
Факултет по Информационни Науки

# МАГИСТЪРСКА ТЕЗА

**НА ТЕМА:**

**Защита на данните в Интернет среда**

**Дипломант:** Милена Гикова

**Научен ръководител:** Проф. Д-р Георги Петров Димитров

**Специалност:** Софтуерна архитектура и управление на качеството

**София 2018г.**

## Резюме

Основаната цел в настоящата магистърска теза е да бъде описано подробно какви заплахи съществуват в Интернет средата, по какъв начин неоторизирани лица могат да присвоят конфиденциална информация и как потребителите могат да предпазят своите лични данни, които съхраняват там, най-вече при иновацията в ИТ индустрията- Internet of Things.

Работата се състои от 106 страници, състоящи се от въведение, изложение и заключение. В началото е поместен списък с използваните съкращения и кратко резюме.

Във въведението е описано и разгледано накратко каква е основния принцип на обмен на Интернет данни и защо е толкова важно да се защитаваме и предпазваме от неоторизан достъп там. Също така до каква степен е променило ежедневието и бита ни и до колко е полезно за нас днес.

Моето изложение със състои от четири глави.

В първа глава е представена кратък исторически преглед на развитието на Интернет и комуникационните мрежи през годините както и принципа на работа. Поставен е и въпроса свързан със защитата на Интернет данни в наши дни.

Във втора глава са описани подробно различните видове неторизиран достъп, последствията които биха могли да бъдат причинени ако кибератаката е била успешна. Повече внимание е обърнато и на

последните най-сериозни кибер атаки за последната година и също какво са очакванията за в бъдеще.

В трета глава се набляга на описанието на прости практики и съвети, които обаче биха могли да бъдат много полезни и в даден момент да ни спасят от евентуално хакване /неоторизан достъп/. Също така предоставям на потребителя възможността на подбере най-подходящия вид софтуер, който би могъл да предостави необходимата сигурност на неговите данни, особено ако е в корпоративна среда. Разгледани са различните видове VPN протоколи.

В четвърта глава е дадено решение за защитата на Internet of Things, чрез употребата на VPN връзка.

В заключение е описано предимството на използвания софтуер и потвърждение на неговата необходимост.

## Съдържание

## Списък на използваните съкращения

**VPN -** Virtual private network /Виртуална частна мрежа /

**ARP -** Address resolution protocol

**NAT -** Network address translation /Преобразувател на мрежови адреси/

**PAT -** Port address translation / Преобразувател на портове/

**SSL -** Secure sockets layer

**TLS -** Transport layer security

**TCP –** Transmission control protocol

**UDP –** User datagram protocol

**WAN** – Wide area network /мрежа с голям обхват/

**IPSec** – Internet protocol security

**L2TP** – Layer 2 tunneling protocol

**L2F** – Layer 2 forwarding

**PPTP** – Point to point tunneling protocol

**HTTP** - Hypertext transfer protocol

**HTTPS** - Hypertext transfer protocol secure

**IP –** Internet protocol

**DHCP –** Dynamic host configuration protocol

**OSI –** Open systems interconnections

**ICMP** – Internet control message protocol

**QoS** – Quality of service

**HTML** – Hyper text markup language

**DNS** – Domain name system

**NSF -** National Science Foundation /Национална академична фондация/

**IDS -** Intrusion detection system

**NIST** – National institute of standard and technologies /Национален институт за стандарти и технологии/

## УВОД

Животът ни днес е неизменно свързан със светът на технологиите. В това число се включват не само телекомуникационните устройства като телефони, компютри, таблети, а и всички електроуреди, благодарение на които нашия живот е улеснен и оптимизиран. Разбира се, че в миналото нещата не са били същите и хората не са живели по този начин с всички тези удобства.

Благодарение на развиващите се технологии днес, хората се запознават в Интернет, пазаруват онлайн от там. Развива и обогатява социалните контакти на хората, улеснява изпълнението на ежедневните битови дейности като плащане на сметки, Могат да бъдат изброени безкрайно много предимства, които Интернет дава на хората днес. Аз смятам, че хората са го приели като даденост, като нещо което сякаш винаги го е имало и не биха могли да си представят живота без, например, всички социални мрежи като Facebook, Instagram и Twitter. Интернет, разбира се, дава и много други предимства. Истината е че, никой от съвременните потребители на 21-ви век, не би даже предположил, какво всъщност стои зад тяхната мигновена комуникация в социалните мрежи (като например

Instant messaging).

Комуникацията между хората става бърза и лесна. Но как е било преди? Например, целия процес на писане на писмо до някого, който е в друг град. Колко ли време е отнемало на нашите прадеди да се свържат един с друг и да споделят своите чувства, емоции и вълнения тогава. Днес един имейл може да бъде изпратен за броени минути и то до всяка една точка на света. Може би никой не е предполагал, че точно тази сфера ще се развие до такова ниво.

В какво всъщност се състои това? Интернет е създаден на базата на сложна комуникационна мрежа, изградена от милиарди свързани хардуерни устройства по целия свят. За хармоничното функциониране на тази система, през годините след създаването му, се налагат хиляди правила, формулирани в така наречените комуникационни протоколи. В следващите глави ще бъде подробно описано и разгледано както принцип на работа, така и развитието до днес.

**Проблеми**

Изграждането на такъв тип комуникационна система, никога не е съвършено. Поради тази причина, в тази област има голям проблем със сигурността на данните. Това ме накара да избера точно тази тема: за зашитата на данните в Интернет среда. Голяма част от хората, дори не се замислят всъщност, колко би било опасно за тях, когато са в Интернет

мрежата и използват конфиденциална информация като своите лични данни например. Именно неосведомеността е нещото, от което се възползват злонамерените лица. Хората много често не подхождат отговорно към това и всеки се казва „ Да бе да ама на мен това няма как да ми се случи“.

Сигурността и защитата на данните засяга най-вече ново създалата се технология и тепърва развиваща се- Internet of Things. Най-актуалната технология предоставя на човека възможност да управлява света около себе си. Хората могат управляват всички свои битови уреди, както тези във кухнята така и бойлера, отоплението и климатизацията на сградата.

Това е един огромен скок в света на технологиите и е нещо, което все още трудно възприемащо от хората. В бъдеще, обаче, се очаква голямо развитие на технологията, която ще внесе удобствата на модерния човек, но до колко това ще бъде сигурно?

Интернет технологията даде предпоставки за създаването на криптовалутите и банките за критовалута. Това много улесни онлайн търговията и даде нов метод за разплащане. Тази революция в икономиката, обаче крие и своите големи рискове.

За възникването и равитието на Интернет през годините до днес, ще бъде прегледано в Първа глава.

**Цели и задачи**

**Основната цел на тази магистърска теза е да бъде представен така актуалния проблем, свързан със защитата на Интернет данните днес и да се предложи решение за тяхната защита при използването на Internet of Things.**

За изпълнението на целта за поставят следните задачи:

- ✓ **Ще се направи преглед на различните типове кибератаки и тяхното действие**
- ✓ **Ще бъдат описани методи за предотвратяването на неоторизиран достъп, чрез криптиране и тунелиране на данните.**
- ✓ **Ще бъде представен един от сигурният начин за защита на данни чрез използването на VPN връзка при най-бързо развиващата се иновация в ИТ сферата- а именно Internet of Things.**

По-подробно за сигурността на данните ни в Интернет, ще бъде разгледано във втора глава, а в трета глава ще бъдат описани голяма част

от методите за справяне с опазването на информация там.

В последната четвърта глава ше разгледаме една VPN security връзка-какво представлява, нейната функционалност и предимства.

# ПЪРВА ГЛАВА

## 1.1 Как се заражда идеята за създаването на Интернет

За да открием корените на Интернет, трябва да се върнем назад към 60-те години, към войната във Виетнам и изобщо към Студената война. По време на Студената война много от занимаващите се с военно планиране бяха истински загрижени, че някоя комунистическа страна може да нападне САЩ. Поради тези опасения от чуждо нахлуване, военните започнаха да съставят планове с мерки срещу евентуално нападение. Според част от плановете се предвиждаше да бъде изградена система от автомагистрали, по която войски и боеприпаси да се придвижват из страната от една точка до друга без да се налага да минават задължително през даден точно определен транспортен център (това е днешната Междущатска магистрална мрежа). Войната обаче изисква прехвърляне не само на

войски и боеприпаси, но и на информация. Военните имаха нужда от такъв начин за осъществяване на връзка между две точки, при който информацията да може да се предава по различни маршрути. Това звучи елементарно, но през 60-те години комуникациите не бяха устроени така и плановиците в министерството на отбраната се нуждаеха от ново решение. За целта беше създадена ARPA (Advanced Research Projects Agency, Агенция за авангардни изследователски проекти). ARPA предложи решение, при което информацията се подрежда в малки пратки, наречени “пакети”, на пакетите се поставя адрес и им се задава метод, по който да обикалят из системата, докато стигнат до мястото, към което са отправени.

При този начин на действие като че ли се разчита на случайността и той изглежда неефективен, но предимството му е, че така няма нужда от наличието на разпределителен център, който да насочва информацията от едно място към друго. Въоръжена с този нов метод, ARPA създаде компютърната мрежа ARPAnet и свърза към нея 4 университета. Те вече можеха съвсем лесно да прехвърлят информация помежду си и поради това през 70-те години и други поискаха да се включат в ARPAnet. След като все повече и повече групи, университети, фирми и т.н. пожелаваха и биваха свързвани към ARPAnet, през 80-те години на тази мрежа J дойде много. В този момент в играта влезе NSF (National Science Foundation, Национална академична фондация). В края на 80-те години NSF започна да подпомага създаването на нови и по-усъвършенствани технологии за свързване на групи, университети и фирми, но изискването беше те да се използват само за нуждите на образованието.

## 1.2 Какъв е принципа на работа на Интернет

Както стана ясно в предходните абзаци, Интернет е разработен като средство за осигуряване на комуникацията между множество различни групи и организации. Кой обаче осъществява тази комуникация? В

Интернет комуникацията между всички отделни точки се осъществява от компютрите. Нереалистично е да очакваме, че всички компютри, които се използват по света от различните групи и организации, ще бъдат едни и същи или ще работят по един и същ начин. Също толкова нереалистично е да очакваме и че всеки ще си смени компютъра, само и само за да се свърже с Интернет – преди години никой не би го направил и така Интернет нямаше да може да поеме напред. Така че Интернет наистина е не толкова някакъв определен тип оборудване, а по-скоро начин за съвместяване на различни устройства. Интернет всъщност работи благодарение на създадените за него протоколи.

Протоколите са официалното средство за общуване между компютри: ако два компютъра използват едни и същи протоколи, те ще се “разберат”, дори и да са от различен тип. В Интернет се използва протоколът, наречен TCP/IP (Transmission Control Protocol/Internet Protocol), Протокол за управление на предаването/Протокол за Интернет. Организациите, университетите, фирмите и т.н. обикновено разполагат с локална мрежа, в рамките на която собствените им компютри общуват един с друг. Ако в

една такава локална мрежа има компютър, който може да общува едновременно и с локалната мрежа, и по TCP/ IP протокол, чрез него цялата локална мрежа може да получи връзка към Интернет. Интернет се състои именно от такива свързани една с друга локални мрежи. Следователно, Интернет е не просто една мрежа, а Мрежа от мрежи. Можем да погледнем на Интернет и по друг начин: не като на нещо материално, а като на начин, по който множество малки мрежи общуват една с друга. По-малките мрежи се свързват помежду си чрез големи комуникационни линии, наречени "гръбнаци" *(backbones)*, които преминават през цялата територия на земята и могат да се оприличат на големите автомагистрали. Такива "гръбнаци" кръстосват целия свят и чрез тях всички страни (изключенията са съвсем малко на брой) се свързват в едно в тази огромна Мрежа от мрежи, наречена Интернет.

### 1.3 Развитието на Интернет през годините

В днешно време световната Мрежа е нещо също толкова обикновено, колкото и телевизията, и не учудва никого, дори хората от по-възрастното поколение. Но за 40 години от своето създаване Интернет претърпя фундаментални промени и макар в някои части на света все пак да навлиза бавно, с различна скорост и качество, младите хора вече го приемат като даденост. Интернет вече не е разработка, предназначена само за военните, нито място само за забавление, а и сериозно място за водене на успешен бизнес с многомилионна аудитория. Все пак, полезно е да се знае

историята на тази паяжина, обхванала цял свят и тук ще се спрем на основните ключови дати от нейното развитие.

**В далечната 1969 година:** На 2 септември, между два компютъра в Калифорнийския университет в Лос Анджелис е извършен обмен на данни в хода на първия тест на ARPANET – експериментална мрежа, разработена по поръчка на агенцията за съвременни отбранителни проекти DARPA. Първата връзка между отдалечени точки – Калифорнийския университет и Станфордския изследователски институт, е направена на 29 октомври, макар и мрежата да се „срина“ след предаването на първите букви на домата „logon”. Малко по-късно към Калифорнийския университет се присъединява и Университетът на Юта.

**1970:** Появява се първият мрежов възел на ARPANET на източното крайбрежие на САЩ в компанията BBN Technologies, разположена в Кембридж и която изиграва немалка роля в развитието на Интернет.

**1972:** Рей Томлисън добавя електронна поща към функционалностите на мрежата и въвежда символа „@“, за да обозначи пощенските адреси.

**1973:** Първите мрежови възли на ARPANET в Англия и Норвегия.

**1974:** Винт Сърф и Боб Кан разработват комуникационна технология, включваща протокол с название TCP (Transmission Control Protocol), която позволява няколко обособени мрежи да се разбират помежду си – по този начин се реализира принципът на Интернет. По-късно концепцията приема формата на стек протоколи TCP/IP (Transmission Control Protocol/Internet Protocol), а формалното му приемане е на 1 януари 1983 г.

**1983:** Предложена е система за домейнните имена или DNS (domain name system), която задава съответствието между IP адресите и текстовите имена на мрежовите ресурси, и изпълнява други служебни функции. Суфиксите .com, .gov и .edu се създават една година по-късно.

**1988:** Появява се първият Интернет-червей Morris, който поразява хиляди компютри.

**1989:** Компанията Quantum Computer Services, известна днес като AOL, представя услугата America Online за компютрите Macintosh и Apple II, като започва процес на експанзия, довел до появата на Интернет у 27 млн. американци през 2002 г. В същата година физикът Тим Бърнърс-Ли (сега оглавяващ организацията W3C) измисля World Wide Web (Световната

мрежа) при разработката на отдалечено управление на компютрите в CERN (Европейската организация за ядрени изследвания). Негова заслуга е принципът на публикуване на хипертекстовите документи и създаване на хиперлинкове, както и протоколите HTTP и езикът HTML.

**1993:** Това е годината,  в която се създава първия браузър. Марк Андресен с колегите си от Илинойския университет създава Mosaic – първият браузър, показващ графика и текст на една страница. По този начин той отваря вратите към един нов свят за обмен на информация.

### 1.4 Интернет днес

С развитието на компютърните мрежи и появата на Интернет започва една нова епоха в технологиите на нашето съвремие.

Това оказа голямо влияние и върху нашият живот и се превърна в портал към неограничените възможности.

В ежедневието на почти всеки човек се предоставя възможността за онлайн пазаруване, достъп до голям брой социални мрежи и възможност за осъществяване на аудио и видео комуникация  през мобилното си устройство със целият свят. Това са съвсем малка част от удобствата, които Интернет ни предоставя. Възможностите са неограничени, стига да имаме

осигурено високо ниво на сигурност.

Интернет е нещо, без което повечето хора немогат днес. Това е един безкраен извор на информация за всичко, което ни интересува. Като започнем от готварски рецепти до това с помощта на Google Street View виртуално да се пренесеш във всяко кътче на света по всяко едно време. Несъмнено промяната в живота на човека е колосална.

Всяка година развитието на Интернет на нещата води до появата на нови ‘неща‘ за биотехнологии, производство, умни домове и във всеки аспект от нашето ежедневие. Вече сме виждали настъпващите промени в традиционните индустрии, трансформиране на нашите градове и появата на технологии за безпилотни автомобили. IoT е част от една екосистема, където машинното обучение, изкуствения интелект и анализите на данни ни помагат да разберем нашия свят, повече от всякога.

**Ето 7 прогнози за развитието на Интернет на нещата през 2017 година на Read Write.**

**1. Смарт технологиите ще преобразят начина, по който пазаруваме**

Редица иновационни практики, които включват използването на смарт продукти и апаратура, ще направят магазините да „оживеят“.

**2. IoT и устройствата за носене създават по-високо ниво на персонализация**

Устройствата за носене ще станат важна част от Интернет на нещата, ще взаимодействат безпроблемно с други устройства и ще осигуряват все по-персонализиран опит за техните собственици.

**3. Застрахователните компании ще започнат да инвестират повече, за да се адаптират към Интернет на нещата**

Интернет на нещата ще генерира данни, които коренно ще променят начина, по който информацията трябва да се защитава и пази от различни рискове.

4**. Фокус върху сигурността**

Разбира се, фокусът върху сигурността ще е един от най-важните при развитието на Интернет на нещата, защото хакерите ще имат ново предизвикателство – да пробият от компании до системи за управление на някой град.

**5. IoT анализите ще генерират големи приходи**

Big data включва множество решения за обработка на големи масиви от данни за околната среда, автомобилният трафик, продажбите в търговските вериги и много други сфери и ще е от съществено значение за анализите на данните генерирани от IoT. Ние ще видим повече устройства, способни да анализират данни на местно ниво, да обработват и получават най-важните данни в реално време.

**6. Партньорството**

За да може по-бързо да заживеем в ерата на Интернет на нещата, важно е как производителите на устройствата и софтуера ще си партнират с телекомуникационните оператори.

**7. “Edge” ще се превърне в огромен пазар**

Някои IoT устройства не могат да ползват съществуващите мрежи. Ако има част от глобалната IoT мрежа, която се нуждае от бързи ъпгрейди за да обслужва бизнеса, това е "Edge", границата между IoT устройствата и компютрите в Интернет. Масивните обеми данни които се генерират от IoT трябва да бъдат обработени, редуцирани и анализирани преди да бъдат пуснати в интернет. Това е голяма възможност.

## 1.5 Нашата Интернет сигурност

За съжаление през последните години се наблюдава голямо увеличение на не оторизирания достъп до нашите конфиденциални данни в Интернет.

Тези посегателства се правят от така наречените хакери с цел получаване достъп до информация, която да се използва за лични облаги. Това са лични данни, лична информация от социалните мрежи, пароли на банкови и кредитни карти и банкова информация относно собственост и наличности в сметката ни.

За да можем да използваме Интернет спокойно, и да не пострадаме от това трябва да обърнем голямо внимание на Интернет сигурността и

защитата на нашите лични данни в мрежата. Големите възможности, които Интернет ни предоставя, водят до големи неподозирани рискове по отношение на нашата кибер сигурност.

Една от най-актуалните развиващи се технологии изградени на базата на Интернет е IoT (Интернет на нещата), или познато още като домашна автоматизация. Тази технология дава възможност за пълен контрол на своят дом от голямо разстояние. Тази иновация става мишена за кибер престъпността и това е много актуален проблем с развитието и в днешно време.

Кибер престъпността се разраства и това води до нови и по-големи заплахи за нас и нашето семейство в Интернет средата.

В последните години много недоброжелатели са успели да присвоят данни и ресурси, без това да е било даже доказано.

## 1.6 Сигурността и защитата в интернет е под въпрос за всички потребители. Предизвикателство пред бизнеса и обикновения клиент.

През последните години темата за сигурността в Интернет става все по-наболяла.

Но нека първо да си отговорим на въпроса:

Какво е сигурност в интернет?

Уебсайтовете често изискват регистрация, в която потребителите предоставят лични данни за себе си. Такива са и повечето онлайн магазини, където се въвежда детайлна и чувствителна информация за клиентите.

Идва момент, в който даден сайт разполага с бази данни, чието изтичане при пробив в сигурността би навредило и на клиентите и на самия сайт. Освен за изтекли данни от сайтове, все по-често чуваме и за вирусите, които криптират информацията на вашите компютри и ви искат откуп.

Сайтовете на клиентите са едни от най-честите мишени за злонамерен достъп. Целта на „хакерите“ е не само да направят сайта неработещ или да откраднат информация. В последните години пробивите в сайтовете обикновено са „спящи“. Като мини, които се залагат, за да бъдат активирани по-късно. А когато бъдат активирани, най-често тези компрометирани сайтове се използват за:

„Заразяване“ на други сайтове;

Стартиране на DDoS атаки към трети страни;

Разполагане на phishing сайтове;

Разпространяване на malware (вируси), които заразява клиентски компютри;

Изпращане на SPAM и др.

Друга цел на „хакерите“ са клиентските имейли. Най-често компрометиран имейл се използва за изпращане на SPAM. В по-изолирани случаи и за измами.

## ВТОРА ГЛАВА

## Видове не оторизиран достъп.

## Кибертероризъм - заплахата на модерното време.

### 2.1 Кибертероризъм

Това е сложно модерно явление, което засяга всички развити държави с достъп до компютри и интернет. Кибертероризъм буквално означава виртуална атака, която има за цел внушаване на тревога и страх, посредством компютърни мрежи, свързани с интернет.

Кибер атаките са директна заплаха за сигурността на гражданите и функционирането на държавата, икономиката, обществото, науката и

образованието. Те могат да бъдат извършени от разстояние, с прости механизми и минимални икономически ресурси.

Кибер атаките нямат национални, културни или юридически граници и могат да причинят значителни материални и дори човешки загуби.

Кибертероризмът е атака във виртуалното пространство, която се изразява в мащабно прекъсване на компютърни мрежи или определени персонални компютри, чрез помощта на различни средства (най-използвани са компютърните вируси).

Друга дефиниция е свързана с умишленото внедряване на избрана информация във възможно по-голяма компютърна мрежа с универсалната цел, каквато има всеки терористичен акт, създаване на тревога и паника. Също така, кибертероризмът се разбира като целенасочено използване на компютърни мрежи, за да се унищожат или увредят личните данни, най-често на важна политическа или идеологическа личност.

## 2.2 Кибератака - видове:

Обикновен, неструктуриран- устройване на организирани атаки в отделни компютърни системи, като по този начин се засяга определена, предварително набелязана мишена с помощта на прости инструменти.

Тези атаки се наричат още “хаквания” (вредно техническо влияние) и обикновено се използват от иноватори и “начални” кибертерористи.

Разширен, структуриран - провеждане на по-сложни атаки вече в няколко компютърни системи или мрежи. Има за цел да повлияе на определена група от хора и да създаде състояние на страх или тревога у тях. Друга цел може да е внасянето на хаос в цялостната система на организация или компания.

Комплексен, координиран - добре координирани атаки, които създават масова паника. Те са изключително опасни, трудно контролируеми, тъй като се организират от професионалисти с напреднала техника. Тези хакерски групи са високо мотивирани и освен с цел печалба, участват в такива атаки за собствено удоволствие или в знак на личен протест.

## 2.3 Модерната история познава доста мащабни кибератаки

1. През 2007 година Естонското правителство, банки и медии стават жертва на една от най-големите и сложни атаки в човешката история. Като причина за тях се счита демонтиран в Талин паметник, посветен на Втората световна война. Групата, която успява да свали онлайн услугите и сайтовете, се представя като “Nashi”. Щетите, които претърпява Естония в резултат на безпрецедентната вълна от кибератаки, се изчисляват на десетки милиони евро.
2. Най-мащабната кибератака в света, позната още като “Епсилон”, успява да нанесе изключителни финансови щети на гиганти като JP Morgan и Best Buy. Кражбата на потребителски данни възлиза на 4 милиарда долара.

3. Американското правителство е цел на много кибератаки, а най-ранният опит за разбиване на мрежа с престъпна цел е познат като Moon Maze. Атаката е изключително добре координирана и толкова добре скрита, че в продължение на две години кибертерористите успяват да събират конфиденциална информация за военни операции на САЩ.

4. Titan Rain е друг кибер набез, който успява да проникне в мрежите на NASA, Пентагона и Lockheed Martin /оръжеен производител в САЩ/. Атаката не просто поразява компютърните мрежи, а ги оставя незащитени срещу кибертероризъм от трети страни - чуждестранни хакерски удари).

5. Преди повече от 30 години Американската организация CIA успява със софтуерен код да претовари газопровод в Сибир и по този начин да причини експлозия, която влиза в историята на човечеството.

Кибер атаките са с по-голям потенциал за нанасяне на значителни щети от физическите терористични атаки, тъй като са на сравнително ниска цена, поради факта, че не се инвестира в реални оръжия и взривни вещества. Друго тяхно „предимство“ е, че се провеждат от разстояние и в повечето случаи анонимно.
Множество институции в световен план се занимават със защитата на интернет потребителите.

Все по-масовото проникване на информационните технологии и разрастването на Интернет са предпоставки за разработване на относително нискоструващи кибероръжия, които представляват потенциална заплаха за поддържаната информация не само за системи и мрежи с военно предназначение, но и за мрежови структури с гражданско предназначение

Глобалната мрежа, световните информационни и комуникационни системи могат да се разглеждат като ново поле за водене на бойни действия, за което разстоянията и разположението (местонахождението) са без значение. През последните години се наблюдава тенденция на увеличаване на броя и разнообразието на констатираните кибератаки като обхват, използвани технологии и преследвани цели. Поради тази причина е необходимо да се проследяват, изследват и анализират различните случаи на кибератаки в световната мрежа и възможните щети, които биха нанесли.

## 2.4 Информационната война

През 1999 година директорът на ЦРУ George Tenent прави изказване пред Конгреса, в което изразява мнение, че терористи, са стигнали до извода, че информационната война предлага евтин начин за поддържане на каузата им. Много от тези средства са Windows базирани, изискват минимални технически познания и могат да се намерят свободно и в Интернет.

Dorothy E. Denning разглежда кибертероризма като сливане на тероризма и киберпространството, което обхваща незаконни атаки срещу компютри, мрежи и поддържаната информация в тях, проведени с цел заплаха и насилие на ниво правителство или отделни индивиди, преследвайки политически, икономически или социални цели и интереси.

Целта на кибератаките и пораженията, които могат да бъдат причинени, варират в широки граници и са обект на изследване, анализ и класифициране на много организации с цел осигуряване на превантивни и сигурни мерки за защита. За съжаление може да се каже, че в повечето случаи кибератаките изпреварват киберзащитата или с други думи, кибератаките са възможни поради пропуски в процеса на разработване на информационите и комуникационни системи, на системния и приложен софтуер, а също така и поради недостатъци в системата на киберзащита.

## 2.5 Киберсигурност и нейните аспекти

Най-общо, киберсигурността обхваща:

- Набор от дейности и мерки, целящи защита – от атака, от разрушаване или други заплахи за компютрите, компютърните мрежи, свързаните с тях хардуерни и софтуерни устройства, както и информацията, която съдържат и предават, включително софтуер и данни, както и други елементи на киберпространството.

Дейностите могат да включват одити на сигурността, управлението на версиите, автентификационни процедури, управление на достъпа, и др. Те

могат да включват и, например, оценяване на силните места и уязвимостите на хардуера и софтуера, използван в държавната и икономическата електронни инфраструктури на страната.

Дейностите съдържат също и откриване и реагиране на заплахи за сигурността, намаляване на въздействието и възстановяване на засегнатите компоненти.

Други мерки могат да включват хардуерни и софтуерни защитни стени, физическа сигурност, както и обучение на персонала.

- Състоянието или качеството на защитата от тези заплахи.
- Научните изследвания и анализи, насочени към прилагане и подобряване на дейностите и състоянието, свързани със сигурността.

Най-често срещани видове кибератаки и разрушения, обикновено са тези, причинени от хора - вандали, престъпници, терористи, но е възможно да са в резултат на аварии, големи природни бедствия, земетресения.

*Понятията, свързани с различни аспектите на киберсигурността са:*

- информационна сигурност (information security);
- защита на информацията (information assurance);
- е-сигурност (e-security);
- сигурност в киберпространството (cyberspace security).

Тези аспекти не трябва да се разглеждат като синоними на понятието киберсигурност.

## 2.6 Методи и средства за осигуряване на защита на данните

Мерките, които се взимат, за да се осигури защита срещу кибератаки включват:

- защита от нерегламентиран достъп и кражби на конфиденциална и класифицирана информация,
- предотвратяване на опити за промяна на съществуващи данни и информация,
- ограничаване на загубата на информация, в резултат на преднамерени и случайни човешки грешки,
- формиране на култура за безопасна работа с информационни и комуникационни системи,
- защита при използване на електронна поща и съвременни средства за комуникация – Facebook, Skype и др.

### 2.7 Основни фактори

Три са основните фактора за осигуряване на киберсигурност – човешки, технологични и законодателни.

#### 2.7.1 Човешки фактор

Човешкият фактор играе съществена роля в процеса за осигуряване на киберсигурността на информационно-комуникационните системи. Този фактор е зависим както от морално-етичните характеристики на отделната личност, така и от нивото на неговата подготовка. Човешкият фактор е

пряко свързан и с процеса на създаване на организация за опазване на чувствителна и конфиденциална информация.

Достъпът до обработваните и съхраняваните информация и данни трябва да е съобразен с изискванията на Закона за класифицирана информация, а именно – необходимост да се знае.

Трябва да се предвидят и изпълняват мерки за архивиране и съхраняване на данните, с цел тяхното бързо и надеждно възстановяване в случаи на кибератаки или след възникнали сривове, а също така е необходимо да се алгоритмизират и документират процедурите за възстановяване.

### 2.7.2 Технически и технологични средства

Техническите средства са свързани главно с хардуерна и софтуерна защита на информационните и комуникационни системи и могат да се обобщят по следния начин:

- Средства за физическо осигуряване на компютърните системи срещу кражба, несанкциониран достъп и некоректно използване.
- Средства за контрол на достъпа (защитни стени, пароли, използване на биометрични данни).
- Средства за превенция/откриване на непозволени проникванията (Network Intrusion Prevention Systems – NIPS и Network Intrusion Detection Systems – NIDS).
- Средства за кодиране (системи за PKI и частни ключове).
- Средства за автентификация (цифрови сертификати, маркери, електронни подписи).

- Средства за защита от въздействие на електромагнитни смущения и импулси (EMI/RFI екраниране).
- Средства за контрол на мрежата – използване на подходящ софтуер и хардуер (скенери, снифери, Profilers, Honeypots, Shunts).

### 2.7.3 Законодателни средства

Необходимо е да се съгласува съществуващото национално законодателство със съответното на водещи страни в света, в частта си наказателни мерки спрямо специалистите, които създават и разпространяват злонамерен софтуер, с цел нанасяне на щети и опит за неправомерен достъп до данни и информация, а също така и да се актуализира, в съответствие с динамичната промяна на условията за сигурност.

## 2.8 Развитие на киберсигурността България

От началото на 2009 г., с решение на Министерския съвет на Република България, е създадена длъжност „Национален координатор по киберсигурност“. Като основни задачи, които трябва да бъдат решени на държавно ниво са изготвяне на Национална стратегия за киберсигурност; подобряване международното сътрудничество с цел намаляване на рисковете за България, както от чуждестранни атаки срещу критичната инфраструктура, така и от атаки, инициирани на територията на страната, а също така и използване на експертна помощ на страните-партньори на

България за промени в законодателството на страната по отношение на компютърните престъпления, борбата с кибертероризма и други.

В България, информация за различни аспекти на кибертероризъм могат да се получат и от сайт Национален портал за киберсигурност.
Официалната политика на НАТО по отношение на кибертероризма е одобрена и утвърдена на срещата на високо ниво на НАТО в Букурещ, през януари 2008 г. В резултат на оценяване на опасността от кибератаки, през май 2008 г. е създаден и сертифициран NATO Computer Incident Response Capability – Technical Center (NCIRC – TC). Информацията на страницата на центъра се поддържа от NATO Information Assurance Technical Center (NIATC), като целта е обобщаване и анализ на полезна информация за членовете на комуникационно-информационното общество на НАТО чрез изготвяне на бюлетини и доклади. В Талин е организиран и функционира Cooperative Cyber Defence Centre of Excellence.

## 2.9 Заключение

Като резултат от анализа на тенденциите за нарастване на броя на кибератаките през последните години е необходимо да се дефинират адекватни мерки за противодействие и защита от кибертероризъм. Определено може да се каже, че съществува тенденция за недостатъчно оценяване и дори подценяване на проблема. Поради неговата сложност,

мерките, които се взимат, трябва да бъдат технически и технологични, физически, законодателни и организационни.

**Предлагаме следното обобщение на мерките за защита:**

1. Цел за потенциални атаки са не само военни структури и мисии, а също така и всички държавни, финансови и корпоративни структури, представляващи обекти от държавния и частния сектор. Това налага, за осигуряване на надеждна защита, да се формират съвместни работни групи от военните и цивилни специалисти за набелязване и осъществяване на мерки за противодействие и изготвяне на национална стратегия за защита.
2. Проблемът излиза извън рамката на отделната държава и има международен характер. Това налага взаимодействие между структурите за осигуряване на киберсигурността на отделните държави.

3. С цел противопоставяне на бързото разпространяване на кибератаките и като резултат, ограничаване на размера на нанесените щети трябва да се предприемат мерки за създаване на система за бързо усведомяване на потенциалните цели на тази атака. С оглед на това може да се вземат мерки за изготвяне на бюлетин за констатирани инциденти и мерки за противодейстеие.

4. Повишаване на квалификацията на специалистите от структурите за протииводействие на кибератаки и поддържането на високо и равномерно (еднакво за различни структури и ведомства) ниво на подготовка също може да се разглежда като мярка за противодействие.

5. Да се осигури недеждна система за архивиране на критични данни и възможност за бързото им възстановяване след проведена кибератака.

6. Ефективно използване на нови информационни технологии за противодействие.

7. Да се приеме като основна задача взимането на своевременни мерки за противодействие на манипулативни кибератаки с цел създаване на паника и дезориентация.

8. Във време на криза и агресивно търсене на пазари, голяма цел за киберпрестъпленията представлява корпоративна информация, свързана с ценова политика, търговска дейност, договорни отношения, тръжна дейност, резултати от изследвания, нови разработки и др. Поради тази причина защитата на информация от този тип също трябва да е обект на внимание на специалистите по сигурността.

Осигуряването на надеждна защита срещу кибертерористичните атаки е свързано с използването на различни техники и технологии като криптография, стеганография, защитни стени (firewalls) и др. Прилагането на тези техники и технологи, както и разработването на методики за защита са в основата на разработване на правилните стратегии за защита в условия на кибератаки.

## 2.10 Кибератаките, които впечатлиха света

От зората на модерните компютърни технологии, винаги се намира човек (или група хора), които да изявяват повече интерес към това как могат да експлоатират технологията по непредвиден или необичаен начин. Това често включва и получаването на достъп до права или данни, до които човек не би трябвало да стига, а именно това, което наричаме „хакване“ днес. Въпреки че за много от хората, които го практикуват, това занимание служи за професия, задоволяване на лично любопитство или „за спорта“, винаги има и такива, които решават да използват уменията си за престъпни цели.

Образът на модерния хакер – такъв, какъвто го познаваме от телевизионния екран – сам, в тъмна стая, взиращ се в монитор, по който препускат редове от привидно непознати на човечеството символи, може да не е напълно точен. Атаките, с които искам да ви запозная, обаче, могат да засенчат дори и тези от филмовата индустрия.

## 5. **The Morris Worm**

Първият и един от най-вредните червеи, които се разпространяват онлайн е този, направен от Робърт Морис през 1988. Въпреки, че първоначално Морис цели просто да провери колко голямо е киберпространството, до което има достъп чрез код, който се

разпространява из всички свързани онлайн компютри, той бързо прераства в бедствие, след като започва да причинява грешки в инфектираните системи. Около 6000 компютри биват инфектирани и изкарани извън строя, което по това време би оставило щети на сметка между 10 и 100 милиона долара.

4. **Веригата Target**

В една от най-големите атаки от рода си в САЩ, уязвимост в онлайн услугите на веригата магазини Target бива експлоатирана и дава шанс на неустановените извършители да откраднат между 40 и 110 милиона записа за кредитни карти. Мащабът на атаката не се дължи толкова на уменията на извършилите я, колкото на престъпното игнориране на огромната уязвимост от страна на Target.

3. **Mirai Botnet DDoS**

Internet of Things епохата ни носи много възможности, които сме виждали само в най-клишираните фантастични филми, но ни носи и много уязвимости. Поради все по-бързите темпове на напредване на електрониката, осигуряването на безопасност със сигурност не е приоритет, както ни показва тази атака. Mirai е мрежа от експлоатирани IoT устройства, която стои зад едни от най-големите и вредни DDoS (Distributed Denial of Service) атаки, които познаваме до днес, включително такава, която беше усетена по цял свят.

2. **Red October**

„Червеният октомври“ е инфекция, която е намерена през 2012 година и е действала на глобално ниво с цел крадене на дипломатическа и бизнес информация от различни държави и организации. Не е ясно каква точно е била целта на атаката и кой стои зад нея, но след идентифицирането ѝ, интернет и домейн доставчици от цял свят се обединяват и намират всички 60 домейна, които са служели за приемане на информацията. След акцията, самите извършители на атаката я прекъсват без обяснение.

1. **Stuxnet**

Stuxnet е атака, която бихте очаквали да видите по телевизионния екран. Смятана от много за обединено усилие от страна на САЩ и Израел, атаката цели да изкара извън строя програмата за ядрено въоръжаване на Иран. Най-интересното при нея е начинът и на работа - Stuxnet цели да инфектира компютри в заводи за оръжия.

Веднъж щом зловредният код достига до приемника си, той започва да търси определен тип софтуер, който служи за управление на всякакви видове машини. Щом бъде намерен такъв софтуер, Stuxnet започва да му подава случайни команди, но показва на потребителите, че всичко е наред.

Това, естествено води до редица „нещастни инциденти“, за които, обаче, нямаме информация поради естеството на атаката.

## 2.11 Нови видове кибер атаки набират все по-голяма скорост

Броят на софтуерните продукти за защита на мобилни устройства е нараснал двойно през 2011 г.

Бързо променящият се пейзаж на ИТ сигурността се характеризира с добре планирани атаки, нарастваща уязвимост на мобилните устройства и нови видове заплахи, сочи докладът IBM X-Force, изготвен он Института по сигурността за Азиатско-Тихоокеанския регион на IBM.

"Честите случаи на пробиви на сигурността през тази година показват предизвикателствата, с които организациите се сблъскват най-редовно при изпълнение на тяхната стратегия за сигурност. Въпреки че ние знаем как да се защитаваме на техническо ниво срещу много от тези атаки, организациите не винаги имат разработени вътрешни оперативни практики, за да противодействат сами", казва Том Крос, мениджър Threat Intelligence and Strategy for IBM X-Force Cross.

Докладът стъпва на данни, събрани чрез изследване на IBM върху обществената уязвимост, както и на мониторинг и анализ на близо 12 милиарда случая на ден, свързани със сигурността, от началото на 2011 г. Данните сочат нарастване на случаите на нарушаване на системите за сигурност на тези устройства и утрояване на процента на критичните атаки на сигурността.

Проучването отчита също така двойно увеличаване през настоящата година на броя на софтуерните продукти за защита на мобилни устройства.

Докладът регистрира нови видове атаки на сигурността, които набират скорост през тази година. Сред тях са:

• Екипи на професионалисти, чиято цел е събиране на важна информация и стратегическо разузнаване. Тези атаки често са наричани Advanced Persistant Threats (APTs);

• "Whailing" (китолов) – атака, с която се осигурява достъп до личните данни и информация на лица, разположени на високи постове в дадена компания;

• Атаки от "hacktivist" групи, насочена към уеб-сайтове и компютърни мрежи; най-често имат политически цели, а не само финансова изгода;

• Анонимните прокси сървъри са се увеличили четири пъти за период от три години.

X-Force 2011 разкрива и някои подобрения в областта на компютърната сигурност, които показват напредък в борбата срещу престъпността в интернет. Така например, през първата половина на 2011 г. е отчетен спад на атаките на уеб приложения от 49% от всички оповестени атаки до 37%.

Критичните атаки на уеб браузърите са достигнали най-ниското си ниво от 2007 г. насам. Отчетен е и значителен спад на спам съобщенията през първата половина на тази година.

Докладът IBM X-Force посочва, че страните от Азиатско-тихоокеанския регион имат най-сериозни проблеми със спам съобщенията и ИТ сигурността. От Индия се изпращат около 10% от целия регистриран спам в днешно време, като Южна Корея и Индонезия също имат сериозни подобни проблеми.

## 2.12 Най-големите кибератаки през изминалата 2017 г.

Годината беше белязана от по-големи и по-сложни хакерски атаки, които засегнаха най-уязвимите потребители в интернет, компании и правителствени агенции.
Годината, изглеждаше много несигурна в интенет пространството.

Хакерските атаки се появяваха на бял свят една след друга през 2017 г. - от пробива в Equifax, който компрометира почти половината население на

САЩ до огромните атаки, които струваха на компаниите милиарди долари, пише CNN.

Всичко това подчерта проблемите с уязвимостта на личната ни информация. Повечето от инструментите, използвани от правителствените хакери, станаха публични, и е по-лесно отвсякога да се създаде и разпространи зловреден софтуер или да се откраднат данни от компании. Същевременно фирмите все по-често стават жертва на подобни случаи.

Задават се  още бъдещи прояви на кибер престъпност.

“Докато пренасяме бизнеса си все повече онлайн, а престъпниците осъзнават стойността на данните, които организациите опазват, виждаме повече големи компании да стават жертва на пробиви, виждаме по-сложни пробиви”, коментира Марък Нуниковън, вицепрезидент облачни проучвания в компанията за сигурност Trend Micro.

В частност ransomware атаките (при които хакерите искат пари, за да отключат файловете ви) стават все по-чести.

Анализ на фирмата за антивирусен софтуер Bitdefender откри, че плащанията заради ransomware са достигнали 2 млрд. долара през 2017 г., или два пъти повече отколкото през 2016 г. Междувременно Trend Micro прогнозира, че световната загуба от друга нарастваща тенденция - компрометираните имейли, ще надминат 9 млрд. долара през следващата година.

### 2.13.1 Ето  кои са най-големите хакерски атаки през изминалата 2017 година

**- Equifax**

Киберпрестъпници атакуваха Eqifax, една от най-големите кредитни фирми. Това се случи през юли, а в резултат бяха откраднати данните на 145 млн. души. Този пробив е смятан за един от най-лошите за всички времена заради обема на чувствителната информация, която е засегната. Компанията разкри информация за случая цели два месеца по-късно. Случаят обаче може да има ефект с години, защото откраднатите данни могат да бъдат използвани за кражба на идентичност.

Пробивът в Equifax засили притесненията за обема на информацията, която брокерите събират за своите клиенти. Тя може да варира от списъци с имейли, рождени дати и други лични данни. Фирми като Equifax, TransUnion и Experian продават тези данни на клиенти, като банки например, така че те да могат да научат повече за вас. Дали се прави достатъчно, за да се опазва тази информация на сигурно място, е под въпрос.

Вече бившият главен изпълнителен директор на Equifax подаде оставка, след като атаката беше разкрита. Той даде показания по случая и обвини

служител, който е бил уволнен, за провала в сигурността. Обществото все още не знае кой е отговорен за атаката.

### 2.13.2 Yahoo

Компанията майка Verizon обяви през август, че всеки един от общо 3 млрд. акаунта на Yahoo е бил хакнат през 2013 г. - три пъти повече, отколкото се смяташе в началото. През ноември бившият главен изпълнителен директор на Yahoo Мариса Майер каза пред Конгреса, че компанията е открила пробива чак през 2016 г., когато обяви, че са компрометирани 1 млрд. акаунта. Yahoo все още не знае кой е отговорен за всичко това.

Отделно канадски хакер се призна за виновен, че е участвал в друг голям пробив в системите на Yahoo от 2014 г. Този път са били компрометирани 500 млн. акаунта. Хакерът ще чуе присъдата си през февруари.

# ТРЕТА ГЛАВА

## Зашита на данните

### 3. Основни начини за защита на данни от неупълномощен достъп

### 3.1 С въвеждане на потребителско име (username) и парола (password)

Правила за избор на подходяща парола:

- Да се използват малки и големи букви, цифри, специални символи.

- Да се състои от голям брой символи – желателно е над 12, защото към момента тази дължина затруднява практическото разбиване на паролата.

### 3.2 Със защитна стена (firewall)

### 3.2.1 Роля на защитната стена

Тя ограничава неупълномощения достъп чрез динамично филтриране на опитите за достъп до системата чрез компютърната мрежа. Като резултат засича и предупреждава за атаки в реално време.

Още ограничава програмите работещи на компютъра, изпраща информация или вреден софтуер /вируси/ до други компютри в случай на заразяване с компютърен вирус.

### 3.2.2 Функции на защитната стена

Фигуративно казано, защитната стена представлява **„граничен контролен пункт“** за желаещите да преминат пакети. Целият трафик се осъществява през този пункт, който има за задача да пропуска само което е безопасно. При настройка на защитата има два генерални подхода:

- Пропускат се всички данни и услуги с изключение на изрично забранените,

- Забраняват се всички данни и услуги с изключение на специално разрешените.

### 3.2.3 Основни функционалности

**Три са основните функции на защитната стена:**

- да блокира данните, за които има вероятност да прикриват хакерски атаки,

- да скрива информация за мрежата, като за изходящия трафик маскира IP

адреса на мрежата с IP адреса на защитната стена,

- да води дневници (logs) за информационния поток със записи на определени събития.

### 3.2.4 Блокиране на данни

Данните се блокират тогава, когато не отговарят на правилата за сигурност, зададени от администратора на мрежата. Например, ако от определен източник са регистрирани опити за хакерски атаки или flooding, администраторът задава правило за отхвърляне на всички пакети с IP адреса на този източник. Много често за подобно филтриране не е необходим допълнителен софтуер, а е възможно то да се извърши и от маршрутизатора (всички съвременни маршрутизатори имат такава функционалност). Освен входящите данни могат да се блокират и изходящите. По този начин се защитава останалият свят от локалната мрежа и могат да се забранят някои потенциално опасни услуги и действия от даден хост Също евентуално проникнал Троянски кон няма как да се свърже със стопанина си. Блокирането на данни е в основата на втория генерален подход за реализация на защитните стени. Така по подразбиране се отхвърлят непознатите протоколи и се осъществява по-силен контрол на трафика.

### 3.2.5 Скриване на информация за мрежата

Замяната на адресната информация осигурява анонимност на защитаваната мрежа. Така се прикриват вътрешните мрежови характеристики от външната мрежа.[5] Най-често се скриват DNS, FINGER и други протоколи. Чрез тях би могла да бъде получена вътрешно мрежова информация, чрез която по-нататъшното проникване в мрежата ще бъде максимално улеснено.

### 3.2.6 Документиране на входния поток

В логовете на защитната стена обикновено се пази подробна информация за допуснатите и отхвърлените от стената пакети, като например мрежовите адреси на източника на пакета и дестинацията, номерата на портовете на източника и дестинацията, типа протокол, и други. На базата на тази информация може да се прави одит на причините за възникване на дадено събитие.

### 3.2.7 Допълнителни функционалности

Освен основните си функционалности, защитната стена между мрежи има и допълнителни възможности:

- филтриране на съдържанието (content filtering),

- преобразуване на мрежови адреси и номера на портове (network address translation, port address translation),

- балансиране на натоварването (bandwidth shaping, QoS),

- откриване на пробиви в системата (intrusion detection).

- Филтриране на съдържанието

Когато се налага ограничение за достъп от вътрешни хостове до определени данни и услуги от външната мрежа, то може да бъде реализирано, като се филтрира съдържанието на заявките по адрес или по ключови думи. Обикновено се блокира достъпът до сайтове с пиратско или порнографско съдържание, сайтове за електронна поща. Блокират се и файлове с някои разширения - .AVI, .MP3, и exe.

При тази функционалност на защитните стени списъкът със забранени (banned) сайтове трябва регулярно да се обновява. При филтрирането на съдържанието може да се избегне досадното или зловредно съдържание на pop-up рекламите, спама по електронна поща, Java аплети, ActiveX програми, троянски коне, вируси и др.

### 3.2.8 Защитната стена и преобразуване на мрежови адреси

Като инструмент за използването на NAT технологията. Обявяването само на мрежовите адреси на защитната стена носи значително по-малък риск, понеже стената е специализирана и силно защитена система, достъпна за конфигуриране само от системния администратор, която концентрира контрола върху достъпа до хостовете от мрежата.

Преобразуването на номерата на портовете (port address translation, PAT) е сходно с NAT. При него във всички пакети от изходящия трафик реалният номер на порта е заменен с друг номер. Идеята е да се елиминират външните атаки, извършвани по определен номер на порт. PAT е

наложително и когато множество защитавани хостове използват като клиенти един и същ външен мрежов адрес на защитната стена – в този случай PAT се използва освен за защита, но и за идентификация на връзките между многото хостове и външния сървър.

### 3.2.9 Откриване на пробиви в системата

Защитните стени придобиват тази допълнителна функционалност когато в тях се интегрира система за откриване на пробивите (intrusion detection system, IDS). Тази система сканира съдържанието на всички преминаващи през стената данни и е способна да проследява хакерските атаки в развитие. Съвременните IDS типично се състоят от множество monitoring станции, свързани към централни сървъри, които анализират данните. Например, ако атакуващият сондира защитната стена за слаби места през една връзка, а се опитва да ги експлоатира през друга връзка, има много голяма вероятност IDS да разкрие източника на атаката.Недостатъкът на IDS е, че за изпълнението му са необходими повече ресурси.

### 3.2.10 Устойчивост на срив

Често наричани high-availability, усъвършенстваните средства за устойчивост на срив позволяват защитните стени да работят по двойки, като второто устройство стои в готовност да поеме работата на титулярното, ако настъпи срив и то престане да функционира. Някои от

съвременните защитни стени, които поддържат този и други механизми за устойчивост на срив, са реализирани в Cisco PIX или Nokia/Checkpoint.

### 3.2.11 Политики на защитните стени

Понякога вместо по-академичното „политики“ се казва просто „настройки“.

Преди да бъде изградена защитата, трябва да се артикулира и политиката на тази защита. Тази политика обикновено представлява документ, който специфицира правата на достъп и ползване на ресурсите на глобалната мрежа за всеки от хостовете в мрежата. Политиката на защитната стена е съобразена както с характера на мрежата и външните услуги, които са ѝ необходими, така и с вътрешните ресурси, които могат да представлява интерес за външни потребители (а много често тези ресурси са и основният обект на хакерски действия).

Политиката на защитната стена определя коя част от трафика, преминаващ през стената, ще бъде пропусната и коя част ще бъде блокирана и отхвърлена. Политиката на защитната стена се състои от две независими политики: политиката на достъпа “отвън навътре” (inbound access policy) и политиката на достъпа “отвътре навън” (outbound access policy).

Политиката на защитната стена трябва да отговори на следните въпроси:

Каква информация трябва да бъде достъпна за всички вътрешни потребители?

Каква информация трябва да бъде достъпна за всички отдалечени потребители?

Кои външни ресурси трябва да бъдат достъпни за вътрешните потребители?

На какви правила трябва да се подчинява използването на електронната поща?

Какви правила трябва да се спазват за уеб-достъп?

Достъп отвън навътре

Когато целият Интернет трафик произлиза от локална мрежа, политиката на достъпа “отвън навътре” е доста проста. Целият входящ трафик, който не представлява отговор на заявка от локалната мрежа, се блокира. Чрез използването на NAT адресите на хостовете в мрежата не се разкриват пред външния свят, което изключително затруднява пробива им.

Ако обаче към някои ресурси в локална мрежа, трябва да има достъп отвън, трябва да определим критерии за филтриране на този достъп. Колкото по-строги са тези критерии, толкова по-високо гарантирана е сигурността на мрежата. В идеалния случай, адресите на външните хостове с право на достъп до локалната мрежа са известни и входящият трафик от другите адреси се блокира. Други критерии са базирани на данните в TCP-хедъра на пакета, например могат да бъдат позволени само пакетите с порт на получателя 80 – пакети за уеб-сървъра.

Когато филтрирането по адрес и протокол не е достатъчно, трябва да се направи по-обстоен модел на правилата, който се реализира от по-сложни защитни стени като защитната стена с пакетно филтриране и състояние или многослойната защитна стена.

Достъп отвътре навън

Тази политика определя какъв вид информация може да напуска локалната мрежа, както и заявките към какъв тип информация следват да бъдат удовлетворени. Също така, определя кой от хостовете и за какви цели е може да използва Интернет. Например, уеб-достъпът може да е позволен на всички хостове, но FTP-достъпът да е позволен само на някои. Тази политика може да има и времеви параметри: например в една фирма mp3-файлове да могат да се свалят след 18:00, когато свърши работното време.

### 3.2.12 Видове защитни стени

Съществуват 3 основни вида защитни стени — филтриращи маршрутизатори (filtering routers), поддържащи връзката пакетни филтри (stateful packet filters), и приложни шлюзове (application gateways). Повечето защитни стени прилагат съчетания от гореспоменатите видове.

Филтриращите маршрутизатори (англ. filtering routers)разглеждата всеки пакет отделно — т.е. не обръщат внимание на пакета като част от установена вече връзка.

поддържащи връзката пакетни филтри (stateful packet filters ), както подстказва името им разглеждат всеки един пакет като част от вече установената връзка

приложни шлюзове или проксита (англ. application gateways или application proxies) - програми, намиращи се между крайният потребител и публичната мрежа — т.е. шлюзовете изпълняват методите вместо крайните потребители, защитавайки ги така от външни опасности. Тези приложения имат силни защитни свойства понеже крайните потребители никога не комуникират директно с хостове в Интернет

## 3.3 Повишаване на сигурността с инсталация на подходяш и специализиран софтуер

**- Антивирусна програма**

Те са неделима част от защитата на мрежата.

Освен стандартната антивирусна защита често се осигурява и защита от шпионски софтуер (Spyware), който краде информация и я изпраща до други компютри, от нежелана поща (spam), изскачащи прозорци (Pop-ups) и др.

Такава програма е например Windows Defender, която е безплатна.

## 3.4 Препоръки за предпазване от кибератака

**- Разучаване на социалното инженерство**

Кибер престъпността не е просто технически проблем с техническо разрешение. Хакерите днес използват т.нар. социално инженерство, за да ни контролират. Благодарение на информацията, която споделяме, те могат

да намерят начин как да ни влияят негативно. Именно затова, уверете се, че разбирате всички принципи на социалното инженерство. Уеб сайтът на Symantec е едно добро начало.

**- Не се доверявайте прекалено лесно**

Работа от вкъщи - Измамниците прехвърлят откраднати пари към нищо неподозиращите потребители, които след това им ги връщат чрез електронно плащане, задържайки конкретната комисионна. Изводът – току що сте били въвлечени в пране на пари.

**- Използвайте наистина трудни пароли**

Microsoft имат един доста полезен наръчник за това как да си изберете наистина трудна за отгатване парола. Компанията, освен това, ви дава възможност и да тествате сигурността на избраната от вас парола.

**- Използвайте няколко имейли**

Минималното, което можете да направите е да използвате един имейл за социалните мрежи и един за бизнес. Обикновено, имейлите, с които се регистрирате в социалните мрежи привличат повече внимание, така че можете да сте поне малко по-спокойни, че по-ценната ми информация се съхранява другаде.

**- Внимавайте с обществените мрежи**

Никога не използвайте обществени мрежи за финансови транзакции и изпращайте своя лична информация само чрез мрежи, които самите вие сте създали или, които наистина считате за сигурни. Никога не можете да знаете дали компютърът, който използвате, не записва вашата информация.

**- Използвайте виртуален компютър**

Идеята е проста – създайте виртуален компютър, използвайте го, за да сърфирате в Интернет и, след като приключите, го унищожете, заедно с всички вируси, които може да са го заразили. Най-лесния начин за това е да създадете виртуален компютър в Ubuntu.

**- Пазарувайте само с кредитна карта**

Онлайн магазините са едно от най-мощните оръжия на измамниците. Избягвайте сайтове, които приемат само пари в брой или с чек. Пазарувайте само от сайтове, които приемат кредитни карти. Уверете се, че магазинът има физически адрес.

**- Запомнете следното правило:**

Никога не казвайте в Интернет това, което не бихте казали в реалния си живот. Никакви настройки за сигурността не могат да ви защитят от умишлена хакерска атака.

**- Внимавайте с горещите теми**

Винаги, когато нещо е особено популярно, например излиза нов дългоочакван филм или става скандал с известна личност, виртуалното пространство се изпълва с фалшиво съдържание, което уж е свързано с това събитие. Помислете няколко пъти преди да кликнете върху някой линк, който обещава да ви покаже нещо грандиозно.

**- Използвайте кредитна, а не дебитна карта**

Компаниите, предоставящи кредитни карти, ви плащат компенсация, ако станете невинна жертва на измама – нещо, което компаниите, които предлагат дебитни карти не правят. В същия случай те ще ви обвинят, че не сте положили достатъчно усилия за картата си.

**- Научете се да разпознавате фалшивите продукти**

Един от най-популярните видове измама е продажбата на фалшиви продукти, които приличат досущ на оригинала. Никога не купувайте нищо от съмнителни сайтове, дори да се предлага на страхотна цена.

- Ако се съмнявате в легалността на даден сайт има услуги, които ви позволяват действително да проверите дали този сайт е регистриран. Един такава услуга, например е Whois.net.

- **Откажете се от Internet Explorer 6**

Разбира се, възможността да използвате този браузър е малка и все пак – откажете се от него. Той не само, че вече не поддържа Google и YouTube, но има хиляди дупки в сигурността.

- **Използвайте Virus Total**

Ако сте получили файл и се съмнявате в това дали е заразен или не, качете го в сайта virustotal.com, където той ще бъде анализиран и проверен за вируси. Накрая дори ще си получите доклад за неговото състояние.

**- Откажете се от ненужни услуги**

Сигурно компютърът ви е пълен с услуги и приложения, които не ползвате. Всяко едно от тях е потенциален вход за атака в компютърната ви система. Затова внимателно проверете всяка една програма и ако не я използвате, просто я изтрийте.

- **Бъдете предпазливи с новите файлове**

Когато сте изтеглили даден вид файл, изолирайте го и ако можете го отворете във виртуална среда. Чак след като се уверите, че всичко в него е наред, го "пуснете" в компютърната си система.

**- Ъпдейтвайте софтуера си**

Някои приложения, като тези в Windows 7 например, се ъпдейтват сами, но все пак системите за ъпдейт трябва да бъдат проверявани за изправност от време на време. Някои по-малки приложения, пък, изискват ръчно ъпдейтване.

**- Проверявайте сигурността на сайтовете**

Изтеглете си SiteAdvisor на McAfee. Плъгинът за браузър има собствена система, наподобяваща светофар, която определя до каква степен е безопасен сайтът, който посещавате.

**- Тествайте системата си**

Използвайте Elcar, за да тествате системата си. Това е текстов файл, който всички антивирусни програми би трябвало да могат да поддържат.

## 3.5 Мрежова Сигурност

Използването на специални стандарти и протоколи позволява по-надеждна защита на предаваната по Интернет информация. В последно време се появяват цял комплекс стандарти, обхващащи защитата на всички нива на мрежата, от отделния пакет до приложенията, като се отделя значително внимание на въпроса за защита на информацията в Интернет . Ето някои от стандартите за защита на данни в Интернет:

### 3.5.1 Secure HTTP (S-HTTP)

**Има за функция защита на транзакциите в Web пространството.**

Когато даден сайт се зарежда през HTTPS (Например: https://mysupersite.com), връзката със сървъра се криптира чрез ползването на SSL (SSL сертификат). По този начин данните, предавани между потребителя и сървъра, са в криптиран вид и са защитени от проследяване и разчитане от трети лица.

Когато обаче на този сайт има вътрешни или външни ресурси, които се изтеглят през некриптирана връзка (HTTP), уеб браузърите показват предупредителни съобщения и може да блокират зареждането на тези ресурси.

В по-новите версии на някои уеб браузъри като Mozilla Firefox, Google Chrome и Opera автоматично се блокира активното несигурно съдържание например .js скриптове, XMLHttpRequest object заявки и т.н. Други несигурни ресурси може да бъдат заредени например .jpg, .png и други изображения.

Данните предавани по HTTPS не могат да се прихванат и променят, но данните, предавани по HTTP, могат. Докато браузърът зарежда елементите на сайта, през сигурна връзка, отделно прави връзка със сървъра и през

HTTP, за да зареди смесеното съдържание. Тези некриптирани данни може да се прихванат и използват за злонамерено действие от трето лице.

### 3.5.2 Secure Sockets Layer (SSL)- служи за защита на пакетите данни на ниво мрежа.

Защо е важно да имае SSL сертификат на нашият персонален компютър илио сървър? С всеки изминал ден Интернет става все по-важна част от нашето ежедневие. Ние общуваме онлайн, пазаруваме онлайн, разплащаме сметките си онлайн. Прекарваме голяма част от времето си в Интернет, работим или се забавляваме там, използвайки различни уеб базирани приложения, социални мрежи и електронни пощи, електронно банкиране и други.

За осъществяването на тези дейности все по-често се налага и да подаваме онлайн конфиденциална информация към определени уеб сайтове. С това неизбежно започваме да си задаваме и въпроси, свързани със сигурността на информацията:

- Възможно ли е информацията, която въвеждам да отиде при някой, който не е оторизиран и да бъде използвана по престъпен начин?

-Наистина ли съм на правилния уеб сайт?

-Защитени ли са моите данни?

Доверието и сигурността на потребителите са необходими за нашето онлайн съществуване. Без значение дали сме физическо лице или фирма е важно да се погрижим за защита на нашите потребители, така както бихме

се погрижили за нашия дом или бизнес.

За да се решат проблемите, които биха могли да застрашат сигурното предаване на конфиденциална информация в Интернет, са създадени различни криптиращи протоколи. Най-разпространеният от тях е SSL (Secure Sockets Layer) и по-съвременната му версия TLS (Transport Layer Security).

Едно от най-разпространените приложения на тези протоколи е в уеб браузърите, при използването на HTTPS или Hypertext Transfer Protocol Secure. Когато потребителят достъпва Интернет страница чрез HTTPS, се осигурява криптирана връзка между уеб сървъра (сайта) и браузъра на потребителя.

За осъществяването на сигурна криптирана връзка между клиента (уеб браузър) и сървъра е необходимо на сървъра да бъде инсталиран цифров сертификат, или придобилото популярност – **SSL сертификат**. Не всеки SSL сертификат, обаче се разпознава от уеб браузърите и за да бъде признат за валиден даден сертификат, той задължително трябва да отговаря на следните условия:

Датата на изтичане на сертификата да е след текущата дата. Всички сертификати се издават с определен срок на валидност. Ако сертификатът е изтекъл, то той се приема за невалиден и на посетителите на сайта се показва предупредително съобщение;

Името на домейна (сайта), който се опитваме да посетим, използвайки

сигурна връзка, трябва да съвпада с това, което е зададено в сертификата. В случай на несъвпадение, сертификатът се приема за невалиден и на потребителя се показва предупредително съобщение.

**Защитава чрез SSL**

Когато се заговори за сигурност на връзката повечето хора се сещат единствено за криптиране на данните при комуникацията между браузъра и сървъра. Това обаче е последната фаза на SSL комуникацията. Първото и основно нещо, което прави SSL защитата е да подсигури самоличността на сървъра, с който комуникира клиента (браузъра). От тук се появяват и различните нива на валидация и различните видове сертификати.

Втората и не по-маловажна част на подсигуряване на връзката е криптирането на данните. SSL сертификатът е файл, инсталиран на уеб сървъра, на който се намира сайта. Сертификатът се състои от публичен ключ и допълнителна информация. Допълнителната информация може да бъде примерно името на домейна, името на фирмата, друга фирмена информация и т.н. в зависимост от типа на самия SSL сертификат, като цялата информация е закодирана в сертификата.

Публичният ключ се съдържа в сертификата и се изпраща на браузъра, след което браузърът проверява, дали сертификатът е валиден и верифицира, дали уеб сървърът е точно този, за който се представя.

Опростено описание на стъпките, през които минава една SSL/TLS сесия между браузъра и сървъра:

1. Браузърът се свързва със сървъра.

2. Сървърът изпраща своя сертификат към браузъра.

Браузърът прави проверка на сертификата – дали е издаден от валиден сертифициращ орган, дали срокът на валидност на сертификата не е изтекъл, дали името на сайта, което е закодирано в сертификата, отговаря на реалният адрес, който е зареден в браузъра.

3. След като проверките минат успешно браузърът и сървърът определят какъв симетричен криптографски алгоритъм да използват за комуникация, примерно AES, RC4, 3DES и т.н., след което браузърът генерира произволен код (ключ), който криптира с публичния ключ на сървъра и изпраща криптирания код към сървъра.

4. След като сървърът получи кода браузърът вече може да прави заявки към сървъра, като използва за криптиране кода и криптографският алгоритъм, определен със сървъра на предходната стъпка.

**Принцип на работа на SSL**

По този начин между браузъра и сървъра се установява сесия, в която данните протичат криптирани и могат да бъдат декодирани (разчетени) единствено от уеб сървъра и съответния браузър.

**Защита на сайта ни чрез SSL сертификат.**

Ако е необходимо посетителите на вашия сайт да въвеждат лична и/или конфиденциална информация (платежни данни, информация за профили и акаунти, пароли за достъп, данни от кредитни карти, банкови сметки, документи за самоличност и т.н.) е на практика задължително да имате инсталиран валиден SSL сертификат и въвеждането на информацията да става чрез SSL протокола.

SSL сертификат е необходим и при всички външни страници, скриптове и уеб приложения, които се зареждат през Facebook.

### 3.5.3 VPN Виртуални частни мрежи

VPN (Virtual Private Network или виртуална частна мрежа) е частна мрежа, която използва публичната телекомуникационна инфраструктура и осигурява защита на предаваната информация като използва протоколи за тунелиране и криптографски алгоритми. Тя може да бъде противопоставена на система от притежавани или наети линии, които се използват само от една компания. С други думи VPN е комуникационно оборудване, при което достъпа се контролира за да се допуснат равни връзки само вътре в определената общност от интереси. В този случай частния ресурс се изгражда набазата на логическо разделяне, а не на физическо.

Има 3 основни VPN технологии:

•trusted VPN - доверена VPN;

•secure VPN – сигурна VPN;

•hybrid VPN – смесена VPN.

VPN тунелите, построени чрез криптографски алгоритми, позволяват използването на публичната мрежа Интернет за сигурен пренос на данните след като напуснат защитата на firewall-а. Това, което прави една VPN "виртуално" частна мрежа са тунелите. Тунелните технологии криптират и капсулират нашите мрежови протоколи в Internet protocol (IP). По този начин можем да рутираме, свързваме и поставяме филтри по същия начин както с всяка обикновена WAN връзка.

Аутентикация /Автентификацията/. Още един стъпка опредедляща за сигурността при VPN комуникацията е аутентикацията. На тази стъпка, получателят на данните определя дали изпращача наистина е този за който се преддставя (User/System Authentication) и дали данните са били пренасочвани или повредени по пътя (Data Authentication).

Аутентикацията на VPN клиента включва проверката за истинност на самоличността на машината и на потребителя, който инициира VPN връзката. Аутентикация може да бъде осъществена на нивото на машината. Например, когато една VPN връзка, базирана на Windows 2000, използва IPSec за L2TP VPN мрежа, сертификатите на машините се обменят като част от изграждането на IPSec асоциация за сигурност. Потребителят може

да бъде автентифициран с помощта на един от няколкото метода за автентификация, като Extensible Authentication Protocol (EAP), Challenge Handshake Authentication Protocol (PAP) или Shiva PAP (SPAP).

Оторизация означава зададените ограничения, на базата на които на едни потребители се предоставя достъп до VPN, а на други се отказва.

Криптирането служи за защита на данните във VPN мрежи. Могат да бъдат използвани най-различни технологии за криптиране. Много VPN реализации позволяват да се избере метода на криптиране, който трябва да бъде приложен. Криптирането осигурява сигурност на данни, които пътуват по VPN мрежата. Без тази сигурност данните биха могли лесно да бъдат прехванати, докато се предават по обществената мрежа.

Криптирането е техника на кодиране и разкодиране на информация. На всеки край на VPN тунела има VPN gateway в софтуерна или в хардуерна форма. Gateway-а на изпращача криптира информацията преди да я изпрати по тунела през Internet. VPN gateway-я на получателя декриптира информацията.

Ключът е код, който криптиращият алгоритъм използва за да създаде уникален кодирана информация. Нивото на сигурност зависи непосредствено от дължината на използваните ключове. VPN продукти днес използват 168 и повече bit-ови ключове.

Повечето VPN използват IPSec технологии. IPSec е съвместим с повечето различен VPN хардуер и софтуер и е най-популярен за мрежи с клиенти, които ползват отдалечен достъп. Даден IPSec тунел основно играе ролята на мрежов слой, който предпазва всичките пакети от информация, които преминават, независимо от приложението.

### 3.5.4 Предимства и недостатъци на VPN мрежите

Предимствата на VPN мрежите са свързани с намаляване на разходите за междуградски разговори, когато отдалечените потребители се намират извън областта за набиране на локални номера. Тези мрежи изискват по-малко телефонни линии за осигуряване на отдалечен достъп до множество потребители едновременно. Също така изискват по-малко хардуерно оборудване, например банки от модеми. VPN мрежите, базирани на ISP, редуцират цените за администриране и обучение.

Като недостатък може да се приеме изискването за връзка към Internet в двата края на VPN мрежата. Това може да бъде проблем, ако единият или двата края имат ненадеждна връзка към Интернет. Друг недостатък на VPN мрежите се състои в проблемите, свързани с производителността. Те могат да бъдат от незначителни до съществени, в зависимост от типа на реализацията на VPN и от типа на използваните Internet връзки. Проблемите на производителността, свързани с VPN мрежите, могат да

бъдат категоризирани по два начина: общи проблеми на производителността и проблеми, които са специфични за конкретни VPN реализации.

Една от алтернативите на VPN мрежата е dial-up комуникацията. В някои случаи dial-up сървърът може да постигне същата цел както VPN мрежата, но при много други обстоятелства виртуалната мрежа има определени предимства пред услугата на dial-up сървъра за отдалечен достъп.

Проблемите свързани с производителността на VPN мрежите, могат да бъдат категоризирани по два начина: общи проблеми на производителността и проблеми, които са специфични за конкретни VPN реализации. Повечето сериозни проблеми на производителността се дължат на глобалната мрежа Интернет. Често възникват прекъсвания на достъпността от регионален и от всеобщ характер. Тежкият трафик може да предизвика забавяния и блокирания на системите. Освен това отделни ISP доставчици могат да се сблъскат с изключвания на сървъри, които обслужват стотици или дори хиляди свои потребители. Технологията на VPN мрежите може също да доведе до различни количества допълнителни служебни данни, които намаляват производителността. VPN мрежи на ниво вериги не могат да постигнат скоростта на виртуалните мрежи на ниво мрежа. Когато се използва обществената мрежа за установяване на връзката, се загубва елемента на контрол, който се реализира при директна входяща dial-up връзка.

### 3.5.5 Secure Electronic Transaction (SET) служи за защита на транзакциите с кредитни карти

Защита на електронната търговия. Система за защита на електронните транзакции SET.

Защита на електронната търговия. За осигуряване на сигурност на транзакциите се използва SSL - протокол за връзка между браузера на клиента и сървъра. В момента в който влезете в режим на SSL, на най-долния ред на браузера се появява знак /жълт ключ на син фон при Netscape Navigator или жълт катинар при Microsoft Internet Explorer/. Ако натиснете този знак с мишката, се появява и при двата браузера прозорец с информация за сертификата, който сървъра притежава и за режима на криптация /шифриране/ на данните, които се обменят с клиента.

След като сървъра е разпознат, двете страни си обменят криптографски ключ, който ще служи за криптиране да данните от предстоящата сесия между тях. Този ключ важи само за текущата сесия, при всяка следваща връзка на клиента със сървъра ключът е друг. SSL използва алгоритъм за обмяна на ключове с публична и секретна част (напр. RSA).

За да може сървърът да се увери, че клиентът е този, за който се представя под SSL е необходимо клиентът да има свой собствен

сертификат. Тъй като това е трудно да се реализира (и скъпо), тази схема се прилага само между сървъра и търговците. Клиентите се представят пред сървъра със своята потребителска парола.

Secure Electronic Transaction (SET) или на български - Защита на електронния паричен превод е стандартен протокол за осигуряване на транзакции на кредитни карти през несигурни мрежи, и по-конкретно, в Интернет. SET не е система за плащане, а по-скоро набор от протоколи и формати за сигурност, която позволява на потребителите да използват съществуващата кредитна карта за плащане в една отворена мрежа по сигурен начин.

При използване на SET се прибягва от страна на търговеца до услугите на трето лице, финансов посредник. Номерата на картата на потребителя не се разкриват директно на търговеца. В момента на плащането, банковите данни се изпращат в криптирана форма директно до лицата, ангажирани пряко с извършването на паричния превод. Те единствено могат да дешифрират данните, така че да проверят валидността на превода. След това тяхната система изпраща кодирано потвърждение до търговеца, че плащането е осъществено. Този метод дава допълнителна безопасност поради факта, че търговецът никога не вижда банковата информация, а посредникът съхранява информацията само за периода на извършване на паричния превод.

# ЧЕТВЪРТА ГЛАВА

## 4.1 Конфигуриране на защитена VPN връзка

Има две големи групи VPN технологии така наречените Carrier и Enterprise типове. Най-просто разликата между тях е следната:

При Carrier типа, доставчика ти на телекомуникационната услуга се грижи някак си да я направи тази частна мрежа. Може да използва свои технологии (най-добре Layer2 мрежа, като Ethernet, с Ethernet VLAN или 802.1ac, ad, 1ag, 1ah, QinQ или MACinMAC технология, или грешката на природата – MPLS, за която мога да пиша много, или L2TPv3), това няма значение. Важното е, че потребителя, не прави нищо, за да съществува тази мрежа. Не му трябва специална конфигурация. Не му трябват специални устройства. Не му трябва специален софтуер.

При Enterprise VPN технологиите, потребителя си прави всичко, а доставчика на телекомуникационни услуги обикновено дори не знае, че потребителя прави такива неща. Към тези технологии се числят L2F, GRE, IPSEC, PPTP, L2TPv2, SSL Tunnels и други.

Дори обаче да имате Carrier VPN осигурен от някакъв телекомуникационен доставчик, обикновено вие не искате да се откажете

от възможността през интернет да се свържете с „корпоративната мрежа” и да точите от там големите корпоративни тайни. Особено, ако пътувате често, като мен, възможността винаги, и от всякъде да можете да достъпите офисните ресурси е много ценна. Така достъпвате вътрешните сървъри, или звъните на импулсни телефони през фирмената IP телефонна система, или може да изпращате mail от фирмата, и дори да заблуждавате успешно шефа си, че работите. Този отдалечен метод на работа май се наричаше “telecommuting”, и има много качества, и един основен недостатък за фирмата – няма как шефа да разбере дали отдавате времето си на работата, или на странични занимания.

Всички експериментират с вградените в Windows така наречени стандартни технологии (PPTP, IPSEC, L2TPv2) или с частни имплементации като Cisco и Juniper-ските VPN клиенти.

Макар да става все по-очевидно, че повечето технологии за криптиране на VPN са сертифицирани и разработени от Националния институт по стандартизация и технологии (NSA), новите разкрития от страна на Едуард Сноудън, които показват, че NSA са работили в продължение на години по разработването на начини за разрушаване и кракване на тези технологии, са някак шокиращи. Това определено повдига въпроса „Надеждни ли са наистина тези VPN технологии“?

В следващия абзац са представени VPN протоколите и как те мога да покрият нуждите на потребителите.

## 4.2 PPTP

Този тип протокол е основан от корпорацията Microsoft. Point-to-Point Tunneling изгражда виртуална частна мрежа върху dial-up мрежи, и от самото си създаване е стандартния протокол за VPN. Това е първият VPN протокол поддържан от Windows, PPTP предоставя защита, като разчита на множество методи за заверка, като MS_CHAP v2, който е най-обикновеният от всички.

Всяко подходящо за VPN устройство и платформа има наличен PPTP по подразбиране, и предвид това, че настройването му е относително лесно, той си остава първи избор, както за VPN доставчиците, така и за бизнеса. Също така, прилагането му изисква сравнително малко служебни ресурси, което го прави един от най-бързите VPN протоколи налични днес.

Макар и да използва 128-битово криптиране обаче, този протокол е доста уязвим откъм сигурността, с възможността декапсулирана MS-CHAP v2 заверка да е най-пагубна. Поради това, PPTP може да бъде кракнат за два дни. И макар пролуката да бе закърпена от Microsoft, самият технологичен гигант препоръчва на VPN потребителите да ползват SSTP или L2TP вместо това.

Тъй като PPTP е толкова несигурен, едва ли е изненада, че декриптирането на PPTP криптирани комуникации почти сигурно е стандарт в NSA. Въпреки това, още по-тревожен е фактът, че последните са декриптирали (или са напът да го сторят) огромни количества по-стари

данни, които са били криптирани когато PPTP все още се смяташе за надежден протокол от експертите по сигурността.

Предимства

- Бърз.
- Вграден клиент в почти всички платформи.
- Лесен за настройване.

Недостатъци

- Компрометиран е от NSA.
- Не е съвсем надежден.

### 4.3 L2TP и L2TP/IPsec

Layer 2 тунелен протокол, за разлика от други VPN протоколи, не предоставя никаква поверителност или криптиране на трафика, преминаващ през него. Поради това, той обикновено се имплементира със сюита от протоколи познати като IPsec, за да криптира данните преди предаване, предоставяйки на потребителите поверителност и сигурност.

Всички съвременни съвместими с VPN устройства и операционни системи са с вграден L2TP/IPsec. Настройването е също толкова бързо и лесно като PPTP, но може да има и проблеми, тъй като протоколът

използва UDP порт 500, който е лесна цел за блокиране от страна на NAT защитни стени. Следователно, може да се изисква препращане на порт, ако се използва със защитна стена.

Няма някакви големи уязвимости, асоциирани с IPsec криптирането, и все още може да е надеждно ако бъде приложено правилно. Джон Гилмор, който е един от основателите и специалист по сигурността в Electric Frontier Foundation, твърди, че е много вероятно протоколът да е бил целенасочено отслабен от NSA. Още повече, предвид това, че LT29/IPsec протоколът капсулира данните два пъти, той не е толкова ефикасен в сравнение със SSL базираните решения, и следователно е малко по-бавен от другите VPN протоколи.

Предимства

- Обикновено се определя като надежден.
- Наличен на всички модерни устройства и операционни системи.
- Лесен за настройване.

Недостатъци

- По-бавен от OpenVPN.
- Може да бъде компрометиран от NSA.

- Може да бъде проблематичен ако се използва с ограничаващи защитни стени.

- Вероятно е NSA преднамерено да са отслабили протокола..

### 4.4 OpenVPN

Сравнително нова технология с отворен код, OpenVPN използва SSLv3/TLSv1 протоколи и OpenSSL библиотека, ведно с комбинация от други технологии, за да предостави на потребителите надеждно и силно VPN решение. Протоколът предлага подробно конфигуриране и работи най-добре на UDP порт, но може да се настрои да работи също и на всеки друг порт, което прави изключително трудно за Google и други подобни услуги да го блокират.

Друго чудесно предимство на този протокол е, че неговата OpenSSL библиотека поддържа разнообразни криптографски алгоритми, като 3DES, AES, Camellia, Blowfish, CAST-128 и други, въпреки че Blowfish или AES се използват изключително от VPN доставчиците. OpenVPN идва с вградено 128-битово Blowfish криптиране. То обикновено се смята за надеждно, но има също и някои известни слабости.

Когато става дума за криптиране, AES е най-новата достъпна технология и се смята за „златен стандарт“. Това е така, просто защото няма известни слабости, дотолкова, че е приета от правителството на САЩ и правителствените агенции, които я използват за защита на „надеждна“

информация. Тя може да се справя с по-големи файлове сравнително по-добре от Blowfish, благодарение на нейния 128-битов размер на блока в сравнение с 64-битовия блоков размер на Blowfish. Въпреки това, и двете технологии са сертифицирани по NIST шифри, и макар вече да са широко разпознаваеми като проблематични, има някои конкретни проблеми с тях, които ще разгледаме по-долу.

Първо, колко бързо работи OpenVPN протоколът зависи от нивото на използваното криптиране, но обикновено е по-бърз от IPsec. Макар вече OpenVPN да е протоколът по подразбиране за VPN връзка за повечето VPN услуги, той все още не се поддържа от всички платформи. Поддържа се обаче от всички софтуерни продукти от трети страни, което включва Android и iOS.

Относно настройването, то е малко по-усложнено от това на L2TP/IPsec и PPTP, особено когато се използва общият OpenVPN софтуер. Не само, че трябва да свалите и инсталирате клиента, но трябва също да настроите допълнителни конфигурационни файлове, което изисква проучване. Няколко VPN доставчици се сблъскват с този конфигурационен проблем предвид наличието на персонализирани VPN клиенти.

Взимайки предвид всички тези фактори обаче, както и предоставената от Едуард Сноудън информация, изглежда OpenVPN нито е бил отслабен, нито компрометиран от NSA. Той също така се смята за имунизиран срещу атаки от страна на NSA, поради това, че използва краткотраен обмен на ключове. Безспорно, никой не е наясно с пълните възможности на NSA, но

наличните данни и чисто математически зависимости сочат, че най-вероятно OpenVPN в комбинация със силен шифър, е единственият VPN протокол, който може да се смята за надежден.

Предимства

- Може да заобикаля повечето защитни стени.
- Позволява подробно конфигуриране.
- Тъй като е с отворен код, лесно може да бъде проверен за задни вратички.
- Съвместим е с множество алгоритми за криптиране.
- Изключително надежден.

Недостатъци

- Може да е малко сложен за настройване.
- Изисква софтуер от трети страни.
- Поддръжката за настолни системи е отлична, но за мобилни устройства се нуждае от подобрения.

## 4.5 SSTP

Представен за първи път от корпорацията Microsoft в Сервизен пакет 1 на Windows Vista, тунелният протокол за защитени сокети (SSTP) вече е наличен за SEIL, Linux и RouterOS, но все още е ориентиран предимно към Windows базирани системи. Предвид това, че използва SSL v3, той предоставя предимства, сходни с тези на OpenVPN, като например способността да предотвратява проблеми на NAT защитни стени. SSTP е стабилен и лесен за ползване VPN протокол, отчасти защото е интегриран в Windows.

Той обаче си остава патентован стандарт, собственост на Microsoft. Макар технологичният гигант да има история на сътрудничество с NSA, съществуват и теории за вградени в операционните системи Windows задни вратички. Ето защо този протокол не буди такова доверие както други стандарти.

Предимства

- Може да заобикаля защитни стени.
- Нивото на сигурност зависи от шифъра, но обикновено е надеждно.
- Изцяло интегриран в операционната система Windows.
- Поддръжка от Microsoft.

Недостатъци

- Предвид това, че е патентован стандарт, собственост на корпорацията Microsoft, не може да бъде проверен за задни вратички.

- Работи само на Windows-базирани платформи.

### 4.6 IKEv2

IPsec базираният тунелен протокол, Internet Key Exchange Version 2, е разработен съвместно от Cisco и Microsoft, и е интегриран в 7-ма версия и тези след нея на Windows платформите. Той идва със съвместими и разработени версии за Linux и множество други платформи, и също така поддържа Blackberry устройства.

Наричан от Microsoft VPN Connect, той е добър в автоматичното възстановяване на VPN свързаност при временно разпадане на интернет връзката. Мобилните потребители имат най-голяма полза от IKEv2, предвид това, че Mobility и Multi-homing протоколите предлагани от този стандарт, правят смяната на мрежи изключително гъвкава. Освен това, той също така е отличен стандарт за Blackberry потребители, тъй като IKEv2 е измежду малкото VPN протоколи, които поддържат Blackberry устройства. Макар IKEv2 да е наличен за сравнително малко платформи в сравнение с IPsec, той се смята за еднакво добър по отношение на стабилност, сигурност и производителност.

Предимства

- Изключително надежден – поддържа многообразие от шифри като 3DES, AES, AES 256.

- Идва с поддръжка на Blackberry устройства.

- Стабилен е, особено при възстановяване на свързаността при разпадане на връзката или при прехвърляне от една мрежа на друга.

- Лесен е за настройване, поне от страната на обикновения потребител.

- Сравнително по-бърз от L2TP, PPTP и SSTP.

Недостатъци

- Поддържа се на ограничен брой платформи.

- Използваният UDP 500 порт е лесен за блокиране в сравнение със SSL базираните решения, като SSTP или OpenVPN.

- Не е с отворен код.

- От страната на сървърите, изпълнението на IKEv2 е доста усложнено, което може да доведе до няколко потенциални проблема.

## 4.7 Проблеми и концепции

За да разберете криптирането, трябва да схванете няколко ключови концепции, всяка от които ще разгледаме по-долу.

**Дължина на криптиращия ключ**

Най-грубият начин за определяне на времето, нужно за разбиване на даден шифър, е известен като дължина на ключа, който представлява прости числа съставени от единици и нули, които се използват в шифъра. По същия начин, задълбоченото търсене на ключ (или брутални силови атаки) е най-грубата форма на атака върху даден шифър, когато опитвате всяка възможна комбинация до откриването на правилната. По отношение на дължината на ключа, нивото на криптиране използвано от VPN доставчиците е между 128 и 256 бита. По-високи нива се използват за удостоверяване автентичността на данни и при използване на Handshake протокола, но това означава ли, че 256-битовото криптиране е по-добро от 128-битовото?

За да намерим отговор на този въпрос, нека погледнем няколко статистически данни.

- За да се разбие надеждно 128-битов шифриращ ключ, са нужни 3.4×10(38) операции.

- За да се разбие надеждно 256-битов шифриращ ключ, е нужна 2(128) пъти повече изчислителна мощ в сравнение със 128-битов шифриращ ключ.

- Бруталната атака на 256-битов шифриращ ключ изисква 3.31 x 10(65) операции, което почти се равнява на броя на атомите във Вселената.

- Fujitsu K, най-бързият суперкомпютър за 2011, постигна Rmax скорости до 10.51 петафлопа. Взимайки тази стойност предвид, да разбие 128-битов AES ключ по силовия метод, би му отнело приблизително около 1 милиард години.

- NUDT Tianhe-2, най-бързият суперкомпютър в света за 2013, регистрира Rmax скорости до 33.86 петафлопа. Това е почти 3 пъти по-голяма бързина от тази на Fujitsu K, и за да разбие 128-битов AES ключ по силовия метод, би му отнело приблизително около една трета от 1 милиард години.

Допреди новите разкрития на Едуард Сноудън, масово се шириле убеждението, че 128-битовото криптиране е непробиваемо по силовия метод, и че това ще остане така през следващите 100 и повече години. Предвид факта обаче с какъв необозрим ресурс разполага NSA, доведе до това, няколко експерта и системни администратори по света да обновят дължината на шифриращите ключове. Заслужава си да споменем, че правителството на САЩ използва 256-битово криптиране, за да обезпечи сигурността на важни данни (128-битово криптиране се използва за рутини нужди). Въпреки това обаче, дори и при използването на този метод, AES, може да създаде известни проблеми.

## 4.8 Шифри

Шифрите представляват математически алгоритми, които се използват за криптиране, тъй като слабите алгоритми са уязвими откъм хакерски атаки, като им позволяват лесно да разбиват криптирането. Blowfish и AES са безспорно шифрите, на които потребителите на VPN е най-вероятно да се натъкнат. Освен това, RSA се използва за криптиране и декриптиране на шифроващите ключове, докато SHA-1 и SHA-2 се използват за разпознаване на данни като остаряла функция.

Днес обаче, AES се счита за най-надеждния шифър за VPN, дотолкова, че приемането му от страна на правителството на САЩ се отрази значително на популярността и възприемането му като много надежден. Има причини да се вярва обаче, че това доверие може да е неоправдано.

NIST

SHA-1, SHA-2, RSA и AES, всички те са сертифицирани или разработени от Националния институт по стандартизация и технологии на САЩ (NIST), който е институция, работеща в тясно сътрудничество с NSA за разработването на нейните шифри. Сега като знаем за системните опити от страна на NSA за изграждане или отслабване на задни вратички в стандартите за криптиране, със сигурност има смисъл от повдигането на въпроси относно интегритета на NIST алгоритмите.

Макар NIST винаги да са отричали да са извършвали каквито и да е злодеяния (иначе казано преднамерено отслабване на криптографски стандарт) и да са се опитвали да увеличат публичното доверие, канейки

хора да вземат участие в предстоящите им стандарти свързани с криптиране, NSA бе обвинена от New York Times за заобикаляне на одобрен от NIST стандарт за криптиране, чрез подриване на публичния процес на разработване и чрез въвеждане на неоткриваеми задни вратички, с цел отслабване на алгоритмите.

На 17 септември 2013, недоверието нарасна още повече, след като на потребителите бе тайно съобщено от RSA Security, да спрат да използват конкретен алгоритъм за криптиране, тъй като в него имало пролука, умишлено поставена от NSA.

Още повече, за един от стандартите за криптиране Dual EC DRBG, създаден от NIST, се шири мнението, че е бил несигурен в продължение на години, дотолкова, че попада в полезрението на технологичния университет в Нидерландия през 2006. Въпреки тези поводи за сериозно безпокойство обаче, там където NIST води, индустрията охотно я следва, най-вече поради факта, че спазването на стандартите на NIST е изискване за спечелване на договори от страна на правителството на САЩ.

Имайки предвид, че стандартите на NIST са вездесъщи по цял свят, през всички сфери на бизнеса и индустрията, свързани с поверителността, като например VPN индустрията, всичко това може да изглежда доста обезсърчително. След като много е заложено на тези стандарти, експертите в сферата на криптографията не показват желание да се заемат с проблема. Единствената компания, която го направи, Silent Circle, избра да преустанови пощенската си услуга Silent Mail, вместо да я види

компрометирана от NSA, и обяви, че отказва да се съобразява със стандартите на NIST през ноември 2013.

Благодарение на отразяването на този проблем, малкият, но въпреки това иновативен VPN доставчик, LiquidVPN, започна тестове и експерименти с нестандартизирани от NIST шифри. Това обаче е единственият VPN доставчик, за който знаем, че поема в тази посока. Следователно, засега ще трябва да се опитате да извлечете най-доброто от 256-битовото AES криптиране, което към момента е най-добрият наличен стандарт за криптиране.

**NSA атаки, насочени към криптирането с RSA ключове**

Едно от последните разкрития на Едуард Сноудън показва, че програма с кодово име „Cheesy Name“, е била разработена да набелязва криптиращи ключове, наречени „сертификати“, които може да са изложени на риск от разбиване от суперкомпютрите в GCHQ. Това определено предполага, че тези сертификати, които обикновено са защитени с 1024-битово криптиране, са по-слаби отколкото сме предполагали, и лесно могат да бъдат декриптирани, при това, доста по-бързо отколкото са очаквали от GHCQ и NSA. Един път декриптирани, целият минал и предстоящ обмен ще бъде компрометиран, чрез използване на перманентен личен ключ за декриптиране на всички данни.

В резултат на това, няколко форми на криптиране, които са зависими от временни ключове и сертификати трябва да се смятат за нефункциониращи, включително TLS и SSL. Това ще има огромен ефект върху целия HTTPS трафик. Все пак има и добри новини. OpenVPN, който

използва временни ключове, не би трябвало да бъде засегнат от това. Защо? Защото за всяка обмяна се генерира нов ключ, следователно на сертификатите не се дава шанс да се утвърдят.

Дори някой да успее да се добере до личен ключ на даден сертификат, декриптирането на комуникацията просто няма да е възможно. С атака от типа „посредник в средата“ (MitM), може да е възможно да се вземе на мушка OpenVPN връзка, но тя трябва да бъде специално взета под прицел, а и личния ключ трябва също така да бъде компрометиран. Откакто новината, че GHCQ и NSA са в състояние да разбиват 1028-битово криптиране стана публично достояние, доста VPN доставчици вдигнаха рязко нивата си на криптиране на 2048 бита, и дори на 4096 бита.

Perfect Forward Secrecy

Друга добра новина е, че решението на този проблем, дори за TLS и SSL връзки, не е толкова трудно ако уебсайтовете започнат да включват Perfect Forward Secrecy системи, при които за всяка сесия се генерира нов личен криптиращ ключ. За съжаление, поне до този момент, единствената голяма интернет компания включила системата Perfect Forward Secrecy е Google.

В края на този материал, бихме искали да последвате мъдрите думи на Едуард Сноудън, че криптирането работи криптосистемите трябва да се включат за подобряване на сигурността. Какъв е изводът, който следва да си направите от този материал? Всъщност е много прост. OpenVPN е най-надеждният наличен протокол и VPN доставчиците трябва да продължат да работят по утвърждаването и прилагането му. Би било просто чудесно,

ако доставчиците започнат да се отказват от NIST стандартите, но за това определено ще трябва да почакаме.

•PPTP е крайно несигурен. Той вече е компрометиран от NSA и дори Microsoft го изостави, ето защо би следвало да се избягва изцяло. Макар вероятно да намерите съвместимостта му с различни платформи и лесни настройки привлекателни, помнете, че потребителите могат да получат много от тези предимства и значително по-добро ниво на защита, като използват L2TP/IPsec.

•Като става дума за по-широка употреба, L2TP/IPsec е правилното VPN решение за вас, въпреки че е бил значително отслабен и компрометиран от NSA. ако търсите бърза за настройване VPN услуга обаче, която не изисква допълнителен софтуер, L2TP/IPsec все пак е полезен, особено за мобилни устройства, където поддръжката на OpenVPN остава колеблива.

•Въпреки необходимостта от сваляне и инсталиране на софтуер от трета страна на всички платформи, OpenVPN безспорно е най-доброто VPN решение за всички ваши нужди. Той е бърз, надежден и макар настройването му да отнема малко повече време, високото ниво на защита и поверителност, което ще ви предостави при сърфиране в интернет, определено си струва.

•IKEv2също е бърз и надежден протокол ако се използва заедно с решения с отворен код, особено за мобилни потребители, благодарение на способността му да се свързва отново автоматично при разпадане на връзката ви. Освен това, тъй като е един от малкото

VPN протоколи, които поддържат Blackberry устройства, той със сигурност е най-добрата опция, с която разполагате.

•SSTP предоставя на потребителите почти същите предимства, които предлага и една OpenVPN връзка, но само за базирани на Windows платформи. Ето защо, ще го намерите много по-добре интегриран в операционната система Windows от другите VPN протоколи. Той обаче далеч не се поддържа от всички VPN доставчици, поради това ограничение, а и поради факта, че Microsoft има продължително и добро сътрудничество с NSA, SSTP е протокол, на който нямаме особено доверие.

Накратко, би следвало винаги когато е възможно да ползвате OpenVPN, докато за мобилни устройства, добра опция е IKEv2. Като бързо решение, L2TP би се доказал като достатъчен, но предвид растящия брой OpenVPN мобилни приложения, ние все пак предпочитаме OpenVPN пред всички други протоколи.

Тук обаче аз искам да обърна внимание на един доста подценяван VPN клиент, който обаче за мен е номер едно, а именно OpenVPN клиента.

OpenVPN има няколко основни технологични качества, които много хора подценяват, но пестят много поддръжка и откриват много нови възможности. Първото качество (не особено технологично) е, че е Open. И се разпространява се на source. Работи и покрива всякакви платформи (освен телефони, за сега). Няма разлика между клиент и сървър. Всеки клиент, може да е сървър (и да се закачват към него други клиенти), и всеки сървър може да е клиент (който си е играл с Cisco PIX и е забелязал, че не може да имаш едновременно EasyVPN client и server на една и съща машина, ме разбира какво искам да кажа).

OpenVPN използва TCP или UDP сесия, за да реализира тунела си до сървъра. Тук може да звучи не толкова тържествено колкото използването на IPSec да речем, но реализирането на VPN на 6ти и 7ми слой по OSI модела, а не на 3-ти има съществени предимства. Много незапознати хора си мислят, че в Интернет света всичко е прекрасно, че всичко се развива логично, че протоколите са перфектни, няма дефекти, няма грешки, няма войни между производителите, и всичко е съвместимо. Много технологии са се развивали трудно и в противоречие с други. Някой са си направо несъвместими. Например Network Address Translation (NAT) технологията в продължение на дълги години (над 6) не позволяваше използването на IPSec протокол отворен от вътрешната към външната мрежа. Дори сега съществуващия направо смешен (за който го е чел) patch за IPSEC – така наречения NAT-T, не минава във всички възможни случаи, не се поддържа добре от производителите (да споменавам ли тук името Cisco? Например се поддържа в XP едва от последния Service Pack), както и Layer3 протоколи не съдържащи портове, като GRE например, не могат да минат

native през NAT.

Обаче поради свършването на IP адресите и бавния (поради бизнес причини) development на IPv6 правят така, че NAT е задължителният механизъм за връзка към Интернет на практически всяка фирма. Това значи, че ако сте на гости на някой във фирмата му, и искате да отворите VPN към вашата, и вашият VPN клиент използва технологии като IPSec или PPTP/L2TP (GRE), най вероятно няма да можете да отворите повече от една сесия (ако сте двама колеги), а вероятно дори и една. Да, някой Firewall-и (не и Cisco, предимно Linux базирани) поддържат инспекция на PPTP тунелите и позволяват пускането на повече от един (чрез инспектиране на Session ID-то в GRE тунела), или допускат IKE на 500 порт едновременно с IKE на 4500 порт, за да се осъществи NAT-T negotiation-а и да мине NAT-T на IPSec. Но пак да спомена – масовия Windows не поддържа NAT-T. Масовите Firewall-и не позволяват повече от една (дори и една) GRE сесия. Да не говорим за друг масов случай – параноята, която кара администраторите на някой мрежи да търсят механизми да стопират възможността за отваряне на VPN сесии от вътрешната мрежа на фирмата, към някъде навън, за да не може чуждия гост, да открадне голямата фирмена тайна (както споменахме – телефона на секретарката). Отделно някой фирми използват Proxy-та (къде заради кеш, къде, за да може шефа да събира най-интересните порно сайтове посещавани от служителите му, и после да си ги прегледа и той на спокойствие) и през тях не минава нито GRE (PPTP, L2TP), нито IPSEC. Представете си, че сте администратор, и нещастието ви е наложило да използвате някой от традиционните VPN механизми? Вашите още по-

нещастни колеги, търговци, щъкат по света и страната, и се опитват да си го вкарат (компютъра) в коя ли не мрежа, източвайки фирмените тайни на нещастните си клиенти. В момента, в който в напрегнат момент (търговецът е хванал секретарката на фирмата, а тя му разказва всичките тайни и тайни белези на шефа) вашия колега се опитва да се закачи към фирмената ви мрежа, за да изпрати ултра важен email, и не успее, виновния за това сте вие. Той ви се обажда, и вие имате срок от 30 секунди да направите дедукция на ситуацията, и да намерите най-простия механизъм да обясните на човека какво да направи със свободната си ръка, за да осъществи VPN сесията си. И това се случва всеки път, на всяко различно място. Вие си мислите „колегите ви са истински идиоти", колегите си мислят „администраторът е тъпак, не можа да подкара един VPN да работи като хората". А в действителност виновни са не еволюиралите технологии, и начина, по който са направени мрежите, които ползвате.

OpenVPN няма нито един от тези проблеми. Той минава през UDP или TCP. Може да бъде скрит зад HTTP request или каквото и да е. Може да работи с всеки Source и Destination порт. Може да го пуснете на DNS порта, и да изглежда като DNS заявка. Може да мине през 80-ти порт, през нормално или Transparent Proxy, изглеждащ като HTTP заявка. Може да мине през Socks (за разлика от Cisco Easy VPN, Juniper VPN, PPTP/L2TP/IPSec клиента в Windows, и какво ли още не). Това значи, че практически няма случай, ако сте в мрежа, където да има достъп до нещо от интернет каквото и да е то, и да не се закачите към фирмената си вътрешна мрежа. Ако конфигурационният файл е направен добре, клиента

може да пробва автоматично 4-5 различни начина за свързване, и повярвайте ми, аз така съм го направил, не съм намерил място, от където да не съм могъл да се свържа до сега.

OpenVPN отваря логически интерфейс за всеки тунел. Това за някой звучи естествено. За други може да прозвучи като „странен feature, какво значение има?”, но за нещастните потребители борили се като прасе с тиква с Cisco Easy VPN клиента, това значи много. И то много, много. Защото значи, че можете да пуснете повече от един VPN клиент едновременно, свързан към различна мрежа. Така, ако правите поддръжка и се намирате някъде в чужбина, може да сте закачени едновременно и към фирмата ви мрежа, и към мрежата на клиента, на който искате нещо да му наконфигурирате. Заради архитектурни дефекти според мен (аз имам теория тука, а тя е, че Индийските програмисти са лакоми, и ръцете им са заети да държат непрестанно фалафелите, които ядат, затова те програмират с краката си) Cisco VPN клиента не създава логически интерфейс. Поради това не можете да премаршрутизирате през него мрежа, която спешно поради някаква причина искате да мине от там. Не можете да пуснете повече от една VPN сесия едновременно от компютъра ви, да не говорим, че понеже е базиран на частна имплементация на IPSEC протокола (върху XAUTH IKE механизъм), не можете да имате QoS Policer и Security Policer пуснати на същия Windows, което значи, че не можете да управлявате QoS, или да използвате IPSEC или какъвто и да е друг VPN клиент базиран на IPSEC. Или щом сте с Cisco, ще сте с Cisco до живот, за добро или най-вече за лошо. Ако някой иска да си го чука у главата Cisco Easy VPN технологията, по добре да използва по-хубавия (и безплатен,

няколко пъти по-бърз, няколко пъти по-малък, с отворен код, по-малко бъгове и най-сетне имплементирани логически интерфейси) клиент – vpnc.

OpenVPN поддържа автоконфигурация. Това звучи странно, защото на фона на съвмрененните VPN клиенти, това е нещо нормално, но все пак има много такива, които не поддържат автоконфигурация. Например IPSEC не поддържа стандартно. Затова и има частни разширения (като това на Cisco през XAUTH в IKE-то) или изпълнения като пускане на IP върху PPP върху L2TPv2 върху IPSEC върху IP (Juniper и Microsoft, поне е сравнително стандартно). На OpenVPN можете да конфигурирате компресия, криптиращи и оторизационни протоколи, оторизация, мрежи, приоритети, DNS и Wins сървър, както и всяка DHCP възможна опция.

Една от екстрите е възможността да слагате приоритети на кофигурационните параметри в случай на конфликт. Така ако си пуснете VPN-а докато се намирате във вътрешната си мрежа, ако не сте с OpenVPN, най вероятно ще настане loop, мрежовият достъп ще преустанови, или VPN клиента ще умре с досадно съобщение (заради конфликт на IP адреси, или опит на тунела да си прекара собствения трафик през тунела) или просто няма да се отвори. Това е особено забележим проблем с Cisco VPN клиент под Windows. OpenVPN има механизъм как тези проблеми да бъдат решени незабележимо от страна на потребителя. Това значи, че администратора може да го инсталира (примерно openvpn-gui от http://www.openvpn.se) така, че да се стартира автоматично, винаги, и потребителя без значение къде се намира – в офиса или навън, ще достъпва офисните ресурси по скрит и незабележим за него,

но в същия момент сигурен начин. Служителите на фирмата може дори да не знаят, че имат VPN клиент.

OpenVPN поддържа огромен набор операционни системи – Windows (включително 95), всякакъв UNIX, върху всякакви платформи и процесори, Embedded Systems (като embedded Linux върху WRT54GL на Linksys), MACOS и други. В момента има експерименти за портването му под Symbian и Windows CE/Mobile. Това разнообразие е неприсъщо за друга технология, освен PPTP.

OpenVPN поддържа VPN сесия с Ethernet Bridging, а не само Routed VPN сесия. Повечето VPN клиенти изискват VPN сесията да бъде с различни IP адреси, и трафика към нея да се маршрутизира на Layer3 по OSI модела. Това обаче създава огромни проблеми, особено в по-големи фирми с по-сложни конфигурации. Налага се да се заделят специално IP адреси за VPN, да се провизионират по различен начин (без значение дали се ползват или не), и някак си да бъдат маршрутизирани към VPN сървъра. Което пък поставя ограничения къде в мрежата може да бъде VPN сървъра и т.н. При OpenVPN всички тези проблеми са решими, но има и по-хитър начин – Bridged клиента. Можете да направите така, че компютъра във VPN сесия да изглежда така все едно се намира в мрежата ви директно, да си взима IP адрес и конфигурация (дори и чрез 802.1x) по стандартния начин, от вашия DHCP сървър, и менажирането и следенето на това какво става да е централизирано, имайки в добавка и всички други споменати до сега предимства.

OpenVPN поддържа оторизация със сертификати, пароли или трети механизъм. Може да бъде разширен със скриптове, които да се стартират автоматично от страна на сървъра или клиента при закачване и да правят нещо допълнително, непредвидено в протокола. А и се разработва изключително активно. Може да оторизира не само в посока клиент-сървър, но и клиента може да оторизира сървъра и така да се пази от man in the middle атаки нещо, което е принципен проблем за всеки VPN.

Една друга възможност е използването на ptunnel - това е малко програмче, което позволява тунелирането на TCP трафик върху ICMP (или върху обикновен PING). То тунелира само една TCP сесия върху PING, но на мен това ми е достатъчно. Аз прекарвам отгоре OpenVPN сесия, през която си пренасям каквото си искам. Най-често употребявам комбинацията, когато съм в чужбина. Винаги се намира някой Wi-Fi доставчик, искащ половин кралство за 1ac, който е изфилтрирал TCP трафика (пренасочил го е), докато не сте си платили, но е забравил да изфилтрира PING-а. Така безплатно мога върху PING чрез ptunnel и OpenVPN да си прекарам VPN сесия, и да си ползвам интернет и офисни ресурси, без да плащам (истински Българин съм).

Създаване на прост VPN под Windows

Windows пристига зареден с клиент, който поддържа VPN PPTP и L2TP/IPsec протоколи. Инсталационният процес е прост: ако използвате Windows 8, просто изберете „Търсене” от страничната изскачаща лента на старт менюто и въведете в нея VPN, след което стартирайте VPN пътеводителя, като кликнете върху „Set up virtual private network (VPN)

connection”.

Използвайте този клиент, за да установите сигурна връзка с други Windows компютри или с други VPN сървъри, които поддържат PPTP и L2TP/IPsec протоколи - вие само трябва да зададете IP адрес или име на домейн на VPN сървъра, към който искате да се свържете. Ако ще установявате връзка с корпоративен или търговски VPN, ще се наложи да се свържете с администратора, за да научите правилния IP адрес. Ако имате ваш собствен VPN сървър под Windows, IP адреса му може да разберете, като въведете „CMD” в полето „Търсене”, след което ще се стартира конзолата, където на командния промпт напишете „ipconfig”. Този прост трик е по-удобен, когато използвате вашето Windows PC за VPN сървър, за да получите сигурен отдалечен достъп до вашите файлове отвсякъде.

Когато сте инсталирали PPTP VPN връзка под Windows, трябва да конфигурирате и вашият мрежов рутер да пропуска VPN трафика към Windows компютъра, към който искате да имате отдалечен достъп. За да направите това, първо трябва да се логнете в контролния панел на рутера (прегледайте потребителското упътване на производителя, за да разберете как става това) и задайте в port-forwarding или virtual-server настройките да препрати порт 1723 до IP адреса на компютъра, с който искате да се свързвате. Също така PPTP или VPN passthrough опциите трябва да бъдат разрешени в защитната стена, но обикновено те по подразбиране са така.

## Практическа реализация

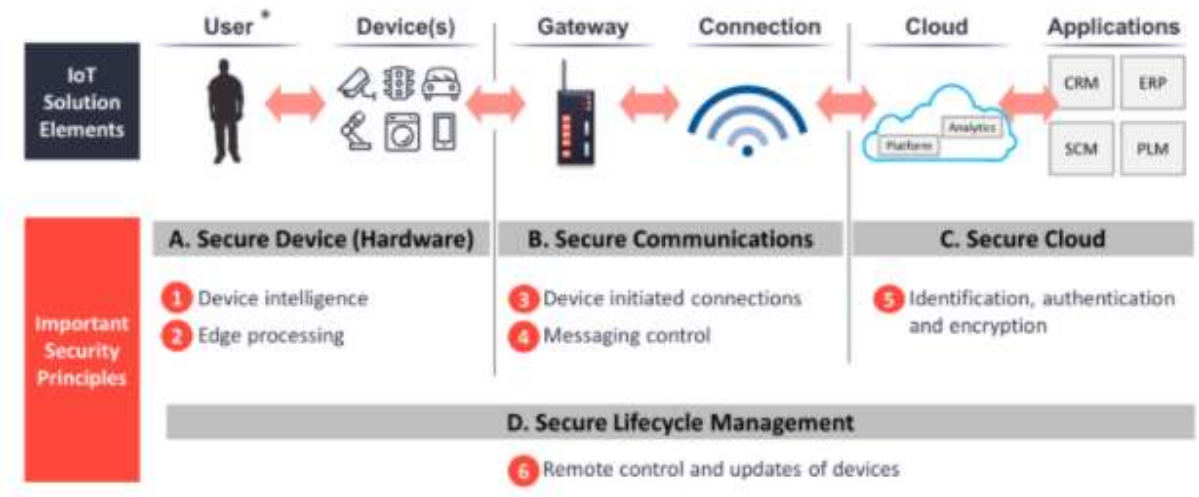
Наистина изисква малко работа и време, за да направите VPN, но това е една от най-умните и най-прости стъпки, които можете да предприемете, за да направите онлайн дейността си по-защитена и сигурна.

Решенията да предпазим всички входни и изходни данни при автоматично управление на нашите уреди (Internet of Things) се избира в зависимост от това колко устройства са свързани в мрежата. Ако са твърде много и не желаем на всяко едно от тях да бъде инсталиран VPN, може да се предпочете варианта да имаме VPN рутер.

## Направете ваш собствен VPN рутер

Ако искате да осигурите стабилен отдалечен достъп до цялата мрежа или site-to-site връзка, може да използвате рутер за вашата мрежа, който има VPN сървър и клиент.

Най-голямото предимство на това е, че ви позволява да свържете неограничен брой устройства към Интернет, като използвате една единствена VPN връзка. Правилният избор на протоколи, съобразени с нашите нужди и изисквания ще ни предостави най-добрия избор, който да ни осигури необходимата защита.




Фигура 1

В фигурата, дадена по-горе е описано концепцията за сигурността на Интернет на нещата. Първата А област, обхваща потребителя и комуникационните устройства, които използва. Това са смартфони, таблети, компютри. Защитата, която може да бъде осъществена тук е задаване на аутентикация, например парола, пин или пръстов отпечатък, с цел да осигурим допълнителна защита на своите комуникационни устройства.

В Б областта е комуникационния „канал“, който осъществява връзката между производител и потребител. Основната защита, която може да се предложи тук е изпълването на гореописания VPN рутер. Криптирането на данните е най-важната част от защитата тук. Дори и част от транзитните данни да бъде прихванатa, зложелателите няма да имат възможността да я декриптират, тъй като няма да имат криптиращия ключ.

За осигуряването на защитата на данните избрах OpenVPN, защото поддържа огромен набор операционни системи – Windows (включително 95), всякакъв UNIX, върху всякакви платформи и процесори, Embedded Systems (като embedded Linux върху WRT54GL на Linksys), MACOS и други.

Тук аз избрах да използвам следния модел рутер: ASUS RT-AC68U (Editor’s Choice: Best Overall)

Фигура 2

Този модел е компромисен вариант между цена, качеството, ниво на сигурност и спецификации. Има съвместимост със следните протоколи: PPTP, L2TP, and OpenVPN.

***Характеристики:***

**Производител:** ASUS; **Модел:** RT-AC68U

**Стандарт Wi-Fi:** 802.11ac

**Портове LAN:** 4 x RJ-45

**Портове WAN:** 1 x RJ-45

**Скорост на прехвърляне Ethernet (Mbps):** 10/100/1000

**Захранване:** 19V / 1.75A

**Тегло (кг):** 0.640

Антена: 3 x външна антена

Честота (GHz): 2.4 - 5

**Сигурност:**

WEP 64/128 bit

WPA, WPA2

WPS

Избрах този вид рутер, поради гореизброените в текущата глава предимства. Надеждност, гъвкавост, съвместимост и лесната конфигурация са предимствата, върху които наблегнах при избор на подходят хардуер.

**Заключение**

Развитието на телекомуникационните технологии, води освен до прогрес и до задълбочаване на проблемите в сигурността. Тъй като технологията се развива с изключително бързи темпове, пропуските в сигурността са все по-големи. Това налага обръщането на все повече внимание от производителите на софтуерни приложения, за които е необходимо осигуряването на надеждна защита на личната конфиденциална информация, която въвежда потребителя. Защитата на информацията е двустранен процес- както от страна на производителя, който трябва да осигури надеждна връзка между клиента и облачната платформа , така и

друга страна от самия потребител.

В настоящата магистърска теза беше представено подробно описание на актуалния проблем със защитата на Интернет данни днес. Бяха разгледани в детайли различните типове кибератаки, също така най-мащабните такива през последните години.

Представени са също и методи и практики за предотвратяване на неоторизиран достъп до конфиденциална информация. Благодарение на това, потребителите ще имат възможността да приложат методите и да успеят да осигурят своята Интернет сигурност. На вниманието на потребителя е представено VPN виртуална частна мрежа, която осигурява необходимата сигурност между двата участника в комуникационния процес.

**Списък на използвана литература**


1. http://www.soft-press.com/uploads/products/book74/chapter/chapter.htm
2. https://www.manager.bg/%D0%BB%D1%8E%D0%B1%D0%BE%D0%BF%D0%B8%D1%82%D0%BD%D0%BE/27-%D0%BD%D0%B5%D1%89%D0%B0-%D0%BA%D0%BE%D0%B8%D1%82%D0%BE-%D0%B7%D0%B0%D0%B3%D1%83%D0%B1%D0%B8%D1%85%D0%BC%D0%B5-%D1%81-%D0%BF%D0%BE%D1%8F%D0%B2%D0%B0%D1%82%D0%B0-%D0%BD%D0%B0-%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-1
3. https://softuni.bg/cms/news/details/265
4. https://technews.bg/article-23709.html
5. http://cio.bg/3964_aspekti_na_kibersigurnostta
6. http://www.aktivnasigurnost.org/bg/news-article/636/
7. http://vguides.net/view/69
8. https://www.investor.bg/analizi/262/a/nai-golemite-kiberataki-na-2017-g-252471/
9. https://www.investor.bg/temi/кибератаки/
10. http://tasicomputers.blogspot.bg/2015/03/blog-post_3.html
11.https://www.digital.bg/novini/20-%D1%81%D1%8A%D0%B2%D0%B5%D1%82%D0%B0-%D0%B7%D0%B0-

%D0%BF%D0%BE%D0%B2%D0%B5%D1%87%D0%B5-%D1%81%D0%B8%D0%B3%D1%83%D1%80%D0%BD%D0%BE%D1%81%D1%82-%D0%B2-%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-news18458.html

12. https://help.superhosting.bg/ssl-certificates-secure-communication.html

13.https://help.superhosting.bg/the-connection-to-this-website-is-not-fully-secure.html

14. http://techs-mobile.blogspot.com/2010/03/vpn.html

15. http://techs-mobile.blogspot.com/2010/05/blog-post.html