрез наблюдение и корелация на събития от множество устройства. Правилният подход при внедряването на такава система включва:

- Конфигуриране на източниците на данни – събиране на събития от маршрутизатори, защитни стени, трафика, минаващ през тях (NetFlow), IDS, дневниците със събития от операционните системи на сървъри и работни станции, пощенските сървъри, бази данни, антивирусни решения и други;
- Нормализиране на трафика – определяне на нормалното поведение на системите и мрежовия поток, съпроводено от наблюдение за аномалии;
- Корелация на събития от различите устройства – като пример за корелация е предупреждение, което се появява при наличие на трафик по рядко използван порт, съпроводен от 5 грешни опита за потребителско достъпване на система X, като опитите са с 3 или повече различни потребителски имена и идват от един и същ IP адрес в рамките на последните 15 минути.
- Последващо създаване на допълнителни правила за корелация и конфигуриране на конкретни случаи за вдигане на аларма – ръчното създаване на правила за корелация изисква познаване на последователността от действия и методологията на даден тип атака. Има възможност за откриване на ботнет трафик, измамни DNS и релейни сървъри, нерегламентирано използване на акаунти и т.н.

Разликата между SIEM и другите системи за откриване и превенция е, че SIEM наблюдава на всички нива от OSI модела. При коректно внедряване в

инфраструктурата, тези решения отварят възможност за разпознаване на атаката още преди да е изпълнена или доведена до край. По този начин SIEM може и да подобри сигурността, като даде отправна точка за подобрение на мерките за защита. Въпреки ползите, които SIEM решенията носят, те са по-скоро реактивни, отколкото проактивни системи.

Изводи към трета глава:

1. Добрите практики представляват добре отъпканият път, по който всички се стремят да минават. Те не са предназначени за безусловно следване, а целта им е да покажат как да се извлече оптималното от вече направени стъпки. Добрите практики не са приложими навсякъде и на сто процента, но са отправна точка при осигуряване на по-защитена среда.

2. Когато говорим за изграждане на механизми за сигурност, защитаването единствено на периметъра или на части от него вече не е достатъчно. Дори с изграждане на многопластова сигурност предотвратяването на заплахите не може да бъде напълно гарантирано. За постигане на ефективно и ефикасно решение са нужни комплексни методи, включващи както защитен параметър, така и добре структурирана вътрешна мрежа.

3. Необходимо е осъзнаване, че дейността на етичните хакери има стойност. Техните знания, методи и практики са предназначени да ни помогнат да предотвратим действията на недобронамерените лица, които търсят начини за нерегламентиран достъп до нашите данни.

4. Пробив на мрежовата сигурност и компютърните системи не е въпрос на „дали“, а по-скоро на „кога“. Залагането на механизми за възстановяване е задължителен елемент, за да сме подготвени, когато този момент настъпи.

Заключение

Когато става въпрос за сигурност на компютърните системи и мрежи, ние трябва да сме прави всеки път, докато атакуващият трябва да бъде прав само веднъж. За него това е достатъчно, за да се сдобие с достъп до нашата мрежа, а веднъж стане ли това, щетите може да са огромни. В настоящата дипломна работа са разгледани само част от многобройните разновидности на компютърните атаки срещу мрежи, системи и потребители, както и основните методи, с които можем да се защитим. Развитието на съвременните технологии налага постоянен стремеж към модернизиране на мерките за сигурност, качествено интегриране и наблюдение. Това от своя страна следва да повиши нивото на зрелост на организациите (правителствени и неправителствени), когато става въпрос за киберсигурност. По този начин, когато настъпи инцидент, свързан със сигурността, то те ще са организационно и технически подготвени да реагират адекватно, за да възстановят контрол над системите си. Сигурността е отговорност на всички ползватели на компютърни системи и електронни услуги. С общи усилия може да се постигне такова ниво на сигурност, което да затрудни дори най-вещите нападатели, а когато усилието е по-голямо от извлечената полза, атаката се обезсмисля.

Настоящата работа представи най-широко разпространените атаки срещу компютърните системи и мрежи, описа използваните методи за защита и доказа как чрез имплементиране на конкретен тип средства интегритета, конфиденциалността и достъпността на информацията могат да бъдат запазени. Използването на защитна стена за уеб приложенията защитава интегритета на информацията, съдържаща се в базата данни; load balancer и DDoS смекчаващите устройства осигуряват достъпност, а употребата на протоколи за сигурност гарантира конфиденциалността и т.н. Текущият труд също така даде поглед върху добрите практики, прилагани за защита на специфични елементи от ИТ инфраструктурата, както и такива за цялостен поглед върху сигурността. За всяка от разгледаните добри практики са посочени последователност от действия,

които да спомогнат за правилното внедряване и приложение на ефективни мерки за сигурност.

Общи изводи:

1. Имплементирането на едно средство, един метод или една-единствена добра практика не е достатъчно за едновременното спазване и на трите принципа на информационната сигурност. За адекватното запазване на конфиденциалността, интегритета и достъпността на информацията следва да бъде използван комплексен набор от средства и методи, които в комбинация да могат да гарантират оптимален резултат.

2. С все по-нарастващата роля на информационните технологии в ежедневния живот расте и отговорността на потребителите към опазването на информацията и ресурсите, които използват. Те следва да са адекватно информирани за това, което се изисква от тях, както и за тенденциите в развитието на информационната сигурност на потребителско ниво.

3. С цел минимизиране усилията от страна на потребителя при използване на информационните системи, разработчиците често залагат по-скоро на системната функционалност, отколкото на системната сигурност. Както при всяка крайност, прекаленото наблягане върху един аспект се превръща от удобство за едни във възможност за други.

4. Приемането на GDPR[18] поставя нови предизвикателства в сферата на информационната сигурност. С разширяване на понятието „лични данни“ корпоративните политики за защита на информацията ще бъдат адекватно променени. Това ще наложи развитието и въвеждането на нови подходи към защитата на компютърните системи и мрежи и информацията като цяло.

Препоръки:

1. Сигурността е от основно значение за коректното функциониране на всяка организация, но тя не следва да е прекалено рестриктивна за потребителя, тъй като негов естествен инстинкт е да заобиколи наложените му ограничения за

[18] GDPR – Regulation EU 2016/679. Регулаторна рамка за защита на личната информация в границите на ЕС.

по-лесно изпълнение на поставените му задачи. Сигурността и функционалността трябва да са в равноправни отношения при изграждането на информационните системи.

2. Техническите мерки за сигурност трябва да бъдат комбинирани с управленски такива. Трябва да се провеждат редовни обучения на хората, отговарящи директно за сигурността, както и на ползвателите на информационните системи.

3. Тестовете за проникване и цялостната оценка на риска е препоръчително да бъдат извършвани на всеки три месеца, а сканирането за уязвимости – ежемесечно. За целта трябва да се изготви официален план, който да включва период, обхват и начини за провеждане на посочените дейности.

4. Трябва да се насърчи проактивността в областта на киберсигурността. Могат да бъдат организирани срещи и посещения на експерти в университети и специализирани училища. Това от една страна ще повиши осведомеността на една от най-големите таргет групи, а именно млади хора, които все още не осъзнават важността на това информацията им да е добре защитена. От друга страна ще представи киберсигурността в нова по-разбираема светлина, което би повишило интереса към тази област на съвременната наука. Подобни посещения биха могли да прераснат в професионално взаимодействие, което да даде на експертите нови идеи, а на младите хора – амбиция за развитие.

5. Периодичното напомняне за сериозността на последиците от атака не бива да ни плашат и съответно да следваме принципа „ако не го разбирам, го избягвам“. Трябва да се осъзнае, че в случая правилният подход не е да бягаме от непознатото, а да се научим да го използваме правилно и ефективно.

Освен посочените в настоящата работа методи за защита, съществуват и други, по-централизирани решения за киберсигурност, които напълно да защитят нашите данни, било то по отношение на обикновен потребител, или на цяла компания. Повечето хора смятат, че подобно решение са облачните услуги, но в края на краищата всичко, което е създадено от човек, може да бъде разрушено от него. Не съществува напълно сигурна среда и колкото по-бързо разберем това, толкова по-бързо ще се научим как да предпазим себе си.

ИЗПОЛЗВАНИ ИЗТОЧНИЦИ

Източници от печатни издания:

1. Целков, Веселин, Исмаилов, Орхан. Сигурност на информацията. София, „За буквите-О писменехь“, 2017, ISBN 978-619-185-253-6.
2. Целков, Веселин, Стоянов, Николай, Исмаилов, Орхан. Управление на риска, тестване и оценка на мрежовата и информационната сигурност. София, „За буквите-О писменехь“, 2016, ISBN 978-619-185-159-1.

Уеб ресурси:

3. Roose, Kevin. Real Future Episode 8. 24 Feb 16. 26 Feb 17. <http://fusion.net/story/281543/real-future-episode-8-hack-attack/>.
4. The European Union Agency for Network and Information Security. 31 Oct 17. <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary>.
5. Herzberg, Ben., Bekerman, Dima., Zeifman, Igal. Breaking Down Mirai: An IoT DDoS Botnet Analysis. 26 Oct 16. 30 May 18. <https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html>.
6. Fox-Brewster, Thomas. An NSA Cyber Weapon. 12 May 17. 07 Nov 17. <https://www.forbes.com/sites/thomasbrewster/2017/05/12/nsa-exploit-used-by-wannacry-ransomware-in-global-explosion/#603e7d5e599b>.
7. Noerenberg, Erika., Costis, Andrew. 16 May 17. 16 Nov 17. <https://logrhythm.com/blog/a-technical-analysis-of-wannacry-ransomware/>.
8. Cimpanu, Catalin. Over 98% of all WannaCry victims were using Windows 7. 20 May 17. 13 Feb 18. <https://www.bleepingcomputer.com/news/security/over-98-percent-of-all-wannacry-victims-were-using-windows-7/>.
9. McDowell, Mindi. Understanding DoS Attacks. 04 Nov 09. 14 Nov 17. <https://www.us-cert.gov/ncas/tips/ST04-015>.
10. Khandelwal, Swati. World’s largest 1 Tbps DDoS attack. 27 Sept 16. 14 Nov 17. <http://thehackernews.com/2016/09/ddos-attack-iot.html>.

11. Paganini, Pierluigi. 150,000 IoT Devices behind the 1Tbps DDoS attack on OVH. 27 Sept 16. 14 Nov 17. <http://securityaffairs.co/wordpress/51726/cyber-crime/ovh-hit-botnet-iot.html>.
12. Fisher, Dennis. What is a Man-in-the-Middle Attack. 10 Apr 13. 15 Nov 17. <https://blog.kaspersky.com/man-in-the-middle-attack/1613/>.
13. Imperva. Social Engineering. 16 Nov 17. <https://www.incapsula.com/web-application-security/social-engineering-attack.html>.
14. Musthaler, Linda. Best practices to mitigate DDoS attacks. 10 Jan 13. 17 Nov 17. <http://www.networkworld.com/article/2162683/infrastructure-management/best-practices-to-mitigate-ddos-attacks.html>.
15. Jelic, Filip. Man in the middle attacks. 10 Oct 16. 17 Nov 17. <https://www.deepdotweb.com/2016/10/10/man-in-the-middle-attacks/>.
16. How Antivirus Works. 18 Nov 17. <https://antivirus.comodo.com/how-antivirus-software-works.php>.
17. Peterson, Curtis. 23 Social Engineering Attacks You Need To Shut Down. 16 March 16. 20 Nov 17. <https://www.smartfile.com/blog/social-engineering-attacks/>.
18. Krebs, Brian. DDos on Dyn Impacts Twitter and Spotify. 16 Oct 16. 03 Nov 17. <https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/>.
19. Son, Do. Hackers successfully penetrated BSNL intranet, over 47000 employees info were leaked. 06 Mar 18. 17 Apr 18. <https://securityonline.info/hackers-successfully-penetrated-bsnl-intranet-over-47000-employees-info-were-leaked/>.
20. Khalimonenko, Alexander., Kurpeev, Oleg., Ilganaev, Kirill. DDoS attacks in Q4 2017. 06 Feb 18. 29 Apr 18 <https://securelist.com/ddos-attacks-in-q4-2017/83729/>.

21. Metivier, Becky. Network Segmentation: Considerations for Design. 16 Jun 17. 30 Apr 18. <https://www.sagedatasecurity.com/blog/network-segmentation-considerations-for-design>.
22. Wichers, Dave. SQL Injection Prevention Cheat Sheet. 06 Feb 18. 02 May 18 <https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet>
23. Allen, Lee. Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide. Packt Publishing Ltd. ISBN 978-1-84951-774-4.
24. Common Vulnerability Scoring System v3.0: User Guide. 03 May 18 <https://www.first.org/cvss/user-guide>
25. Leal, Rhand. Requirement to implement network segregation according to ISO 27001 control A.13.1.3. 02 Nov 15. 04 May 18 <https://advisera.com/27001academy/blog/2015/11/02/requirements-to-implement-network-segregation-according-to-iso-27001-control-a-13-1-3/>.

ИЗПОЛЗВАНИ СЪКРАЩЕНИЯ

2FA	Two Factor Authentication
ACK	Acknowledge
ACL	Access Control List
ARP	Address Resolution Protocol
BYOD	Bring Your Own Device
C&C	Command & Control
CCTV	Closed Circuit Television
CD	Compact Disk
DDoS	Distributed Denial of Service
DNS	Domain Name System
DNSSEC	Domain Name System Security
DoS	Denial of Service
GDPR	General Data Protection Regulation
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IoT	Internet of Things
MAC	Media Access Control
MitB	Man-in-the-Browser
MitM	Man-in-the-Middle
NAC	Network Access Control
NGFW	Next Generation Firewall
NSA	National Security Agency
OSI	Open Systems Interconnection
PKI	Public Key Infrastructure
SMB	Server Message Block
SSL	Secure Socket Layer

SQL	Structured Query Language
SQLi	Structured Query Language Injection
SYN	Synchronize
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
USB	Universal Serial Bus
WAF	Web Application Firewall
XSS	Cross-site scripting